Proposta de Uso Dinâmico do IPSec no IPv6

Aritana Pinheiro Falconi
Instituto de Estudos Avançados - IEAv/CTA
falconi@lac.inpe.br

Ulisses Thadeu Vieira Guedes
Laboratório de Computação e Matemática Aplicada – LAC/INPE
ulisses@dem.inpe.br

Resumo

Este artigo tem como objetivo propor uma de nova abordagem no uso da plataforma de segurança IP Security – IPSec – sobre o Internet Protocol Version 6 – IPv6 – no intuito de aumentar o desempenho da comunicação entre máquinas interligadas por uma rede de computadores. O uso do IPSec interfere enormemente no desempenho da comunicação de dados. Propõe-se habilitá-lo quando estritamente necessário, sem criar um túnel criptógrafico durante toda a seção. No caso do serviço de POP3, por exemplo, o IPSec seria usado apenas durante a transferência de senha de um usuário do serviço, desabilitando-o durante a transferência dos dados da aplicação.

1. Introdução

IPv6 é a abreviação de *Internet Protocol Version* 6, a próxima geração do protocolo de rede projetado pela *Internet Engineering Task Force* – IETF para substituir a versão atual do *Internet Protocol*, IP Versão 4 ou IPv4. [2]

O IPv6 fixa alguns dos problemas do IPv4, tal como o número limitado de endereços IP, além de também adicionar muitas características ao seu antecessor. Como curiosidade, a capacidade total de endereçamento do novo protocolo é de 340.282.366.920.938.463.374.607.431.768. 211.456 endereços, o que dá 665.570.793.348.866.943. 898.599 endereços por m^2 do planeta Terra. No entanto, tendo em conta as políticas de atribuição de endereços que possam vigorar, a visão mais pessimista prevê que venham a existir "apenas" 1564 endereços por m^2.

Outra questão que o IPv6 tenta resolver é da falta de segurança, em vista de que originalmente, o IP não tinha nenhum intuito de prover segurança. A Internet se restringia aos meios científicos e acadêmicos, os problemas de segurança não eram tão críticos porque havia um certo controle baseado em códigos de uso ético da rede. Mas, com a abertura da Internet para o setor privado, principalmente comercial, os problemas de segurança se intensificaram e ficaram críticos.

Em resposta aos desafios de segurança, o grupo de trabalho *IP Security Protocol* da IETF, desenvolveu a plataforma *IP Security* – IPSec [4]. Esta plataforma foi desenvolvida para prover serviços de segurança de alta qualidade, baseados em criptografia, para o protocolo da camada de rede IP e/ou para as camadas superiores da pilha de protocolos TCP/IP. O conjunto de serviços oferecidos inclui controle de acesso, integridade não orientada à conexão, autenticação da origem dos dados e confidencialidade.

Esses serviços são implementados através da utilização conjunta de protocolos de segurança de tráfego de dados, o cabeçalho de autenticação (AH - *Authentication Header*) [5], o cabeçalho de encapsulamento seguro do conteúdo dos dados (ESP - *Encapsulating Security Payload*) [7] e de procedimentos e protocolos de gerência de chaves criptográfica, também conhecido como IKE [3].

O cabeçalho de autenticação assegura ao destinatário que os dados são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações. A segurança do encapsulamento IP garante a confidencialidade dos dados encapsulados no pacote IP. O protocolo de gerência de chaves torna possível a troca de chaves criptográficas de forma segura.

Por questões de garantia de interoperabilidade, as definições dos protocolos AH e ESP estabelecem que todas as implementações devem suportar alguns algoritmos pré-definidos. Para autenticação de cabeçalho, os algoritmos obrigatórios são os seguintes:

- HMAC-MD5, (RFC2403, 1998)
- HMAC-SHA-1, (RFC2404, 1998);

e para o encapsulamento seguro do *payload*, além destes dois já citados acima, os outros algoritmos são:

- *DES-CBC (RFC2405, 1998)*
- *Null Encryption Algorithm*. (RFC2410, 1998)

As especificações IPSec também suportam negociação de compressão IP definidas pela (RFC2393, 1998) - *IP Payload Compression Protocol.*

Os algoritmos de autenticação e criptografia citados acima utilizam o conceito de associação de segurança entre o transmissor e o receptor. Assim, o transmissor e o receptor devem concordar com uma chave secreta, segredo este garantido pelo protocolo IKE e com outros parâmetros relacionados à segurança, conhecidos apenas pelos membros da associação.

2. Proposta

Atualmente, várias aplicações já foram reconfiguradas para funcionarem com IPv6, incorporando os novos tipos de endereços de 128 bits e demais formatos característicos ao cabeçalho IPv6. No entanto, nem todas as novidades estão sendo aproveitadas. Por exemplo, os AH e ESP têm sido pouco explorados, sendo utilizados apenas em estudos e aplicativos, como o Security Shell (SSH), que cria túneis de comunicação.

Segundo Ariga [1], o uso dos cabeçalhos AH e ESP em uma comunicação pode diminuir a taxa de transmissão em até 90%, se comparado à uma comunicação sem o uso do IPSec. Tal perda de desempenho é bastante significativa devendo utilizá-los somente em aplicações onde os procedimentos de segurança são estritamente necessários.

A figura abaixo mostra o desempenho do IPv6 utilizando IPSec para pacotes TCP em uma *rede fast ethernet* com desempenho nominal de 100 Mbits/seg. O tamanho MTU é de 4096 *bytes* e os tamanhos do *buffer* do *socket* é de 57.344 *bytes* para TCP_STREAM.1 e 32.768 *bytes* para e TCP_STREAM.2

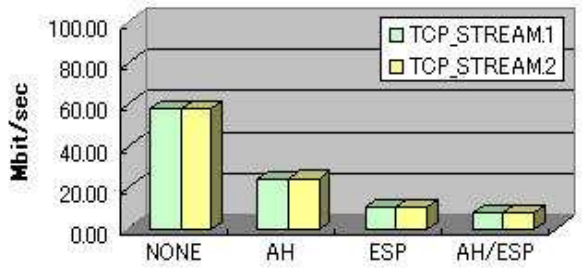

Figura 1. Comparativo de desempenho do IPSec [1]

Pretende-se sugerir o "bom uso" dos cabeçalhos de autenticação e de encriptação do IPSec. Estes itens não têm sido muito utilizados porque interferem enormemente no desempenho da comunicação de dados, como visto anteriormente. Assim, espera-se usar a autenticação e encriptação dos dados somente durante a transmissão de dados sigilosos procurando aumentar o desempenho de toda a comunicação.

Hoje, o IPSec é utilizado para criação de VPN (*Virtual Private Network*). Neste sentido, são criados túneis de criptografia entre dois *gateways* capazes de assegurar a segurança de todos os dados transmitidos de forma transparente às máquinas de cada rede. Entende-se por *gateway*, uma máquina por onde passa todo o tráfego da rede.

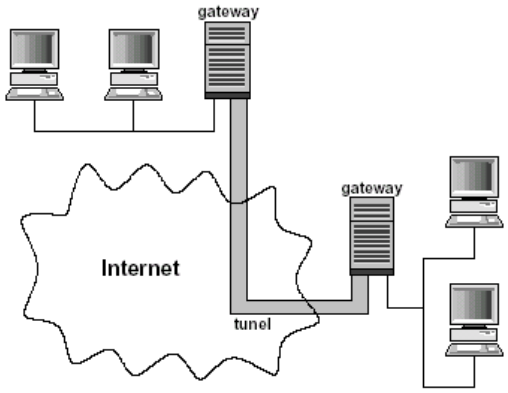

Figura 2. Modelo de uma VPN

A figura 2, mostra uma arquitetura básica de uma VPN bastante utilizada. O problema, neste contexto, é que não existe uma seleção do que precisa ser protegido pelo túnel, assim como não existe uma classificação do tipo de aplicação que está utilizando tal recurso. Todos são tratados igualmente no túnel de criptografia.

Se considerarmos que os dados que estarão trafegando são confidencias, é necessário que toda a comunicação se faça em sigilo, ou seja, criptografada. No entanto, se os dados não são considerados sigilosos, não há motivo para que se perca tempo em tarefas dispendiosas de encriptação e desencriptação desnecessárias. O ideal, neste caso, é fazer a comunicação de forma segura apenas no momento da autenticação do usuário da aplicação, sem maiores formalidades nas outras etapas do processo de transferência dos demais dados.

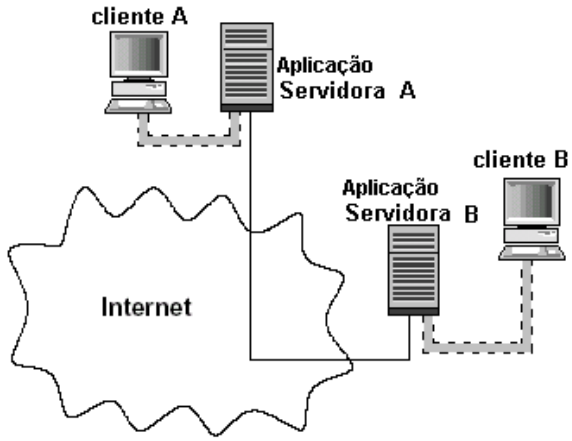

Figura 3. Exemplo de aplicação do modelo proposto.

Em nossa abordagem, ilustrada logo acima na figura 3, deixariam de existir túneis estáticos entre dois *gateways*

sem a interferência das aplicações. Cada aplicação deve escolher se fará e quando fará uso do IPSec. Seria interessante, em termos de desempenho, habilitar toda a segurança provida pelo IPSec durante a autenticação do usuário de uma aplicação servidora e depois desabilitá-la.

A figura 3 mostra a aplicação do método proposto em uma comunicação entre aplicações clientes e servidoras de e-*mail* (POP3, por exemplo). O túnel, mostrado com o contorno cerrilhado, tenta ilustrar que a conecção não foi criptografada durante toda a seção, apenas durante a transferência de senha do usuário da aplicação servidora de *e-mail*. Veja abaixo a figura 4 :

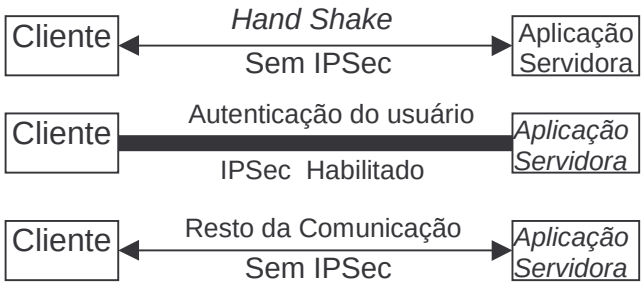

Figura 4. Diagrama da comunicação segura proposta.

A segurança provida pelo IPSec é baseada na seguraça entre máquinas. A segurança proposta neste trabalho permite que cada aplicativo tenha diretamente acesso às configurações do IPSec através de funções ou bibliotecas. Pretende-se ter o controle total sobre a política de segurança e quando ela deve ou não ser ativada. Esta é a visão que se quer enfocar, a flexibilização do uso do IPSec e seu acesso através das aplicações.

4. Conclusão

O trabalho proposto é facilmente justificado pelos resultados de desempenho no uso do IPSec, obtidos por outros trabalhos e exibidos na seção anterior. O embasamento teórico, necessário para a realização do trabalho, propicia um conhecimento profundo sobre o funcionamento do IPSec, das VPN´s e da tecnologia iminente do IPv6. Isso também é um fator motivante para o trabalho, secundário ao objetivo principal.

Com a utilização do método de uso dinâmico da autenticação e encriptação no cabeçalho IP, pretende-se obter um ganho considerável quanto ao tempo gasto em toda a comunicação se considerássemos uma comunicação totalmente encriptada.

Tal técnica será testada em alguma aplicação que não necessariamente precise de confidencialidade total de suas informações. Dentre as aplicações que se enquadram nesta característica, podemos citar as que implementam os serviços de POP, SMTP, FTP.

Após a implementação, um teste comparativo entre as técnicas de comunicação atuais irá dizer se houve real ganho na utilização da técnica proposta.

5. Referências Bibliográficas

[1] Ariga, Seiji; Nagahashi, Kengo; Minami, Masaki; Esaki, Hiroshi and Murai, Jun. Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks. In Proceedings of the 10th Annual INET Conference, Yokohama, Japan, Julho 2000.

[2] Deering, S.; Hinden, R. Internet Protocol, Version 6 (IPv6) Specification. Request For Comments (Informational) RFC 2460, Internet Engineering Task Force. Dezembro 1998.

[3] Harkins D.; Carrel D. The Internet Key Exchange (IKE). Request For Comments (Informational) RFC 2409, Internet Engineering Task Force. Novembro 1998.

[4] Kent, S.; Atkinson, R. Security Architecture for the Internet Protocol. Request For Comments (Informational) RFC 2401, BBN Corp, @Home Network, Novembro 1998.

[5] Kent, S.; Atkinson, R. IP Authentication Header. Request For Comments (Informational) RFC 2402, BBN Corp, @Home Network, Novembro 1998.

[6] Kent, S.; Atkinson, R. Security Architecture for the Internet Protocol. Request For Comments (Informational) RFC 2404, Internet Engineering Task Force. Novembro 1998.

[7] Kent, S.; Atkinson, R. IP Encapsulating Security Payload (ESP). Request For Comments (Informational) RFC 2406, BBN Corp, @Home Network, Novembro 1998.

[8] Kent, S.; Atkinson, R. The NULL Encryption Algorithm and Its Use With IPsec. Request For Comments (Informational) RFC 2410, BBN Corp, @Home Network, Novembro 1998.

[9] Madson, C.; Glenn, R. The Use of HMAC-MD5-96 within ESP and AH. Request For Comments (Informational) RFC 2403, Internet Engineering Task Force, Novembro 1998.

[10] Madson, C.; Doraswamy, N. The ESP DES-CBC Cipher Algorithm With Explicit IV. Request For Comments (Informational) RFC 2405, Internet Engineering Task Force, Novembro 1998.

[11] Shacham, A.; Monsour, R.; Pereira, R.; Thomas, M. IP Payload Compression Protocol (IPComp). Request For Comments (Informational) RFC 3173, Internet Engineering Task Force. Setembro 2001.