SEGURANÇA EM REDE PEER TO PEER USANDO TECNOLOGIA IPSEC EM UM AMBIENTE CORPORATIVO[*]

Giovani Francisco de Sant'Anna – Centro Universitário do Triângulo (UNITRI)
William Rodrigues Gomes – Centro Universitário do Triângulo (UNITRI)

RESUMO: Este artigo propõe a discussão do uso de Redes Peer-To-Peer dentro de um ambiente corporativo fechado, onde requer constante colaboração entre pessoas e empresas espalhados geograficamente. As empresas corporativas contam com uma forma de transmissão de dados segura e com menor custo usando a ferramenta open source FreeS/WAN, por isso a Rede Virtual Privada (VPN)destaca-se como uma alternativa para esses problemas e mostrar a importância de seguir as melhores práticas de segurança da informação para garantir que as informações sigilosas dos dados transferidos entre departamentos e empresas sejam criptografados, para garantir a autenticidade, confidencialidade e integridade dos dados, conforme as normas internacionais e nacionais (ISO 27002 ou ABNT ISO/IEC 27002).

PALAVRAS-CHAVE: IPSEC. Segurança. VPN. Peer to peer. Ambiente corporativo.

INTRODUÇÃO

No decorrer dos anos, as redes Peer-To-Peer (P2P) estão se desenvolvendo muito, por conta do grande interesse de usuários, empresas e meios acadêmicos, na busca de segurança no tráfego das informações. A segurança é o principal motivo de preocupação entre as organizações, uma vez que, seus dados podem estar vulneráveis a ataques de pessoas maliciosas, comprometendo as informações do ambiente corporativo.

As redes P2P são atrativas para essas corporações devidas alguns fatores, Primeiro: porque se dão bem em pequenas, médias e grandes empresas. Segundo: não possui um ponto central de falhas e Terceiro: as redes P2P dentro de um ambiente corporativo oferecem autonomia a seus participantes e administradores, onde poderá ser criada uma política de segurança da informação conforme a necessidade da organização (LOEST, 2007).

Este artigo apresenta como as redes P2P podem se comportar de maneira segura em um ambiente corporativo fechado em conjunto com a ferramenta open source FreeS/WAN, para que a comunicação segura entre matriz, filiais e funcionários operem segundo princípios de confidencialidade, integridade e autenticidade e que assumem uma grande importância nesse contexto.

Para garantir as melhores práticas de segurança da informação conforme as normas internacionais e nacionais (ISO 27002 ou ABNT ISO/IEC 27002) foram seguidas os itens 9.4 Controle de acesso à rede e 9.4.3 Autenticação de usuário para conexões externas.

Foi adotada uma ferramenta open source FreeS/WAN nos dois gateways para atender os itens das normas citadas acima, cuja denominação origina-se do termo *Secure Wide Area Network* (S/WAN). O FreeS/WAN é uma ferramenta de livre distribuição que trouxe para o IPV4 a segurança e criptografia de dados planejado para o IPV6, e uma ferramenta de configuração de VPN baseado no IPSec (SANT'ANNA, 2003).

[*] X EVIDOSOL e VII CILTEC-Online - junho/2013 - http://evidosol.textolivre.org

1 O QUE É UMA REDE PEER-TO-PEER

As Redes P2P são redes de computadores distribuídos e interconectados “ponto a ponto” onde cada nó tem a função de se organizar e compartilhar informações, arquivos, espaço de armazenamento, ciclos de CPU e capacidade de transmissão em uma cadeia descentralizada com tarefas e responsabilidades equivalentes. Essa arquitetura de rede descentralizada é mais difícil de ser interrompida, porque não existe um ponto central de falha (LOEST, 2007).

Todos os nós da rede são clientes e servidores, isso significa que não necessita de um servidor central para o funcionamento da rede, portanto, quanto maior a quantidade de nós na rede, maior será a capacidade de desempenho do sistema P2P (DUARTE *et al*.**,** 2012).

2 SEGURANÇA

A segurança é um dos maiores desafios da arquitetura P2P, o usuário que participa da rede, tem a obrigação de proteger os seus recursos e serviços de usurpação (falsificação). Um dos grandes problemas relacionados à segurança em rede P2P é permitir que usuários externos acessem informações e arquivos de determinados órgãos e empresas através da rede (BARCELLOS, 2006).

Todas as redes de computadores que se preocupam com a segurança, levam em consideração algumas propriedades de segurança, como:

- Disponibilidade.
- Confidencialidade.
- Autenticação.
- Integridade.
- Não repúdio. (KUROSE e ROSS, 2010; BARCELLOS, 2006).

2.1 Tecnologia IPSec

O IP Security Protocol (IPSec) é uma plataforma aberta formada por um conjunto de protocolos de segurança, que provê segurança na camada de rede, desenvolvida pela Internet Engineering Task Force (IETF). O IPSec tem como função proteger os datagramas IP na camada de rede, incluindo servidores e roteadores. A imagem abaixo, descreve como funciona o protocolo IPSec (KUROSE e ROSS, 2010).

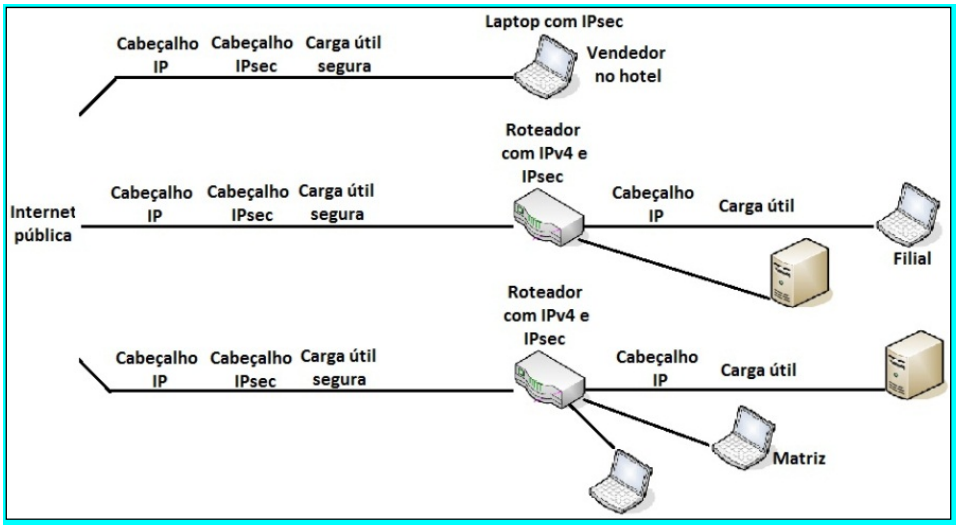

Figura 1: Protocolo IPSec. Fonte: Kurose; Ross (2010).

Conforme a figura 1, o protocolo IPSec trabalha da seguinte forma: quando um funcionário de uma empresa (matriz) manda um datagrama IP, ou seja, uma sequência de dados transmitida por uma rede IP a um vendedor, o roteador de borda da matriz converte o datagrama IPv4 em um datagrama IPSec e o encaminha pela internet.

Os dados IPSec transmitidos possuem também um cabeçalho IPv4 tradicional, portanto os roteadores na internet pública processam ele normalmente na rede. Mas além do cabeçalho IPv4 foi incluído um cabeçalho IPSec codificada, dentro da carga útil do datagrama IPSec. Quando o datagrama IPSec chegar ao laptop do vendedor, o sistema operacional decodifica a carga útil e posteriormente processam outros serviços de segurança, como exemplo a verificação da integridade dos dados, assim os dados não codificados são passados para a camada superior, camada TCP ou UDP (KUROSE e ROSS, 2010).

O IPSec é um conjunto de protocolos de segurança e algoritmos, fornecem alguns serviços como:

- Autenticação da fonte.
- Integridade dos dados.
- Privacidade nos dados.
- Sigilo das informações.
- Controle de acesso lógico.
- Privacidade no fluxo dos dados.
- Prevenção ao ataque de repetição (replay).

Para garantir a segurança citado acima, o IPSec utiliza dois protocolos principais: O Protocolo Cabeçalho de Autenticação (AH) e o Protocolo Cabeçalho de Encapsulamento de Dados de Segurança (ESP). Além desses dois cabeçalhos, o IPSec define também o conceito de associação de segurança (SA) (KUROSE; ROSS, 2010).

2.1.1 Associação de Segurança – SA

Todas as comunicações via IPSec são executadas sobre regras de uma SA, que é uma entidade P2P. A SA possui um conjunto de normas que permite negociar protocolos, chaves e algoritmos de encriptação, a ser usada posteriormente para estabelecer uma comunicação segura entre dois nós. Uma SA é unicamente identificada pela combinação de três parâmetros: pelo Índice de Parâmetro de Segurança *(Security Parameter Index* – SPI), pelo endereço do destinatário e pelo identificador do protocolo de segurança AH (número 51) ou ESP (número 50).

2.2.2 Protocolo Cabeçalho de Autenticação – AH

O objetivo do cabeçalho de autenticação é validar a identidade de entidades que estão se relacionando, entre o emissor e o destino. Isso ocorre para certificar se o emissor é realmente quem diz ser. Outra função do AH, é que ele consegue prevenir contra roubos de conexões, quando o ataque interrompe um pacote no decorrer de uma conexão, e passa a participar da comunicação (DUARTE; LOPEZ, 2003).Para validar a identidade entre o emissor e o destino no IPSec, o cabeçalho de autenticação usam dois algoritmos: o HMAC-MD5, RFC 2403 e o HMAC-SHA-1, RFC2004 (REZENDE e ROTOLE, 2012).

2.2.3 Protocolo Cabeçalho de Encapsulamento de Dados de Segurança – ESP

O Cabeçalho de Encapsulating Security Payload (ESP) foi criado para juntar os serviços de IPv4 e IPv6, ele pode ser executado tanto sozinho como em conjunto com o protocolo AH.

O protocolo ESP fornece integridade e confidencialidade aos datagramas IP através de

cifra dos dados, assegura um modo de encapsulamento num pacote IP inteiro (DUARTE; LOPEZ, 2003).

Portanto, o protocolo AH oferece serviços de autenticação, integridade dos dados, proteção anti-replay e não oferece confidencialidade dos dados. Já o protocolo ESP utiliza todos os serviços do protocolo AH, mais a confidencialidade dos dados e no fluxo dos dados. Como é demonstrado na figura 2, pode-se visualizar toda a estrutura do pacote IPSec, utilizando os protocolos AH e ESP.

Figura 2: Estrutura do Pacote IPSec. Fonte: Barbosa (2004).

O protocolo de cabeçalho de encapsulamento de dados de segurança utiliza dois algoritmos de criptografia: o DES e o 3DES, esses algoritmos são utilizados para confidencialidade de dados. O protocolo ESP possui outra característica muito importante, ele consegue combinar o algoritmo de autenticação HMAC-MD5 ou SHA-1 com o algoritmo de criptografia DES ou 3DES, para autenticação e confidencialidade da carga de dados (SANT'ANNA, 2003).

O Protocolo ESP pode ser utilizado de dois modos, o modo de transporte e o modo Túnel, conforme a figura 3.

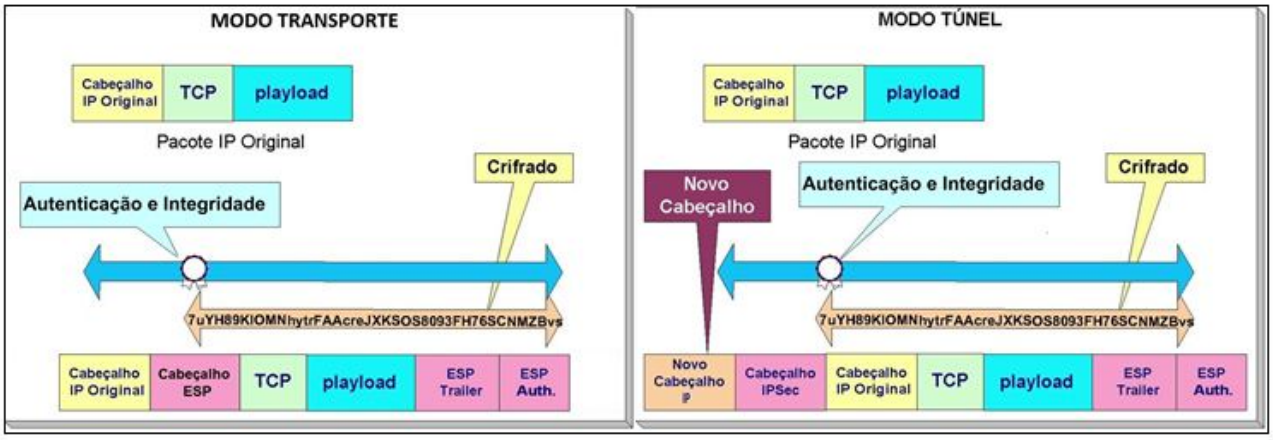

Figura 3: Modo Transporte e Modo Túnel. Fonte: Sant'Anna (2003).

O Modo de Transporte determina proteção dos protocolos da camada superior, na maioria das vezes ele é utilizado na comunicação entre dois nós, ou seja, cliente e servidor. Todos os dados da camada de transporte são criptografados, e o cabeçalho IP original permanece intacto, esse processo possibilita muita vantagem em redes pequenas, nas quais servidores e (nós) programam ou implementam o IPSec. Portanto, o cabeçalho IP passa sem segurança, permitindo que os dispositivos na rede pública vejam a origem e o destino final do pacote (ANDREOLI, 2012).

O Modo de Túnel providencia proteção ao pacote IP, onde é somado o cabeçalho IP original mais a carga de dados (payload) e adicionando um novo cabeçalho IP ao lado do cabeçalho IPSec. O que significa que pode ser usado para enviar dados criptografados através de um túnel, permitindo o envio dos dados independentemente da base utilizada. A grande vantagem que nesse modo à proteção contra a análise de tráfego, já que o atacante só poderá determinar o ponto de início e de fim do túnel, e não a origem e o destino real (ANDREOLI, 2012).

Vários tipos de encapsulamentos são usados para uma comunicação, podendo ser usado

da seguinte forma:

- Gateway-a-gateway
- Servidor-a-gateway
- Servidor-a-servidor

2.2.4 Internet Key Exchange – IKE

A Internet Key Exchange (IKE) é um protocolo de gestão de chaves que usa a porta 500 UDP, responsável pela criação, eliminação e alteração das chaves para autenticação e validação de informações, o IKE foi definido como regras de gestão o protocolo híbrido, constituído pelo ISAKMP e pelo Oakley, também denominado IKE. É usado para criar uma SA no IPSec, ou seja, negocia políticas de segurança e organiza as trocas das chaves de cada sessão (ANDREOLI, 2012).

Uma SA pode ser configurada manualmente em cada gateway por um administrador de segurança, ou pode ser alterada pelo protocolo IKE dinamicamente, para que possa garantir uma segurança ainda maior (SANT'ANNA, 2003).

3 UNIFICANDO A REDE P2P COM O PROTOCOLO IPSEC

Foi realizada uma simulação de um laboratório de análises clínicas no Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT. O principal objetivo é proteger as mensagens e resultados dos exames, que trafegam no interior da rede do laboratório, que estão conectados através dos outros roteadores (SANT'ANNA, 2003).

Na figura 4, é representado um laboratório sem criptografia em que o conteúdo do arquivo transferido da máquina (10.180.2.11) para a máquina (10.180.1.3), está trafegando na rede sem segurança. Dessa maneira um Sniffer (software interceptador de pacotes) poderá invadir a rede e capturar os exames que estão desprotegidos, esse tipo de ameaça faz com que o laboratório fique muito vulnerável em suas atividades, e consequentemente perderá a credibilidade no mercado e principalmente para com os seus clientes (SANT'ANNA, 2003).

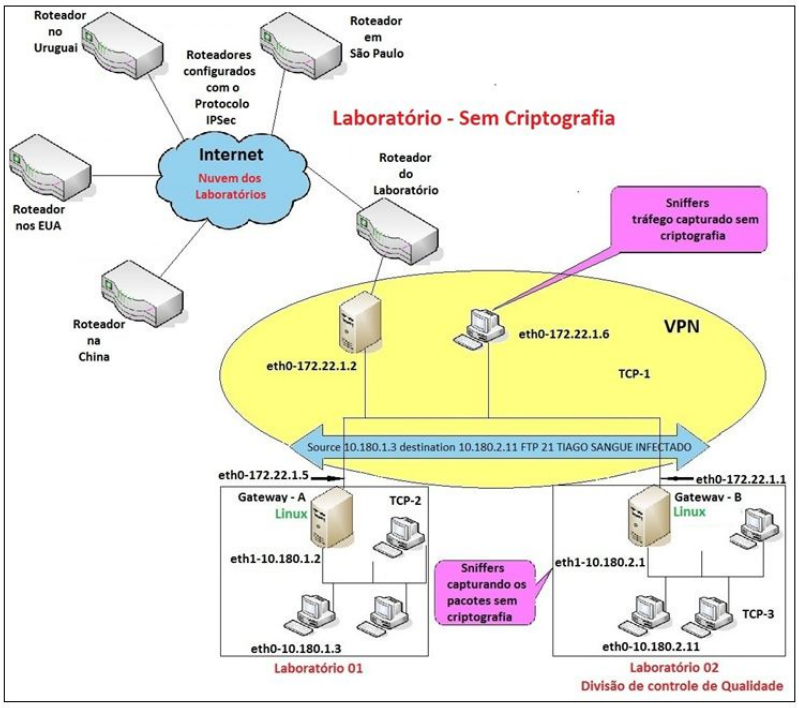

Figura 4: Laboratório – Sem Criptografia. Fonte: (SANT'ANNA, 2003)

Na figura 5, é representado um laboratório com configurações IPSec em sua rede, foi utilizado um túnel VPN formado pelos gateways A e B. A máquina (10.180.2.11) faz uma transferência de um arquivo com resultado de exame para a máquina (10.180.1.3), nota-se que o pacote que esta sendo transferido já foi criptografado pelo protocolo IPSec.

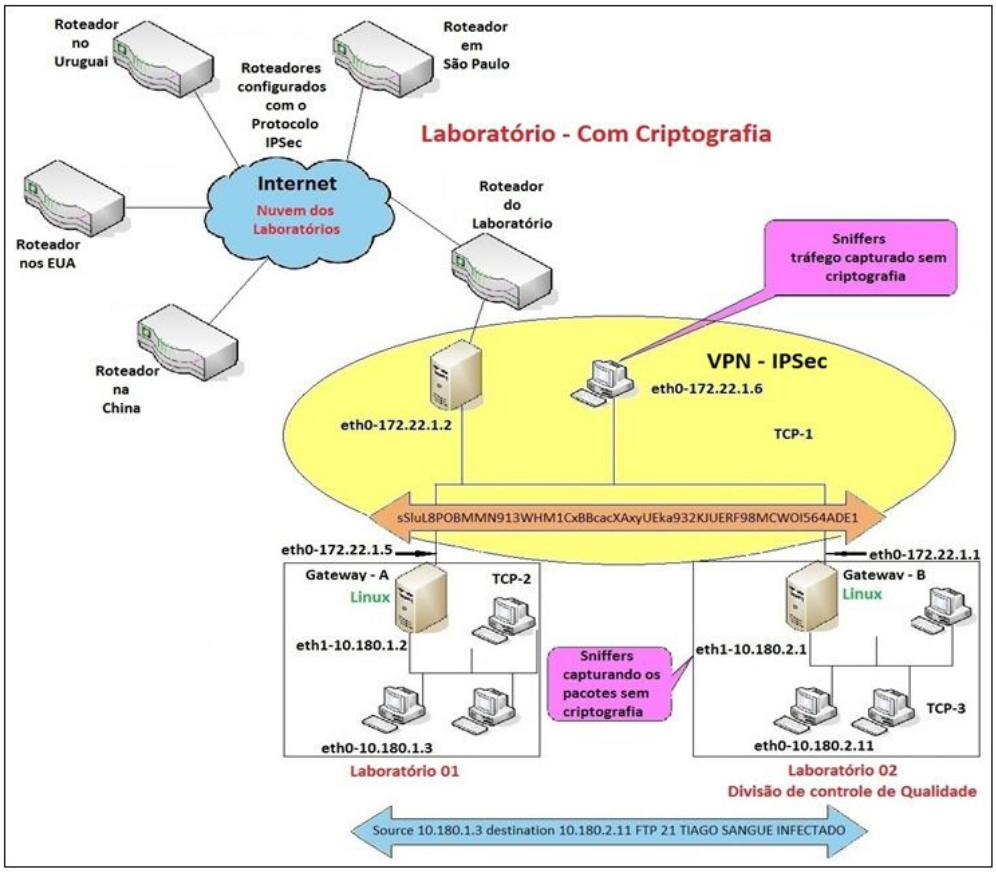

Figura 5: Laboratório – Com Criptografia. Fonte: Sant'Anna (2003).

Com a ajuda de dois Sniffers, conseguimos capturar alguns pacotes transferidos e observamos que os dados já estavam criptografados, como ilustra a figura 13. Dessa maneira as informações e os dados dos laboratórios, poderão ser transferidos de uma forma segura e confiável.

A segurança na transferência dos arquivos dos laboratórios é possível pelo fato de todos os roteadores estarem configurados com o protocolo IPSec, portanto, quando um pacote for navegar na rede interna dos laboratórios e na rede externa (rede P2P), sairão todos criptografados e navegará pela internet utilizando um túnel VPN até os outros laboratórios. (SANT'ANNA, 2003).

CONCLUSÃO

Dentro de um ambiente corporativo utilizando uma rede P2P, a segurança é o principal fator crítico de preocupação das empresas, no qual poderá apresentar riscos para as suas informações.

Analisando-se os tópicos abordados e os resultados obtidos, pode-se concluir que este artigo contribuiu para conceituar os principais aspectos de segurança utilizado na VPN, arquiteturas e o protocolo IPSec, reunido através de uma ampla pesquisa bibliográfica. Este artigo procura

oferecer uma contribuição ao tema “Segurança na Administração de Redes”, aliando dois fatores básicos: segurança e baixo custo de implementação.

O sistema operacional Linux foi utilizado, sendo uma ferramenta bastante flexível, com várias opções de configuração e de código aberto, possibilitando a inclusão de eventuais ajustes de algoritmos para maior segurança da rede. Vários distribuidores de Linux disponibilizam-no gratuitamente pela Internet, reduzindo drasticamente os gastos com licenças e custo total de propriedade.

REFERÊNCIAS

ANDREOLI, Andrey V. **IP Security (IPSec)**. Disponível em: <www.cert-rs.tche.br/docs_html/ipsec.html>. Acesso em: 16 out. 2012.

BARCELLOS, Marinho P. **Segurança em Redes P2P: Princípios, Tecnologias e Desafios**. Rio Grande do Sul: EdUFRGS, 2006.

BARBOSA, Alcenir Soares. **Análise da Qualidade de Serviço de VPN – Redes Privadas Virtuais – Utilizando Redes Sem Fio**. Uberlândia: EdUNIMINAS, 2004.

DUARTE, Otto C. M. B; LOPEZ, Norberto G. **IP Security**. Rio de Janeiro: UFRJ, 2003. Disponível em: <http://www.gta.ufrj.br/grad /03_1/ip-security/>. Acesso em: 10 set. 2012.

DUARTE, Otto C. M. B *et al.* **Redes Peer to Peer**. Rio de Janeiro: UFRJ, 2012. Disponível em: <http://www.gta.ufrj.br/grad/06_1/p2p/index.html/>. Acesso em: 10 set. 2012.

KUROSE, James. F.; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down /James**. 5. ed. São Paulo: Pearson, 2010.

LOEST, Sergio R. **Um Sistema de Backup Cooperativo Tolerante a Intrusões Baseado em Redes P2P**. Curitiba: EdPUCP, 2007.

REZENDE, Pedro A. D. de; ROTOLE, Erick D. **Arquitetura IP Security.** Disponível em: <http://www.cic.unb.br/~rezende/trabs/ipsec.pdf>. Acesso em: 10 out. 2012.

SANT’ANNA, Giovani de F. **Conectividade Virtual Segura e de Baixo Custo Sob Linux.** São Paulo: IPT, 2003. Originalmente apresentada como dissertação de mestrado, Instituto de Pesquisas Tecnológicas do Estado de São Paulo, 2003.