Utilizando o IPSec para garantir segurança a transmissões multimídia em redes IPv4

Eduardo Souza Machado da Silva
esms@acm.org
Joni da Silva Fraga
Jean-Marie Farines
{fraga,farines}@lcmi.ufsc.br

22 de maio de 2001

Resumo

Este roteiro descreve as etapas da contrução de um canal seguro de comunicação entre redes ligadas a Internet utilizando a proposta IP Security [KA98c]. O objetivo é avaliar o custo introduzido pela utilização dos mecanismos criptográficos propostos pela IETF e sua influência no tráfego multimídia seguro.

Trabalho Proposto

- Escolha de plataforma IPSec
- Configuração da VPN
- Escolha das ferramentas para mensuração
- Obtenção dos dados (taxa de transferência, atraso)
- Comparação dos mecanismos utilizados para segurança do tráfego multimídia
- Análise qualitativa e quantitativa dos resultados

IPSec (IP Security)

- *Security Architecture for the Internet Protocol* [KA98c]
- RFC 2401 – RFC 2412
- Confidencialidade, Integridade, Autenticação da origem dos dados e Rejeição de datagramas antigos (anti-*replay*)
- 3 elementos principais:
  - AH (*Authetication Header*) [KA98a]
  - ESP (*Encapulating Security Payload*) [KA98b]
  - IKE (*Internet Key Exchange*) [HC98]
- Encapsulating Security Protocol (ESP) em modo túnel

- Blowfish (DES) e HMAC-SHA1
- Troca de chaves manual

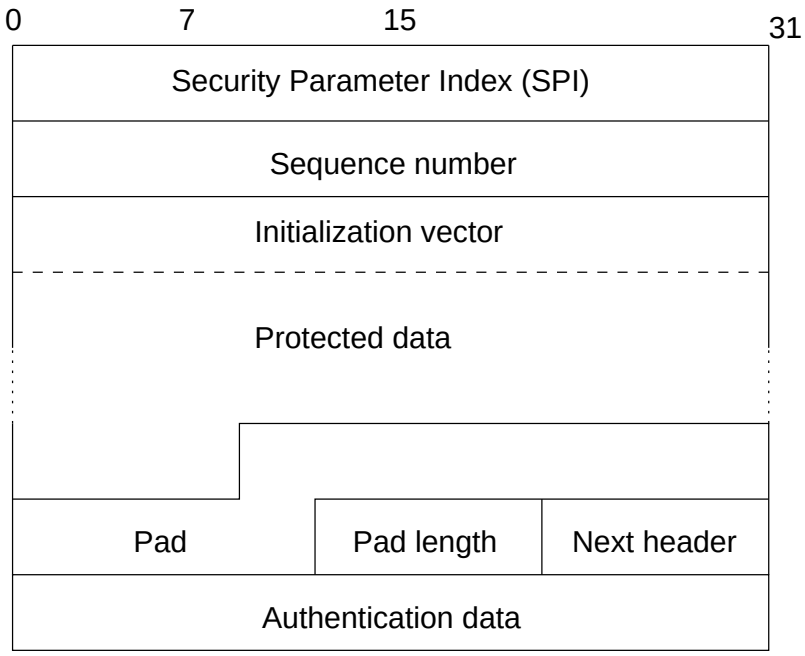

Figura 1: Cabeçalho ESP

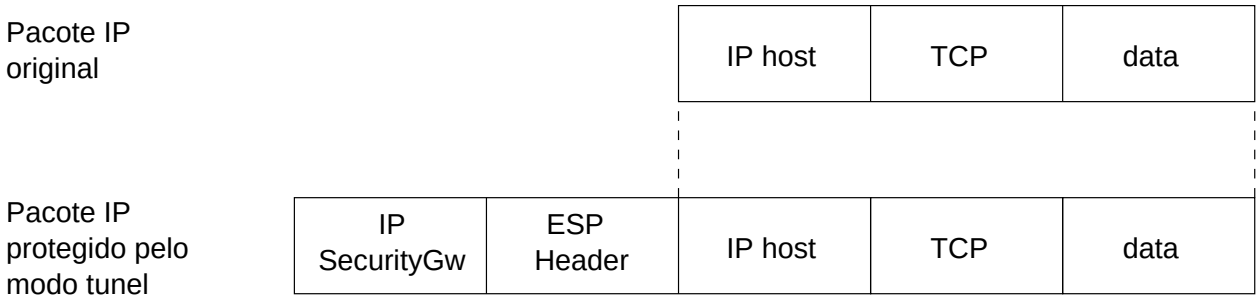

Figura 2: ESP modo túnel

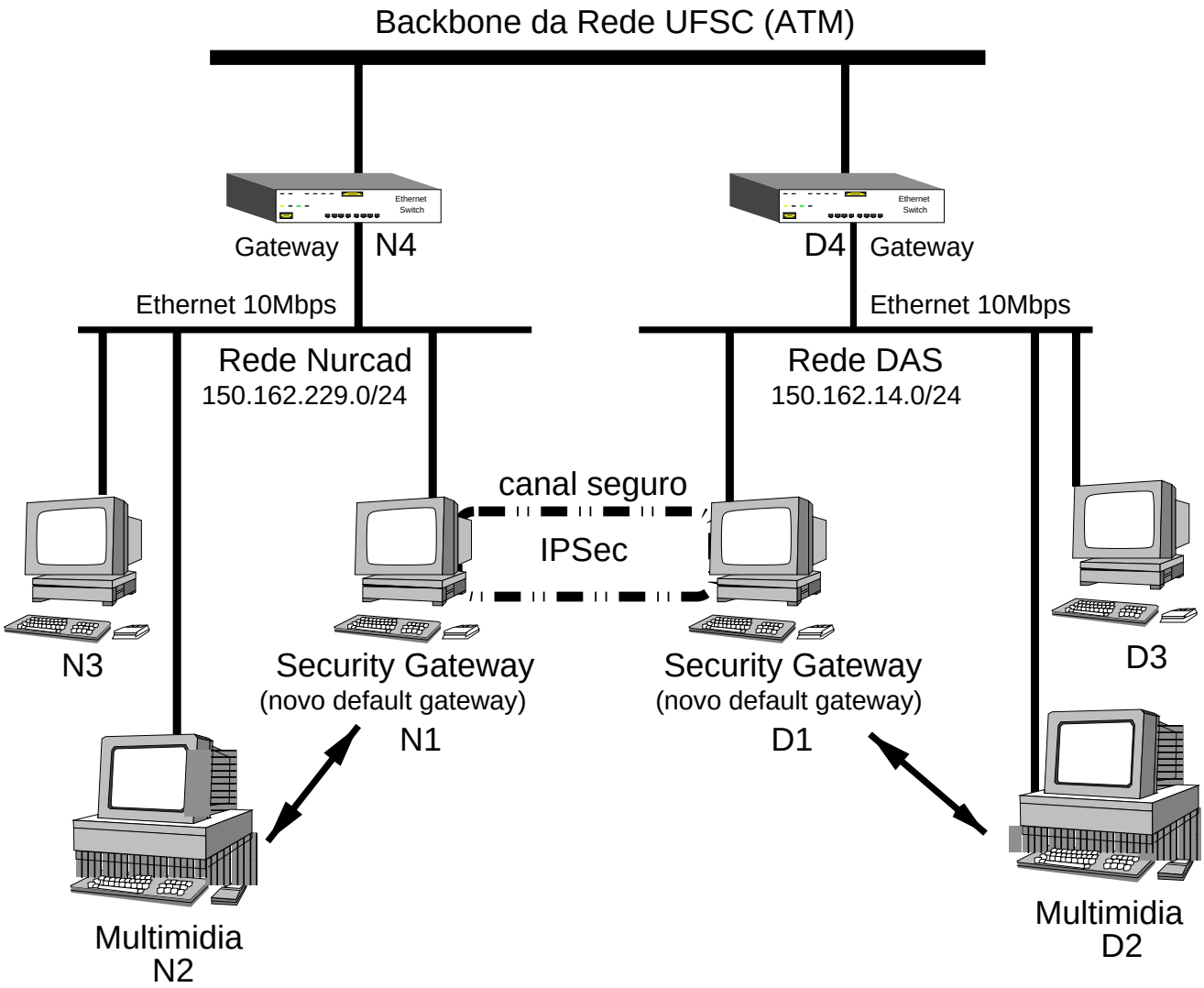

Figura 3: VPN Nurcad e DAS

- Equipamentos envolvidos (*security gateways*)
- Roteadores intermediários
- Pentium 100 MHz 96 MB 3C900 10 Mbps (DAS)
- Pentium 166 MHz 32 MB 3C905 10/100 Mbps (Nurcad)

Mensuração

- `pchar` (derivado do `pathchar` de Van Jacobson)
- *Throughput* e RTT através de pacotes UDP com tamanho variável
- Foram montados 3 cenários:
  - "IP" (sem mecanismo de segurança)
  - "IP-IP" (IP encapsulado em IP, túnel sem segurança)
  - "ESP" (ESP em modo túnel)

Resultados Obtidos

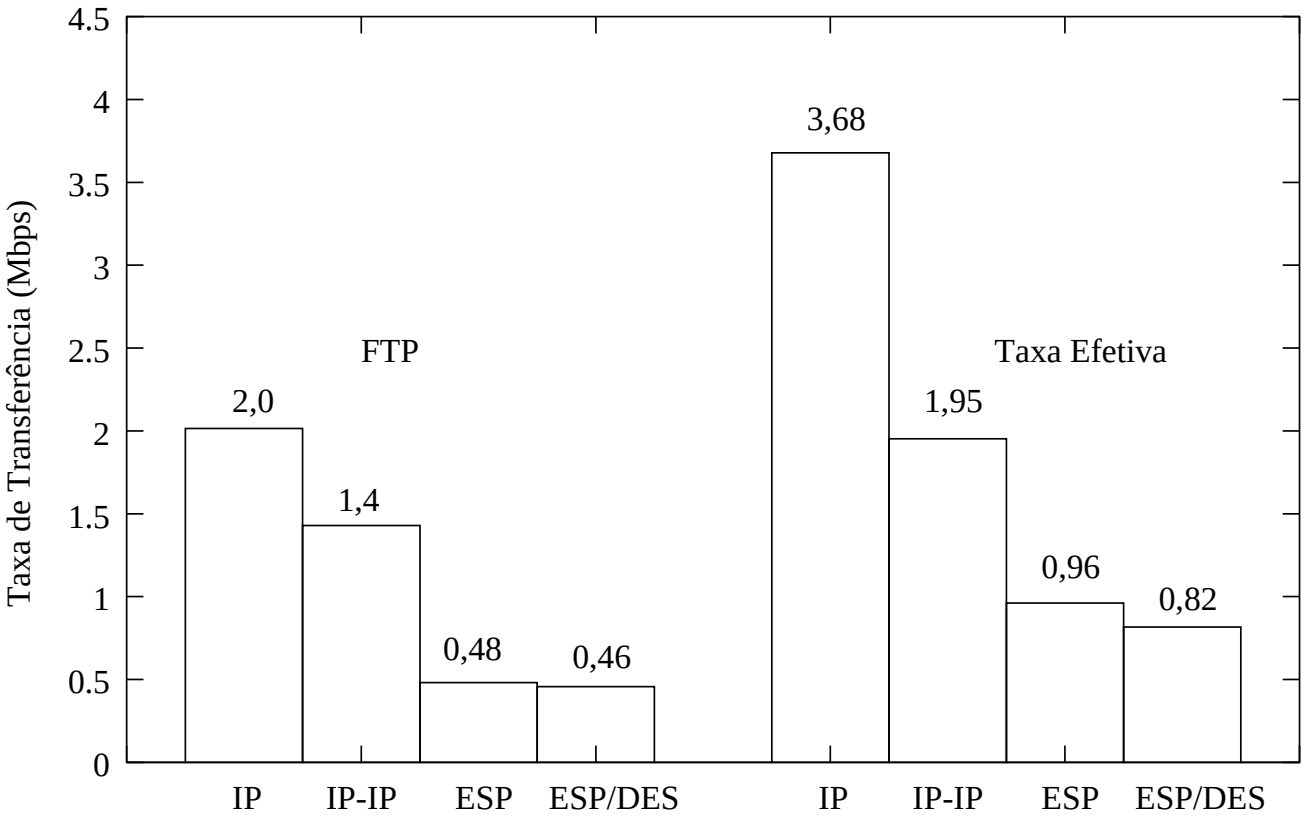

Figura 4: Taxa de transferência de bits nos 3 cenários

- Tunelamento sem IPSec (IP-IP): 50%
- Tunelamento com IPSec (ESP): 75%
- Influência das CPUs dos *Security Gateways*
- Algoritmos

Perspectivas

Bibliografia

Request For Comment (RFC)

`http://www.rfc-editor.org`

Referências

[HC98] Dan Harkins and Dave Carrel. The Internet Key Exchange (IKE). Request For Comments (Proposed Standard) RFC 2409, Internet Engineering Task Force, November 1998.

[KA98a] Stephen Kent and Randall Atkinson. IP Authentication Header. Request For Comments (Proposed Standard) RFC 2402, Internet Engineering Task Force, November 1998.

[KA98b] Stephen Kent and Randall Atkinson. IP Encapsulating Security Payload (ESP). Request For Comments (Proposed Standard) RFC 2406, Internet Engineering Task Force, November 1998.

[KA98c] Stephen Kent and Randall Atkinson. Security Architecture for the Internet Protocol. Request For Comments (Proposed Standard) RFC 2401, Internet Engineering Task Force, Nov 1998.