

HOWTO: Proteger rede wifi com IPsec

Manuel Pata
<pata@alface.de>

23 de Julho de 2006, 6a OpenBSD-PT Meeting, Portugal

- Pequena introdução ao IPsec

- 3 Protocolos:

 - ESP(encapsulation)

 - AH(authentication header)

 - IPComp(compression)

- ESP:

 - Autenticação, Integridade, Replay, Confidencial

- AH:

 - Autenticação, Integridade, Replay

- SAs (Security Associations)

Contém todas as informações relativas à ligação, algoritmo de encriptação, chave de autenticação, chave de encriptação, entre outros.

Ambas as partes têm que ter SAs iguais. (ipsecctl, isakmpd)

□ Modos de operação (tunnel/transport)

○ tunnel: todos os pacotes são entregues ao gateway

○ transport: os pacotes são entregues ao endereço contido no IP header

○ (roubado da man page)

○ sem ipsec:

▷ [IP header] [TCP header] [data...]

○ esp em modo transport:

▷ [IP header] [ESP header] [TCP header] [data...]

○ esp em modo tunnel:

▷ [IP header] [ESP header] [IP header] [TCP header] [data...]

○ Tudo o que vem depois do ESP header está protegido.

□ ipsecctl

- Ferramenta que veio substituir ipsecadm(8) e simplificar a utilização de isakmpd(8)
- Configuração semelhante ao pf

□ Substituir WEP com IPsec

- 1. Gerar certificate authority
- 2. Gerar certificados para cada utilizador
- 3. Uma linha de configuração para ipsecctl

□ Bibliografia

- man 4 ipsec
- man 8 ipsecctl
- man 5 isakmpd.conf
- man 5 ipsec.conf
- Zero to IPSec in 4 minutes <<http://www.securityfocus.com/infocus/1859>