Análise dos Aspectos de Segurança das VPNs MPLS

Marcos A. de Siqueira[1,2], Marcel C. de Castro[1,2], Emílio T. Nakamura[1]

[1]CPqD Telecom & IT Solutions, Centro de P&D em Telecomunicações
Rod. Campinas – Mogi-Mirim (SP-340) km 118,5 CEP 13088-902 Campinas-SP Brasil

[2]Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp)
Caixa Postal 6101, CEP 13083-970 Campinas, SP

{siqueira,mcastro,nakamura}@cpqd.com.br

Abstract. *This paper presents the MPLS VPN architecture focusing its security aspects. The possible threats are classified in two visions: the user side and the provider side. The possible kinds of attacks from/to both sides are discussed, as well as new and well known solutions for attack prevention. Finally, some attack simulations are performed over a testbed network providing MPLS-BGP VPN services.*

Resumo. *Este artigo apresenta a arquitetura de VPN baseada no protocolo MPLS com foco em seus aspectos de segurança. Os possíveis problemas são classificados em duas óticas: a do usuário e a do provedor de serviços. São apresentados os possíveis tipos de ataques de/para ambos os lados bem como algumas soluções novas e outras já conhecidas para a prevenção destes ataques. Finalmente são descritas algumas simulações de ataque em laboratório à uma rede provedora de VPNs BGP-MPLS.*

Palavras chave. *PPVPN, MPLS, Segurança de Redes.*

1. Introdução

Em geral, VPNs (*Virtual Private Networks*) representam soluções de interconexão para sites remotos de clientes através de conexões encriptadas e seguras a partir de uma infra-estrutura pública como a Internet. Isso permite ao cliente economizar em termos de interconexões, com as mesmas facilidades de soluções tradicionais como linhas dedicadas. A conectividade VPN pode ser realizada através de túneis seguros entre os equipamentos do cliente como *Firewalls*. Neste caso, o cliente deve lidar com a complexidade do gerenciamento e configuração das VPNs tendo que custear a aquisição de equipamentos que implementam a funcionalidade VPN bem como o pessoal qualificado para configurar e manter as VPNs. Este é um cenário denominado *customer-based* VPNs.

Por outro lado, serviços VPN podem ser implementados pelo SP (*Service Provider*). Uma das vantagens desse tipo de VPN é que a tarefa de criar e manter as VPNs é realizada pelo provedor. Com isso, os clientes não necessitam adquirir hardware e/ou

software específicos para o estabelecimento de túneis, conectando com a rede do provedor através de soluções tradicionais como Frame Relay. Neste caso, é papel do provedor de serviços criar túneis entre seus nós de acesso e enviar o tráfego dos clientes através dos túneis corretos. Este cenário, chamado PPVPN (*Provider-Provisioned VPN*), permite a implementação de serviços convencionais como VPNs ponto-a-ponto baseadas no protocolo IP, tradicionalmente oferecidas sobre uma infra-estrutura Frame Relay ou ATM (*Asynchronous Transfer Mode*), bem como novos serviços como comunidades virtuais.

O interesse por esse tipo de VPN está crescendo rapidamente tanto pelos consumidores (empresas ou clientes residenciais) como pelos provedores de serviços. A motivação desse crescimento reside em aspectos econômicos e funcionais suportados pelo tipo de comunicação oferecida pelas VPNs IP. Porém um dos fatores limitadores na adoção em larga escala dessa tecnologia são os possíveis problemas de segurança da arquitetura devido a sua natureza baseada no protocolo IP. Este artigo analisa e apresenta soluções para diversos aspectos relacionados à segurança tanto da arquitetura de VPNs MPLS (*Multi-Protocol Label Switching*) como de sua implementação e operação em redes de ISPs (*Internet Service Providers*).

2. A Arquitetura VPN MPLS

Os componentes da Arquitetura VPN MPLS [1] são mostrados na Figura 1. Esta arquitetura foi moldada para satisfazer os seguintes requisitos de segurança [2]:

- **Separação de endereçamento e roteamento:** resolvido pela definição de um novo tipo de endereçamento denominado VPN-IPv4 [3] a ser divulgado pelo MP-BGP (*Multiprotocol - Border Gateway Protocol*) [4] entre os roteadores de borda da rede do ISP, ou PE (*Provider Edge Routers*), através da adição de um distintor de rotas (RD) ao endereço IPv4 de cada rota de cliente a ser propagada através da rede de núcleo. As rotas de diferentes VPNs são identificadas por diferentes RDs e são separadas nos roteadores PE através de tabelas de roteamento independentes denominadas VRFs (*VPN Routing and Forwarding Tables*).
- **Esconder o núcleo da rede dos provedores:** os roteadores dos clientes, ou CE (*Customer Edge Routers*) devem possuir conectividade IP com os roteadores PE, porém não devem ter conectividade IP com os roteadores do núcleo da rede MPLS do provedor, ou roteadores P (*Provider Routers*). O espaço de endereçamento visível pelos CEs deverá estar restrito ao endereço da interface do PE diretamente conectada ao CE e aos endereços de outros sites do cliente contidos na VRF associada a VPN do cliente no roteador PE. No núcleo da rede, os roteadores P comutam os pacotes com base no rótulo MPLS, não sendo necessário que estes conheçam rotas para os roteadores CE.

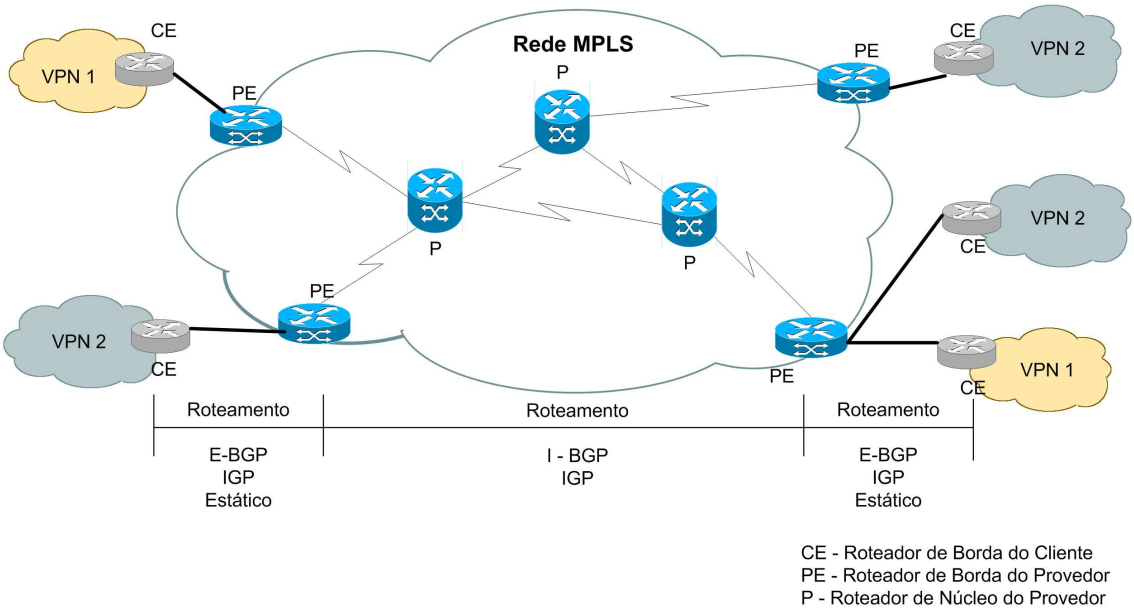

Figura 1: PPVPN (VPN BGP/MPLS)

- **Resistência a ataques provindos de clientes:** como os espaços de roteamento e endereçamento são separados entre diferentes VPNs, inicialmente o único ponto de ataque seria no *peering* entre PE e CE. Neste caso, técnicas de proteção conhecidas como ACLs (*Access Control List*) bloqueando SNMP, Telnet, ataques do tipo DoS, *spoofing* de IP, etc, bem como protocolo de roteamento com autenticação podem ser usadas para proteção de ataques provindos de clientes no circuito PE-CE.
- ***Spoofing* de rótulos MPLS:** para impedir que os roteadores dos clientes insiram pacotes rotulados com a intenção de atacar clientes de outras VPNs, interfaces dos PEs que são associadas a VRFs somente devem aceitar pacotes IPv4 puros, descartando qualquer pacote rotulado, prevenindo este tipo de ataque.

3. Questões de Segurança de PPVPNs

O objetivo de uma PPVPN é que o tráfego destinado a uma localidade chegue ao seu destino com a manutenção de todo o sigilo, a integridade e a autenticidade da comunicação. Isso significa que outro componente de uma rede não pode ter acesso (captura ou modificação) à informação que está trafegando na rede, bem como não deve ser possível injetar novo tráfego para a localidade.

Diversas técnicas e protocolos podem ser utilizados para que os objetivos da VPN possam ser alcançados, seja na camada de enlace (MPLS) quanto na camada de rede (IPSec), bem como na camada de aplicação (SSL) ou mesmo na camada física (arquitetura de rede).

O uso de uma PPVPN pode ser vista na Figura 1, que apresenta uma rede privada virtual definida em um backbone MPLS, que é formada entre PEs. Essas VPNs devem manter o mesmo nível de segurança de uma conexão Frame Relay ou ATM [7], por exemplo.

O nível de segurança da PPVPN envolve a arquitetura, a segurança de cada componente da Figura 1 e a interação existente entre eles. A existência de diferentes entidades também faz com que existam diferentes visões de segurança nesse ambiente.

O cliente PPVPN precisa de um nível de sigilo, integridade e autenticidade nas informações críticas e de negócios que são trocadas entre suas LANs via o backbone MPLS do provedor. Para isso, o cliente depende totalmente da segurança desse backbone MPLS, e deve preocupar-se com outros tipos de ataques que possam vir de outros pontos diferentes do backbone MPLS, que ele está confiando estar seguro. Já o provedor MPLS deve garantir essa segurança do backbone, já que o tráfego entre diferentes VPNs deve estar protegido.

Assim, pode-se considerar que esse cenário pode ser avaliado sob duas óticas: a do cliente (usuário), e a do fornecedor (provedor MPLS).

3.1. Ótica do usuário

O usuário deve considerar todos os aspectos envolvidos com a segurança da informação para proteger os seus negócios, tais como política de segurança, avaliações periódicas, estratégia e tecnologias de segurança (firewall, ids, criptografia, protocolos de segurança, etc). Além disso, o usuário deve conhecer as implicações de segurança relacionadas com a contratação de um provedor MPLS.

Quanto à proteção de sua rede interna, ela deve ser realizada usando-se técnicas e tecnologias amplamente discutidas na comunidade (porém não são simples de se implementar), e não receberá o foco aqui. O foco será dado na sua conexão com o provedor MPLS, que será utilizado para a comunicação com uma outra LAN.

O ponto fundamental existente no cenário que envolve um backbone MPLS é que a VPN é criada entre dois PEs, e eles são geralmente de propriedade do próprio provedor. Com isso, todos os acessos ao backbone MPLS dependem do provedor, de modo que o usuário deve confiar na segurança desse backbone. A próxima seção discute os aspectos de segurança a serem considerados nesse backbone MPLS.

Assim, o usuário que não confia no provedor VPN deve utilizar outros mecanismos de segurança para proteger suas informações, o que é recomendável, visto que a PPVPN é formada na camada de enlace ou na camada de rede, sem o uso de criptografia. Utilizar uma camada adicional de segurança, na camada de rede, como o IPSec, por exemplo, é recomendável nessas situações. Criptografia no nível de aplicação também pode ser utilizada, porém a sua escalabilidade deve ser avaliada antes da adoção dessa abordagem.

O fato do usuário não confiar no provedor de serviços faz com que a tecnologia utililizada para o provimento da PPVPN seja irrelevante do ponto de vista de segurança computacional. Mesmo que o provedor utilize mecanismos para assegurar confidencialidade no plano de dados do MPLS [5],[6], o usuário poderia ter motivos para não confiar nesse serviço. Assim, a solução realmente será o uso de segurança fim a fim na camada de rede a partir da própria rede do cliente.

Para a limitação de ataques do tipo DDoS (*Distributed Denial of Service*), o cliente pode solicitar que o provedor configure limitação na taxa que pode ser utilizada nas interfaces lógicas dos usuários. Isso é necessário quando o equipamento PE suporta

tanto serviço VPN quanto serviço Internet, especialmente quando esses serviços estão em uma mesma interface física.

3.2. Ótica do provedor MPLS

O provedor deve ser capaz de garantir que uma VPN não sofra interferência de outras VPNs, ou seja, cada túnel virtual deve ser acessível somente pelos usuários legítimos. Essa situação em uma rede MPLS é diferente de uma rede IP pura, onde o tráfego pode ser capturado e portanto deve ser cifrado. Em uma rede MPLS, a possibilidade de capturar tráfego de outros componentes não deve existir.

Assim, garantir que o núcleo da rede MPLS deve ser protegido, e mesmo invisível pelos usuários externos é essencial, já que ninguém, além do próprio provedor, pode ter acesso a esse backbone. Os roteadores PE e P devem assim estar corretamente configurados e com as listas de controle de acesso apropriadas. Qualquer erro de configuração do núcleo influi diretamente no nível de segurança, bem como *bugs* e vulnerabilidades, que podem ser exploradas em ataques. Erros na configuração do PE, por exemplo, podem resultar em problemas de segurança, como permitir que determinados CEs pertençam a VPNs erradas [7],[8]. Erros operacionais e na definição da arquitetura também são perigosos e podem resultar em acesso não autorizado ao backbone MPLS.

Deste modo, considerando que o backbone MPLS é seguro, outros métodos de ataques podem e devem ser considerados. Os roteadores PE podem ser atacados, bem como o mecanismo e sinalização do MPLS. Ataques internos do provedor, ou ataques ao provedor, que pode ser usado como ponte de entrada para o backbone MPLS também devem ser considerados.

O ataque ao PE é possível somente a partir da rede do próprio usuário (que pode ser atacado), sendo que não é possível atacar outros roteadores internos do backbone MPLS, devido à separação de endereços feita pelo MPLS.

O uso de ACLs nos roteadores para que somente o CE acesse o PE é importante, bem como avaliar o uso de autenticação dos protocolos de roteamento, como o MD-5 em BGP, OSPF ou RIP2. Mecanismos de proteção como o *dampening*, existente no protocolo BGP, por exemplo, permite que o número de interações de roteamento seja limitado, minimizando possibilidades de ataques DoS.

O *Label Spoofing* é similar ao *IP Spoofing*. Em uma rede MPLS, o redirecionamento é feito baseado nos *labels*, de forma similar ao roteamento baseado em endereços IP utilizado em uma rede IP. Como os *labels* são inseridos nos PEs, esse ataque só é possível caso um ataque ao backbone MPLS ou ao próprio PE seja realizado.

Para tornar os nós da rede de núcleo inalcançáveis, o provedor de serviços pode tornar as interfaces loopbacks dos roteadores (P e PE) inalcançáveis para os usuários externos e usuários internos sem autorização. Isto pode ser obtido através do uso de endereçamento separado para as interfaces loopback, não propagado externamente e com acesso limitado através de ACLs. Além disso, a propagação do TTL pode ser alterada para fazer com que o usuário externo ou sem autorização pense que o backbone MPLS está a um salto da saída, mas deve-se tomar cuidados para a prevenção de loops. Isso evita que o endereçamento do backbone seja exposto através de *traceroute*.

4. Soluções de Segurança

4.1. Erros de configuração dos equipamentos do provedor

Erros de configuração nos roteadores P e PE do backbone podem causar implicações como permissão de acesso indesejável entre VPNs ou mesmo entre usuários da Internet e determinada VPN, já que as PPVPNs deverão ser oferecidas sobre a mesma infra-estrutura de backbone usada para o fornecimento de serviço Internet. Serão descritas duas propostas para a solução deste tipo de problema: a primeira [8] propõe um mecanismo baseado na autenticação de rotas PE-PE propagadas pelo protocolo MP-BGP para solucionar problemas de segurança causados por erros de configuração nos equipamentos do backbone da rede. Já a segunda propõe um mecanismos de troca de tokens entre os CEs para a detecção de configurações errôneas no backbone da rede [9].

Para a autenticação de rotas PE-PE é proposto que a chave MD5 usada para autenticação no roteamento PE-CE seja reusada para autenticação no roteamento PE-PE. Como os PEs possuem várias tabelas de rotas VRFs, eventualmente associadas a VPNs distintas e conseqüentemente a clientes distintos, deverão ser usadas chaves diferentes para cada VRF. É proposto que as mensagens do tipo UPDATE do MP-BGP transportem um novo atributo denominado *UPDATE-authenticator* carregando um código HMAC MD5 da mensagem assinado com a chave PE-CE. A verificação de autenticidade deverá ser feita pelos outros PEs que possuem a chave MD5 obtida também através do mecanismo de autenticação do roteamento PE-CE como mostrado na Figura 2. A restrição é que a mesma chave deverá ser usada para autenticação PE-CE em todos os sites participantes de uma determinada VPN. A vantagem desse mecanismos é que para sua implementação na rede somente são necessárias alterações nos roteadores PEs, não demandando atualizações nos equipamentos de clientes.

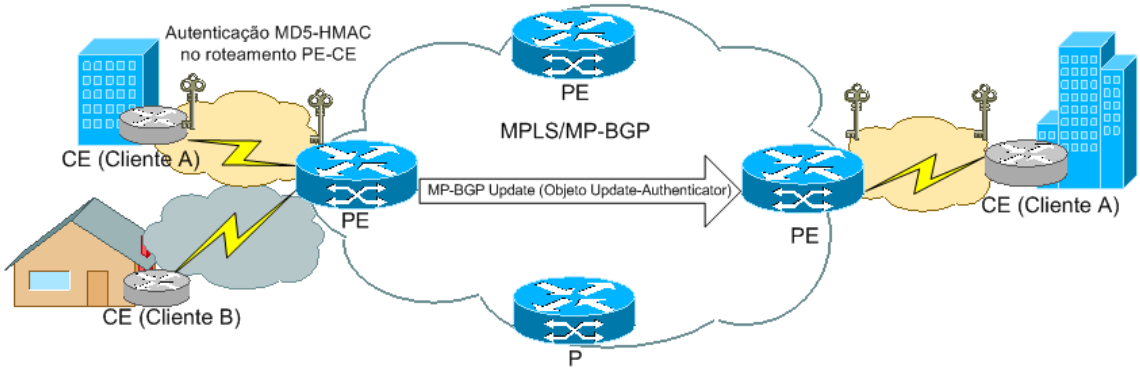

Figura 2: Autenticação de VPNs PE-PE

Já o mecanismos de troca de tokens entre CEs possibilita a geração de alarmes e/ou paralisação do mecanismo de roteamento de CE caso seja detectada a presença de tokens provindos de diferentes VPNs. Este fato caracterizaria um erro de configuração no backbone da rede pois é previsto que todos os CEs de determinado cliente participantes de uma VPN devem usar um único valor de token que deve ser propagado

periodicamente para todos os CEs através dos PEs conectados. Este mecanismo demanda a adição de mecanismos de sinalização tanto entre CEs e PEs como entre os PEs. Isso pode caracterizar uma desvantagem com relação ao modelo de autenticação entre PEs, já que é necessária a inserção de mecanismos de sinalização nos equipamentos dos clientes, o que não é sempre possível.

4.2. Simulação de ataques

Para a validação das técnicas de segurança propostas, foram configuradas duas VPNs baseadas em BGP-MPLS usando roteadores Cisco®. A rede MPLS foi configurada para não propagação de TTL, os roteadores PE foram configurados com ACLs bloqueando acesso de gerência SNMP, Telnet, e CDP originados na rede do cliente, e também ACLs bloqueando IP spoofing a partir da rede do cliente, os endereços das interfaces dos PEs diretamente conectadas aos clientes foram ocultadas através da técnica *IP unnumbered*, e o roteamento PE-CE foi configurado com OSPF com autenticação MD5.

Foram feitas diversas simulações de ataques ao PE e a VPN-B, a partir da VPN-A. As técnicas de *IP spoofing* e *Label spoofing* não obtiveram sucesso, a primeira sendo barrada pela ACL e a segunda pelo descarte de pacotes rotulados feito na interface do PE associada com uma VRF. Não foi possível a tentativa de ataque por *Label spoofing* no núcleo da rede por falta de acesso a esse.

5. Conclusão e Trabalhos Futuros

Após uma vasta investigação concluiu-se que a Arquitetura VPN MPLS apresenta o mesmo nível de segurança oferecido pelas tecnologias de camada de enlace como Frame Relay e ATM. Porém se o usuário não confia no provedor de serviços, nenhuma tecnologia de interconexão permite a garantia na confidencialidade dos dados do usuário. Neste caso, será necessária a aplicação de mecanismos que atuam fim-a-fim na camada rede a partir da rede do usuário, como o IPSec.

O nível de segurança equivalente à tecnologias de camada de enlace oferecido pelas VPNs MPLS pode ser comprometido por erros na configuração dos roteadores PE, podendo impactar na não separação de rotas e tráfego de diferentes VPNs. Foram apresentados dois mecanismos para a detecção e prevenção desse tipo de erro.

Finalmente, a segurança depende da implementação correta pelos provedores dos mecanismos de prevenção de ataques. Foram testadas algumas das possíveis técnicas de violação da arquitetura mostrando que a implementação da arquitetura VPNs MPLS do fabricante Cisco® não permite a aplicação de *label spoofing* na interface CE-PE, além de disponibilizar de diversos recursos como ACLs e roteamento com autenticação, restringindo possíveis ataques.

Considera-se que o trabalho futuro de implementação dos mecanismos de prevenção e detecção de erros de configuração de PPVPNs propostos nas referências [8] e [9] será de suma importância para a validação desses mecanismos.

6. Referências

[1] E. C. Rosen, et al., BGP/MPLS VPNs (RFC2547bis), IETF Internet Draft, Outubro 2002.

[2] R. Callon, M. Suzuki, A Framework for Layer 3 Provider Provisioned Virtual Private Networks, IETF Internet Draft, Março 2003.

[3] B. Fox, B. Gleeson, Virtual Private Networks Identifier, IETF RFC 2685, Setembro 1999.

[4] T. Bates, Y. Rekhter, R. Chandra, D. Katz, Multiprotocol Extensions for BGP-4, IETF RFC 2858, Junho 2000.

[5] T. Senevirathne, Secure MPLS Encryption and Authentication of MPLS payloads, IETF Internet Draft, Julho 2002.

[6] E. C. Rosen, J. D. Clercq, O. Paridaens, Y. T'Joens, C. Sargor, Use of PE-PE IPsec in RFC2547 VPNs, IETF Internet Draft, Fevereiro 2003.

[7] M. Behringer, Analysis of the Security of the MPLS Architecture, IETF Internet Draft, Outubro 2002.

[8] Michael Behringer, Jim Guichard, MPLS VPN Import/Export Verification, IETF Internet Draft, Janeiro 2002.

[9] R. Bonica, Y. Rekhter, R. Raszuk, E. Rosen, D. Tappan, CE-to-CE Member Verification for Layer 3 VPNs, IETF Internet Draft, Fevereiro 2003.