Obtendo Segurança em uma Rede a partir da Utilização de *Intrusion Prevention System*

Gustavo Sandini Linden, Marco Antônio Trentin

Curso de Ciência da Computação **-** Universidade de Passo Fundo - Campus I
Bairro São José - Fone (54) 316 8354 Fax (54) 316 8364
Cx. P. 611 - 99001-970 - Passo Fundo-RS

40579@inf.upf.tche.br, trentin@upf.tche.br

RESUMO. *Este trabalho tem por objetivo realizar um estudo sobre algumas soluções em segurança de redes de computadores, culminando no Intrusion Prevention System (IPS). Esse sistema possui as mesmas características de um Intrusion Detection System (IDS), porém seu maior diferencial é que ele trabalha de modo ativo na rede, ou seja, ele não fica apenas coletando tráfego, mas interagindo com a rede. A proposta desses sistemas de prevenção de intrusão surgiu recentemente devido à habilidade de coletar e analisar tráfego TCP/IP em tempo real, a fim de, sempre que necessário, executar medidas pró-ativas ou, pelo menos, reativas.*

Palavras-chave: *segurança, intrusão, IDS, IPS*.

ABSTRACT. *This work has for aim to carry through a study on some solutions in security of computer networks, with its final results in the Intrusion Prevention System (IPS). This system has the same characteristics of a Intrusion Detection System (IDS), however the biggest difference between them is that it works in active way in the net, or either, does not only collect traffic, but it interacts with the net. The proposal of these systems of prevention of intrusion recently appeared due to ability to collect and to analyze traffic TCP/IP in real time, so that, whenever it's necessary, it performs pro-active or, at least, reactive actions.*

Keywords: *security, intrusion, IDS, IPS*.