8º Encontro de Atividades Científicas
de 26 a 28 de Outubro
Londrina - Paraná
UNOPAR

IMPLEMENTAÇÃO DE VPN EM LINUX UTILIZANDO O PROTOCOLO IPSEC

Autores

FABIO SHINOHARA — *Aluno Pós-Graduação Outra Instituição*

RONI FRANCIS SHIGUETA — *Docente Outra Instituição*

Introdução

Uma VPN corresponde a uma rede privada virtual que permite a interligação entre empresas através de uma rede pública como a Internet. Para isso, deve-se levar em consideração as questões de segurança do tráfego que está passando na rede pública. A solução para isso é criptografar essas informações de modo que, mesmo que as informações sejam interceptadas, elas não possam ser interpretadas. O IPSEC permite realizar a criptografia das informações do tráfego proveniente de uma rede local. Este tráfego será criptografado e enviado a rede pública. Outros protocolos como PPTP permitiriam somente a criptografia ponto a ponto, ou seja entre duas máquinas e são mais utilizadas em situações de mobilidade.

Objetivo

Este trabalho tem por objetivo implementar uma rede VPN em ambiente linux utilizando o protocolo IPSEC.

Metodologia

Como metodologia, implantou-se um protótipo de redes simulando a Internet e em cada extremidade foi colocada uma máquina com a função de gateway (utilizando o sistema operacional linux) para a Internet. A função de cada um dos gateways é estabelecer um túnel VPN responsável pelo transporte dos dados criptografados. Após a implantação do túnel, foram realizados vários testes de conexão e transporte de dados entre as duas redes. Foi utilizado um software sniffer para realizar a captura de pacotes para posterior análise.

Resultado

Para obter os resultados, inicialmente realizou-se a comunicação entre as duas redes com um conexão convencional utilizando roteamento. O sniffer instalado na rede pública, capturou os dados e permitiu observar que as informações no campo de dados estavam completamente legíveis, em texto puro. Num segundo momento, estabeleceu-se o túnel VPN e verificou-se que no campo de dados do pacote, as informações entre as duas redes estavam realmente criptografadas, tornando díficil a interpretação das informações por pessoas não autorizadas. Para a criptografia das informações, foi utilizado uma chave RSA de 128 bits.

Conclusão

Após a realização deste trabalho, pode-se concluir que as informações transportadas através de um túnel VPN (IPSec) tem o seu nível de segurança aumentado devido a criptografia aplicada aos dados, sendo que ela uma solução alternativa e altamente personalizável quando comparada a soluções proprietárias.

Bibliografia

ORTIZ, E. VPN: Implementando soluções em Linux. São Paulo: Érica, 2003.

TANENBAUM, A. Redes de Computadores. Rio de Janeiro: Campus, 1997.

SANTOS, L. Como funciona a VPN. http://www.clubedasredes.eti.br.[online]

http://www.freeswan.org.[online]