# Utilização da arquitetura de segurança IPSec no modo túnel para a implementação de uma rede VPN de baixo custo

**Neustlan A. de A. Junior[1], Walter C. S. Simões[2], Leonardo S. Valcácio[1], Anderson T. de Araujo[1]**

[1]Tecnologia em Redes de Computadores – Centro Universitário do Norte (UNINORTE)
Caixa Postal 227 – 69020-220, Rua Huascar Figueiredo, s/n, Manaus – AM – Brasil

[2](ICOMP), Universidade Federal do Amazonas (UFAM)
Av. General Rodrigo. Octávio, 6200, Coroado I, Manaus, AM, Brasil

***Abstract.*** *The current public networks have a certain native security of your provider, ensuring data delivery to your recipients. But in the matter of security it does not guarantee that their personal or corporative data being intercepted along the way. This paper proposes the use of a method to the problem of reliability in a public medium. The methodology is the implementation of the IPSec security architecture in use over a VPN in tunnel mode with PfSense tool. The result expected by the application of the technique is to provide encryption of data sent and a relationship of trust between points, thus providing a higher level of confidentiality in the network formed.*

***Resumo.*** *As redes públicas atuais possuem uma certa segurança nativa do seu provedor, garantindo a entrega de dados aos seus destinatários. Porém na questão de segurança ele não garante que seus dados pessoais ou coorporativos sejam interceptados no meio do caminho. Este trabalho propõe a utilização de um método para o problema de confiabilidade em um meio público de comunicação. A metodologia aplicada é a implementação da arquitetura de segurança do IPSec sendo utilizada sobre uma VPN no modo túnel com a ferramenta PfSense. O Resultado esperado pela aplicação da técnica é prover a criptografia dos dados enviados e uma relação de confiança entre pontos, proporcionando assim um nível maior de confidencialidade na rede formada.*

## 1. Introdução

O Internet Protocol Security Protocol (conhecido por sua sigla IPSec) é uma extensão do protocolo IP que visa ser o método padrão de privacidade do usuário aumentando a segurança de informações fornecidas pelo meio da internet. IPsec é uma suíte de protocolos que provê segurança no nível da camada IP para comunicações pela Internet. Opera sob a camada de rede (ou camada 3) do modelo OSI. Outros protocolos de segurança da internet como SSL e TLS operam desde a camada de transporte (camada 4) até a camada de aplicação (camada 7), segundo Frankel et al, (2011).

As pesquisas realizadas neste artigo visam apresentar um sistema de interligação Site-to-Site através da técnica VPN, neste cenário é aplicado o protocolo de segurança IPSec, onde o mesmo garante a confiabilidade dos dados trafegados no canal. Essa solução propõem a utilização de um *hardware* de baixo custo de aquisição e um nível de processamento aceitável onde pode-se também aproveitar um *desktop* já obsoleto para atividades comuns, com a configuração de 2Gb de memória ram, processador dual core, um HD com baixo armazenamento ambos trabalhando com uma arquitetura X64, assim como a ferramenta PfSense, que a mesma baseasse na distribuição do sistema operacional Unix

FreeBSD. Aliando o *hardware* e a ferramenta de PfSense busca-se um resultado final satisfatório pelo tempo empenhado e o investimento financeiro necessário.

## 2. Trabalhos Relacionados

Segundo Kurose, (2010), é valido considerar o sigilo na camada de rede entre um par de entidades da rede, (dois roteadores, dois hospedeiros ou roteador e um hospedeiro), as entidades enviam informações úteis de todos os datagramas que o remetente e a entidade destinatária. A carga enviada pode ser tanto do segmento TCP quanto do UDP ou uma mensagem ICMP. Se ambos serviços da camada de rede estiverem em funcionamento, todos os dados de uma entidade a outra estariam ocultos de qualquer terceira parte que possa estar analisando essa rede. Por esta razão a segurança na camada de rede é conhecida por prover "cobertura total", o que justifica a utilização do IPSec.

A escolha de uma ferramenta *open source* segundo José, (2013), é decorrente diretamente a fatores de recursos de investimento disponíveis pois se trata de um sistema de código aberto, além de redução de custos traz flexibilidade e praticidade para aplicar conhecimentos na plataforma, dessa forma o administrador pode configurar um *firewall* de forma muito mais segura e também respaldado em ocasiões de auditorias.

O *IP Security* fornece segurança para transmissões através de redes desprotegidas segundo Wojcik, (2014), onde proporciona confidencialidade, integridade, autenticação e proteção de *Antireplay* aos dados trafegados por meio da VPN estabelecida.

Os trabalhos relacionados descrevem a utilização do IPSec em uma conexão VPN, onde os mesmos se propõem implementar e analisar o protocolo de segurança do IPSec e verificação de suas características, assim como realizar testes de simulação do seu funcionamento verificando os requisitos básicos da tecnologia. Assim como a implementação da ferramenta de *firewall* do PfSense, onde o mesmo possibilita a formação do canal de comunicação e a aplicação da arquitetura de segurança do IPSec.

## 3. Arquitetura Proposta

A Figura 1 ilustra a arquitetura proposta neste trabalho que é composta por: dois servidores com o PfSense instalado, ambos com duas placas de rede inserido, uma para Lan e a outra para conexão com a internet (Wan) logo pois também com a VPN, dois links de internet sendo recebido pelo modem da sua devida operadora, repassando apenas um Ip válido para a porta Wan do servidor correspondente. Para devidos testes da infraestrutura, é necessário haver um computador em cada rede lan, para poder ser feita a comunicação entre as redes distintas. No PfSense é configurado o *firewall*, onde o mesmo dita as políticas da rede local e externa, e prover a conexão VPN aliado com o seu protocolo de segurança IPSec.

Cada servidor PfSense será responsável pela administração da sua rede local, aplicando bloqueios em portas/serviços que se achar necessário para um melhor desempenho na conexão local e trafego externo, ele também tem a principal função de promover o túnel VPN, que promovido pela saída da placa Wan onde o mesmo é aplicado o protocolo IPSec. A configuração de forma rígida e padronizada é necessária para minimizar os pontos de falhas na rede onde possam gerar instabilidades na conexão proposta.

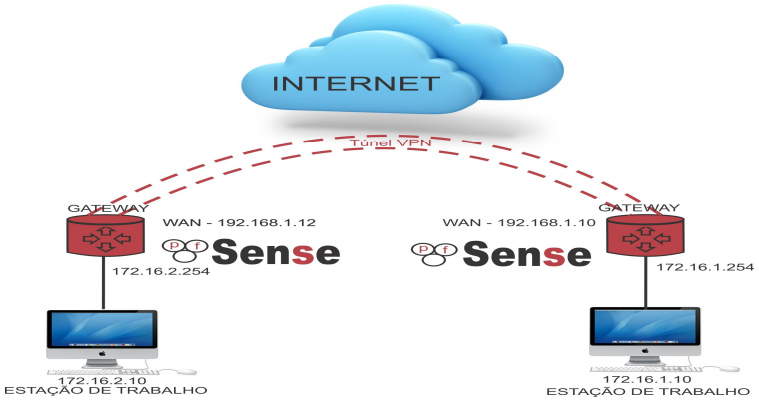


**Figura 1. Cenário geral do modelo.**

O IPSec integra um mecanismo de aplicações de segurança necessários para garantir confiabilidade no tráfego de dados, encriptação, autenticação ou a combinação de ambos, como pode-se observar na Figura 2. A encriptação ocorre entre os dois hosts quando iniciam a sua comunicação via internet, os dados que forem trafegados na rede Lan não são encriptados, isso porque o tráfego será encriptado na camada IP pelo roteador (PfSense) que se encarrega de enviar esses dados não encriptados da rede local para a internet via VPN em forma cifrada.

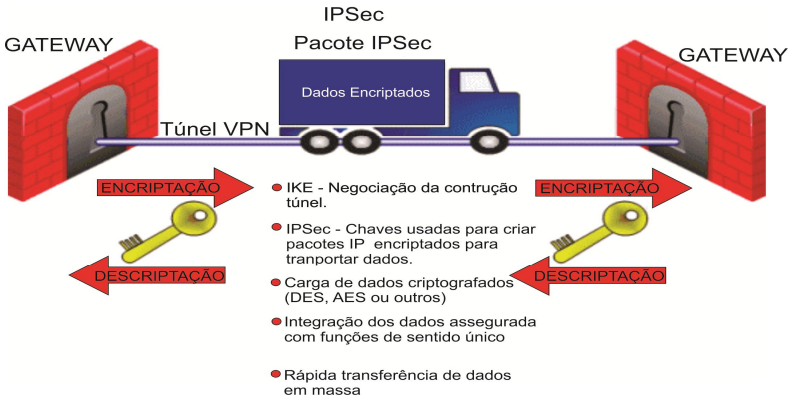


**Figura 2. Demonstração do funcionamento do IPSec.**

Na sequência apresentada Figura 2 é possível ver as definições de segurança que são aplicadas no pacote onde contém as informações que são destinadas a um gateway, desta forma a arquitetura de segurança se compromete em levar e trazer os dados em segurança encriptando e decrepitando os dados de acordo com o seu gateway de destino.

## 4. Testes e Resultados

Os testes propostos devem seguir alguns parâmetros segundo Boava, (2010), tais como habilitar interfaces, desconectar equipamentos da rede ou enviar pacotes de uma estação de teste. O propósito ao testar a conectividade entre dois pontos de uma mesma VPN é verificar a continuidade e qualidade do sinal transmitido, isso pode ser por meio de comandos do ICMP a partir do emissor tentar enviar mensagens de PING para os endereços IP de *loopback* de outros receptores na mesma VPN podendo retornar resultado positivo ou negativo, posteriormente pode ser trafegado arquivos de maior extensão, para fins de aferição de performance na rede, os dados podem ser colhidos e analisados.

Parâmetros de teste que podem ser adotados são teste de vazão, atraso, perdas de pacote e *jitter* que por meio desses pontos abordados pode-se verificar melhorias a serem

feitas, assim podendo proporcionar uma melhor entrega de sinal e performance no canal de comunicação, assim verificando se há perda ou ganho de velocidade de transmissão.

Uma ferramenta que pode ser usado para gerar trafego segundo Boava, (2010), é o iperf onde o seu fluxo pode ser configurado para o fluxo UDP com isso ter a mensura de dados reais passando pelos pontos de comunicação de um gerador ao seu receptor, conforme mostrado na Figura 3.

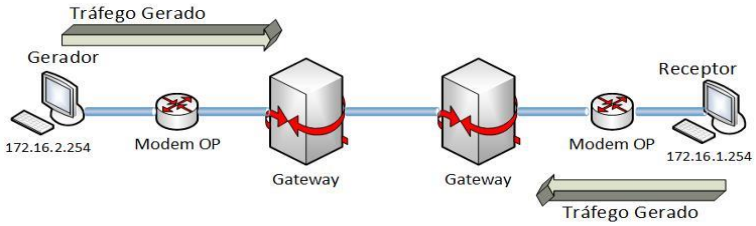


Figura 3. Demonstração da arquitetura de teste.

Como continuidade nos testes de transmissão é necessário que se faça um teste no inverso das pontas, também podemos observar na Figura 3, onde o receptor se torna gerador e o gerador se torna receptor, com isso podemos observar se haverá pontos de congestionamento na arquitetura referida, portanto podemos dizer que desta forma os testes serão realizados em ambos os sentidos.

## 5. Conclusão

Com o a expansão das redes de computadores, e divulgações de informações em nuvens pública, se torna mais evidente a necessidade de se proteger os dados de uma corporação, assim como a interligação de uma a outra em tempo real, pois o mercado competitivo requer informações rápidas e prontas de imediato, a proposta visou mostrar a interligação de dois pontos de forma mais sucinta e segura, visando os baixos custos de investimentos e a integridade de dados ao trafegar pelo meio proposto.

Como continuidade do trabalho será desenvolvido um manual de auxílio a implementação da solução proposta, podendo assim ser de mais fácil entendimento e de rápida aplicação em um ambiente real e de produção, podendo contribuir diretamente com profissionais da área que passam por problemas semelhantes.

## 6. Referências

WOJCIK, Eduardo. Análise e Simulação de VPN com IPSec em Roteadores Cisco. Curitiba, 2014

LEANDRO, Jefferson Ferreira. Estudo de Caso de Soluções em VPN IPSec com Servidores Usando Software Livre. Curitiba, 2013

JOSÉ, Fernando Simplicio. Implementação de Firewall de Alta Disponibilidade Através do PfSense. Passo Fundo, 2013

FRANKEL, S. N. KRISHNAN, S. E. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. M aryland, 2011

BOAVA, ADÃO. Avaliação da Qualidade de Serviço das VPN IP MPLS Para Redes de Nova Geração (NGN). Campinas, 2010

INC, Cisco System. IPsec VPN WAN Design Overview. San Jose, 2006.

TANENBAUM, Andrew S. Redes de Computadores. Rio de Janeiro, 2003.

KUROSE, James G. Redes de Computadores e a Internet: uma abordagem top-down. São Paulo, 2010.