

Análise da Utilização do IPSec como Garantia de Segurança na Comunicação em Redes TCP/IP

Luis Godinho Junior¹, Madianita Bogo¹

¹ Sistemas de Informação - Centro Universitário Luterano de Palmas (CEULP/ULBRA)

Palmas – TO – Brazil

{luisg,mbogo}@ulbra-to.br

Abstract. *Currently, the information passage through of computer network, mainly for InterNet, it's inevitable and grows exponentially. The packages routing is made by the IP (Internet Protocol), currently in the version 4, that's not secure. A IP new version, version 6, is being tested has some time. Parallel to IPv6 development, was created a protocol of security named IPSec, to be used by the IPv6. However, the networks changes for IPv6 are being gradual, therefore the IPSec was adapted to supply the support to the current version. Because the security guarantee in the data passing in the networks is very important, this work presents a theoretical study about the IPSec and some concepts about network security, results of practical tests and description of the necessary actions for IPSec configuration in the Windows.*

Resumo. *Atualmente, a troca de informações via rede de computadores, principalmente pela Internet, cresce de forma exponencial. O roteamento dos pacotes é realizado pelo protocolo IP, atualmente versão 4, que não fornece segurança. Uma nova versão do IP, versão 6, está sendo testada há algum tempo. Paralelamente ao desenvolvimento do IPv6, foi criado o protocolo de segurança chamado IPSec, para ser utilizado pelo mesmo. Porém, como a alteração das redes para a nova versão do IP está sendo gradativa, o IPSec foi adaptado para dar suporte à versão atual. Devido a importância da garantia da segurança no tráfego dos dados pelas redes, esse trabalho apresenta um levantamento teórico sobre o IPSec e alguns conceitos de segurança de redes, além resultados de testes práticos para verificar a vulnerabilidade de redes não protegidas e a segurança oferecida pelo IPSec, sobre o Windows 2000.*

1. Introdução

Atualmente, a troca de informações via rede de computadores é inevitável, seja para o envio de uma simples mensagem de *e-mail* ou execução de outras aplicações mais específicas, como compras pela Internet. Assim, em muitos casos trafegam dados extremamente sigilosos. A maioria da comunicação em rede utiliza o conjunto de protocolos TCP/IP, pelo fato deste ser o padrão da *Internet*. Um dos principais

protocolos desse conjunto, responsável pelo roteamento de dados, é o IP (*Internet Protocol*), que atualmente está na versão 4.

Como o acesso a Internet se popularizou rapidamente a IETF (*Internet Engineering Task Force*) começou a se preocupar com a escassez do espaçamento de endereçamento IPv4 e criou, em 1996, um grupo de desenvolvimento para a criação de um novo protocolo, o IP versão 6 (IPv6). O IPv6 mantém as principais características que fizeram do IPv4 um sucesso mundial, porém, além do espaço de endereçamento maior apresenta várias melhorias, como prover segurança.

Assim, paralelamente ao desenvolvimento do IPv6, a IETF iniciou o desenvolvimento do IPSec (*IP Security Protocol*) para acrescentar segurança na camada de rede, com baixo custo financeiro e operacional, que é mandatário no novo protocolo. Como a implementação do IPv6 demorou a ser finalizada e a migração está acontecendo de forma gradativa e lenta, o IPSec passou a ser desenvolvido de forma a oferecer suporte também ao IPv4.

O objetivo desse trabalho é apresentar os resultados de estudos e de testes práticos, sobre a plataforma Windows 2000, para verificar a vulnerabilidade de redes não protegidas e a segurança oferecida pelo IPSec (*IP Security Protocol*) com o IPv4, que é o protocolo usado atualmente na grande maioria das redes. Vale ressaltar que, esses estudos servirão de base para a realização de garantia de segurança em redes IPv6, já que o funcionamento do IPSec é praticamente o mesmo nas duas versões.

2. Considerações sobre Segurança de Redes

Numa rede sem proteção os dados podem ser facilmente capturados, durante o tráfego. Por exemplo, contas e senhas podem ser descobertas com a utilização de programas destinados à captura de dados que transitam na rede, os *sniffers*. Além disso, os acessos não autorizados (ataques) a computadores se tornaram freqüentes nos últimos anos, como (Braghetto, 2003):

- *Spoofing*: técnica para personificar endereço IP, (troca do IP original por outro), podendo assim se passar por um outro host, e dificultar auditoria em caso de suspeita de invasão;
- DOS-DDOS: negação de serviço, sobrecarga no servidor ou “alvo”, através de inúmeras requisições de serviço disponibilizado pelo servidor atacado. Nesse caso, o *host* atacado é forçado a parar o serviço que disponibiliza.

Para resolver esses problemas é necessário utilizar meios que garanta a segurança na comunicação, ou seja, garantir que as informações sejam acessadas, copiadas ou modificadas apenas por pessoas que possuem autorização para realizar essas ações. Os problemas clássicos podem ser evitados por mecanismos que forneçam serviços como:

- Autenticidade: confirma a identidade da outra parte (entidade) envolvida na comunicação, garantindo se é o não quem alega ser.
- Confidencialidade/Privacidade: restringe ao remetente e ao destinatário o entendimento da mensagem, pois somente estes podem decifrá-la.

- Não-repúdio: impede que uma entidade envolvida em uma comunicação negue a sua participação no evento.
- Integridade: garantir que a informação não sofreu alterações durante seu percurso na rede.

Para que estes serviços possam ser garantidos é necessário que as informações sejam codificadas (cifradas) e/ou resumidas digitalmente (*Hash*), garantindo a confidencialidade e a integridade, respectivamente [Brocardo, 2001].

3. Sistemas de Criptografia

Ao enviar uma mensagem pela rede o remetente precisa ter a garantia de que apenas o destinatário consiga ler a mesma e, para este, é interessante ter a certeza de que o remetente é realmente quem gerou aquela mensagem. Para conseguir isso, podem ser utilizados sistemas de criptografia.

A finalidade de um sistema de criptografia é codificar uma mensagem através de um método de cifragem, ou encriptação. A figura 1 apresenta o modelo básico de um sistema de criptografia.

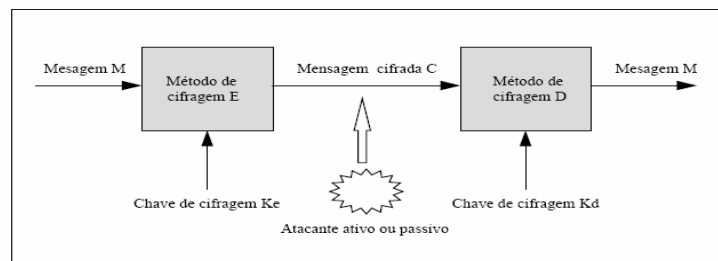


Figura 1 – Modelo básico de um sistema de criptografia

De acordo com a forma com que utilizam as chaves no processo de cifragem e decifragem das informações, os sistemas de criptografia pode ser classificados em simétricos e assimétricos [Galiano,1997]:

- **Sistemas simétricos:** utilizam uma única chave para cifragem e decifragem, que deverá ser mantida sob sigilo, sendo conhecida apenas pelos envolvidos na troca de mensagens. Os principais sistemas simétricos são: DES, 3DES, RC2, RC4 e RC5.
- **Sistemas assimétricos:** conhecidos também como sistemas de chave pública, utilizam um par de chaves, sendo uma de uso privado, que é mantida em sigilo pelo usuário, e outra de uso público, que pode ser acessada por qualquer pessoa. As chaves são diferentes e a partir de uma não se pode chegar à outra. Os principais sistemas assimétricos são o DH (*Diffie Hellman*) e o RSA.

Os sistemas de chave pública são bastante seguros e oferecem algumas vantagens em relação aos de chave simétrica, como a dificuldade de se enviar ou dizer a chave (senha) de forma segura, neste sistema não existem a necessidade de dizer ao destinatário qual foi a senha utilizada para a cifragem, pois existem duas e uma delas tem esta finalidade. Porém, vale ressaltar que os sistemas simétricos ainda são bastante utilizados,

principalmente quando se trata de proteger arquivos locais e de cifrar a chave privada gerada pelos sistemas assimétricos.

A velocidade de processamento da cifragem utilizando os sistemas simétricos é superior à dos sistemas assimétricos, o que os tornam bastante eficientes em conexões seguras na Internet, pois se já existe um canal seguro a troca de chaves pode ocorrer sem riscos. Muitas vezes os sistemas simétricos e assimétricos funcionam em conjunto, para garantir segurança sem queda de desempenho.

Os sistemas de criptografia são de suma importância para se conseguir segurança, pois é através deste que se obtém a autenticidade, privacidade e integridade dos dados, que são utilizados como componentes essenciais na segurança provida pelo IPSec.

4. IPSec

O IPSec integra mecanismos que fornecem ao pacote IP serviços que são providos pelos Sistemas de Criptografia (autenticidade, privacidade e integridade), garantindo segurança na camada de rede. O IPSec localiza na terceira camada (camada de rede) do modelo de referência RM-OSI. Desta forma, a segurança será garantida mesmo que as informações estejam sendo transportadas por meio não seguro, como a Internet.

O IPSec não impossibilita que os usuários instalem outros *softwares* de proteção, apenas é mais um mecanismo de defesa que criptografa e/ou certifica digitalmente os datagramas IP. Além disso, possibilita que as empresas implantem uma VPN (*Virtual Private Networks*), que é uma rede privada sobre uma rede pública, na qual é essencial adicionar proteção aos datagramas IP.

Para que sejam alcançados os objetivos do IPSec, é necessária a utilização de protocolos de tráfegos seguros: *Authentication Header(AH)* e *Encapsulating Security Payload(ESP)*, e de procedimentos e protocolos de gerência de chaves (IKE) (Rotole,2002). A figura 3 apresenta a arquitetura do IPSec, apresentada na RFC (*Request for Comments*) 2411 que estabelece as diretrizes para o conjunto de protocolos IPSec.

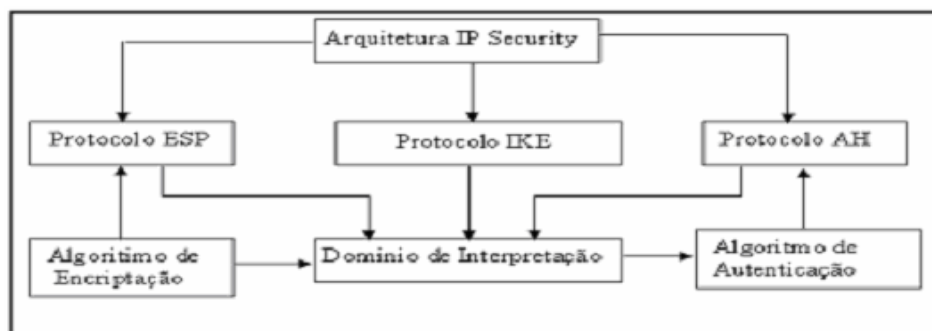


Figura 2 - Arquitetura IPSec

Na figura 2 pode ser observado que são empregados 3 protocolos: o ESP, IKE, AH a seguir será visto um pouco sobre cada um.

O protocolo AH é um protocolo que oferece segurança adicional ao protocolo IP, fornecendo autenticação, anti-repetição e serviços de integridade para o pacote inteiro, sem criptografar os dados. Desta forma, o destinatário pode ter a certeza que os dados foram realmente enviados pelo remetente que consta na mensagem. Problemas clássicos em IPv4, como a técnica de personificação – *IP Spoofing*, podem ser eliminadas completamente através do AH (Rotole, 2002). Os pacotes passam a estar protegidos pelo protocolo AH que insere um cabeçalho dentro do pacote a ser protegido que passa a conter os campos descritos na tabela 1.

Tabela 1: Descrição dos campos do cabeçalho protocolo AH

Campo	Descrição
Próximo Cabeçalho	Contém o identificador do próximo cabeçalho.
Comprimento do <i>Payload</i>	Tamanho do conteúdo do cabeçalho AH.
Reservado	Campo com 16 bits reservado para extensão do protocolo
SPI (<i>Security Parameter Index</i>)	Índice que, em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma AS (Associação de Segurança) para um determinado pacote.
Número de Seqüência	Identificador dos próximos pacotes, usado para evitar o <i>anti-replay</i> (negação de serviço).
Dados de Autenticação	Este campo de comprimento variável contém o ICV (<i>Integrity Check Value</i>) para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela AS.

O protocolo AH não suporta o *Network Address Translation* (NAT), pois este “mascara” o endereço IP original, perdendo com isso o verdadeiro emissor. O NAT é bastante utilizado em redes IPv4, especificamente em redes internas, com a finalidade de reduzir a utilização de endereços IP válidos, sendo uma alternativa para o problema da escassez de endereços IPv4.

O protocolo AH fornece autenticidade e integridade aos dados, no entanto, em momento algum pode ser garantido que as informações enviadas pela rede tenham sido vistas apenas pelo destinatário, ou seja, o AH não garante a confidencialidade. Para acrescentar esta funcionalidade o IPsec utiliza o protocolo ESP, que cifra os dados antes da transmissão (Silva, 2003). Os protocolos ESP e AH podem ser utilizados em conjunto para garantir uma maior segurança.

O Protocolo ESP assegura que, mesmo que se monitore ou intercepte um pacote IP, os dados contidos nele não poderão ser lidos. Diferentemente do protocolo AH que, apesar de adicionar um cabeçalho aos pacotes IP, não encapsula todo o conteúdo do datagrama o ESP empacota os dados dentro de sua estrutura. A tabela 2 apresenta uma breve descrição dos campos do cabeçalho ESP.

Tabela 2: Descrição dos componentes do protocolo ESP

Campo	Descrição
SPI (<i>Security Parameter Index</i>)	Índice, que em conjunto com o protocolo AH e o endereço fonte, identifica unicamente uma AS (Associação de Segurança) para um determinado pacote.

Número de Sequência	Identificador dos pacotes pertencentes a uma determinada AS, usado como mecanismo <i>anti-replay</i> .
Dados Cifrados e Parâmetros	Este campo contém os dados cifrados e os parâmetros utilizados pelo algoritmo de criptografia usado, definido pela AS.
Dados de Autenticação	Este campo contém o ICV (<i>Integrity Check Value</i>) para este pacote, calculado seguindo o algoritmo de autenticação usado, definido pela AS.

O ESP permite a utilização tanto de sistemas simétricos como assimétricos. Como a criptografia só é possível através das chaves criptográficas, é necessário que a entidade autorizada a visualizar as informações tenha acesso à chave de decifração. Porém, existe um problema em como disponibilizar esta chave de forma segura, sem que entidades não autorizadas tenham posse indevida da mesma. Para resolver esse problema o IPSec utiliza um protocolo de gerenciamento de chaves denominado IKE.

O protocolo IKE (*Internet Key Exchange*) é utilizado para a gerência automática das chaves criptográficas, com o objetivo de disponibilizar as chaves de forma segura e automática caso seja utilizado o protocolo ESP, que criptografa os dados e portanto necessita de uma chave criptográfica (Silva, 2003).

O domínio de interpretação (DOI) funciona como um banco de dados que armazena as informações, como: algoritmos obrigatórios e identificadores dos protocolos. Estas informações são consultadas durante uma negociação de AS (Associação de Segurança) que é o estabelecimento de um canal seguro para a comunicação.

Uma associação de segurança é um acordo que as entidades participantes da comunicação estabelecem para que se consiga uma comunicação segura, sendo identificada por três parâmetros (Rotole, 2002):

- SPI (Security Parameter Index) - é uma string de 32 bits, definida durante a negociação, que registra o endereço IP da fonte e identifica uma AS para determinado pacote.
- Endereço IP do destino – utilizado para mecanismos de gerenciamento da AS e evitar o extravio do pacote.
- Identificador do protocolo (AH ou ESP) - é o número que identifica o protocolo que está sendo utilizado, 51 para AH e 50 para ESP.

Durante a configuração do IPSec podem ser escolhidos os níveis de segurança desejados, para que se consiga uma proteção de acordo com as necessidades do sistema a ser protegido. Esses dados ficam registrados no Sistema Operacional como um conjunto de critérios, que são as diretivas de segurança.

5. IPSec no Sistema Operacional Windows

Para habilitar a garantia de segurança provida pelo protocolo IPSec, que já vem instalado por padrão no Windows 2000, XP ou superior, é necessário criar e ativar diretivas de segurança, sendo que são oferecidas três opções:

- Cliente (responder somente): com o uso desta diretiva o sistema nunca irá requerer segurança, ou seja, comunica-se normalmente e só inicia uma negociação em resposta à solicitação de outro sistema que necessita de segurança.
- Servidor (solicitar segurança): com o uso desta diretiva o sistema passa a solicitar segurança, mas não exige a utilização de segurança IPSec de todos os outros sistemas. Esta é a diretiva mais recomendada, pois sempre que possível a comunicação se estabelece com a utilização do IPSec, mas o servidor continua atendendo clientes que não possuem diretivas IPSec.
- Servidor seguro (requer segurança): com o uso desta diretiva o sistema passa a exigir segurança IPSec para todas as comunicações e negar todas as comunicações que não suportam IPSec. Esta diretiva é aconselhada para servidores que contenha informações extremamente sensíveis.

A partir de diferentes configurações das diretivas IPSec, foram realizados testes para verificar o nível de proteção de cada uma e demonstrar a vulnerabilidade dos sistemas sem proteção.

6. Testes de Segurança Realizados

Com o objetivo de demonstrar a vulnerabilidade das redes TCP/IP não protegidas e para verificar a eficiência do IPSec, foram realizados testes através da execução de um *software* para a captura dos pacotes que transitavam na rede, o Ethereal, que é oferecido gratuitamente na Internet.

Além do Ethereal, foi utilizado o ping para testar a conectividade entre equipamentos interligados em rede. Os dois programas foram executados para analisar a comunicação em máquinas configuradas com diferentes níveis de segurança. Em um primeiro momento, foram realizados testes entre máquinas em que as diretivas IPSec não estavam configuradas, para demonstrar a vulnerabilidade da comunicação. Depois disso, foram definidos os critérios de segurança da diretiva IPSec nas máquinas, para verificar o comportamento do mesmo.

6.1 Testes realizados sem a utilização de diretivas IPSec

O teste foi realizado com a execução do programa Ethereal, que apresenta na tela uma lista com algumas informações sobre todas as mensagens capturadas, que são: número IP da máquina origem e destino, portas de origem e destino; tipo de protocolo utilizado no envio como, por exemplo, TCP, UDP ou ARP; e uma breve descrição da mensagem.

Para visualizar o conteúdo completo da mensagem capturada o usuário deve escolher a opção “Follow TCP Stream” do programa Ethereal após ter finalizado a captura dos pacotes, é disponibilizado uma nova janela com o conteúdo da mensagem escolhida que, apesar de estar um pouco desorganizado, pode ser lido sem maiores problemas, conforme é apresentado na figura 3.

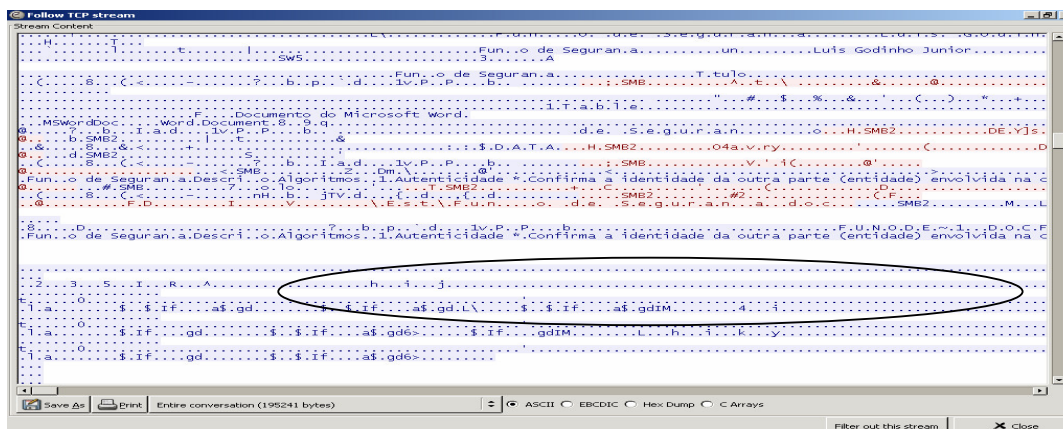


Figura 3 – Tela do Ethereal com a mensagem capturada - sem diretivas IPsec.

Analisando o trecho destacado na figura 3 pode-se perceber que as informações trafegadas sem a proteção do IPsec podem ser capturadas, com o uso de ferramentas como a utilizada (Ethereal) que é disponibilizada gratuitamente na Internet.

6.2 Testes realizados com a utilização de diretivas IPsec

Os testes de comunicação entre as máquinas foram realizados em três situações diferentes, conforme as diretivas escolhidas na configuração do IPsec:

1. **Máquina origem e destino com IPsec configurado com a diretiva solicitar segurança:** Esta é a diretiva mais flexível, pois permite estabelecer comunicação com ou sem segurança, bastando para isso verificar o lado do destinatário se tem ou não diretiva de segurança configurada caso exista a comunicação será estabelecida de forma segura.
2. **Máquina origem sem o IPsec e destino com IPsec configurado com a diretiva requerer segurança:** neste caso a comunicação não será possível, pois com a diretiva requerer segurança a máquina só aceita comunicação com outras que tenham o IPsec;
3. **Máquina origem com IPsec configurado com a diretiva solicitar segurança e a máquina destino sem diretivas IPsec:** neste caso a comunicação acontece sem a segurança IPsec, pois a origem apenas solicita e não recusa a comunicação sem IPsec.

Situação 1

Depois que o IPsec foi configurado, nas máquinas origem e destino, com a diretiva solicitar, foi executado o Ping, para verificar a comunicação entre as máquinas. Como pode ser observado na figura 4, houve toda a negociação de segurança IPsec durante o tempo que apareceu a mensagem “Negociando segurança IP”. Nesse momento também é realizada a troca de chaves pelo protocolo IKE.

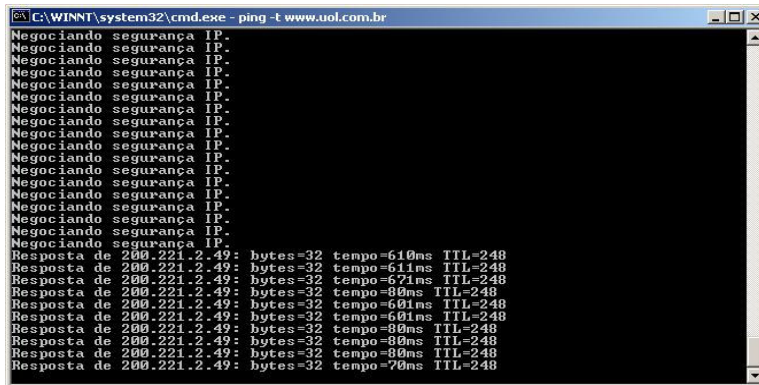


Figura 4 – Ping: máquina origem e destino com IPSec com a diretiva solicitar.

O segundo teste aplicado com as máquinas foi à execução do Ethereal, que apresentou a listagem das mensagens capturadas, como mostra a figura 5.

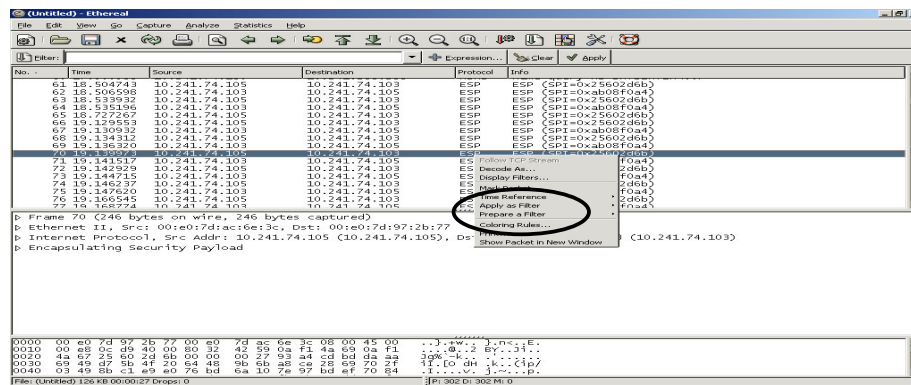


Figura 5 - Ethereal: máquinas de origem e destino com a diretiva solicitar.

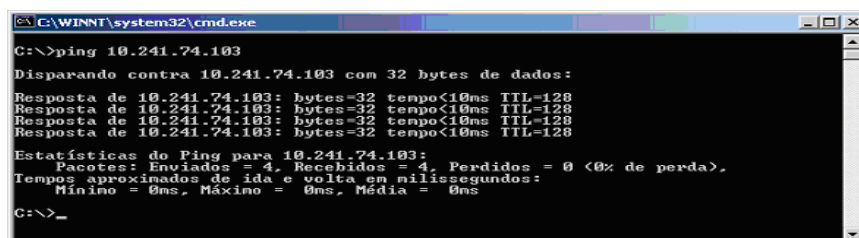
Como pode ser verificado a opção “Follow TCP Stream”, destacada na figura 5, fica desabilitada para quem capturou os pacotes, devido às medidas de segurança fornecidas pelo IPSec.

Situação 2

Nesta situação o IPSec foi configurado com a diretiva requerer segurança na máquina destino e na máquina origem o IPSec não foi configurado. Foi utilizado o Ping, para verificar se a máquina destino estava respondendo, sendo que não houve resposta da mesma. Com esse teste, constatou-se que a máquina destino não respondeu, pois recusou a comunicação pelo fato do iniciador da comunicação não possuir diretivas IPSec.

Situação 3

Por fim, o IPSec foi configurado na máquina origem com a diretiva solicitar segurança e não configurado na máquina destino. A execução do Ping apresentou os resultados mostrados na figura 6.



```
C:\WINNT\system32\cmd.exe
C:\>ping 10.241.74.103
Disparando contra 10.241.74.103 com 32 bytes de dados:
Resposta de 10.241.74.103: bytes=32 tempo<10ms TTL=128
Resposta de 10.241.74.103: bytes=32 tempo<10ms TTL=128
Resposta de 10.241.74.103: bytes=32 tempo<10ms TTL=128
Resposta de 10.241.74.103: bytes=32 tempo<10ms TTL=128

Estatísticas do Ping para 10.241.74.103:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
    Tempo aproximado de ida e volta em milissegundos:
        Mínimo = 0ms, Máximo = 0ms, Média = 0ms
C:\>_
```

Figura 6 – Ping: origem com a diretiva solicitar segurança e destino sem diretivas.

Analisando o resultado percebe-se que a comunicação acontece normalmente sem associação de segurança, pois as máquinas que têm a diretiva solicitar se comunicam sem segurança com as máquinas sem diretivas IPSec e de forma segura com máquinas em que as mesmas estejam configuradas.

9. Conclusões

De acordo com os estudos realizados percebeu-se a importância de procurar alguma forma de garantir segurança na comunicação em rede. Uma delas é a utilização do IPSec para garantir integridade, confidencialidade e autenticidade, de acordo com a configuração de seus níveis de segurança, de forma transparente para os usuários, pois não requer a participação dos mesmos nas negociações de segurança da comunicação. Com a aplicação de testes práticos de comunicação entre máquinas sem configuração de diretivas de segurança e entre máquinas com diferentes configurações dessas diretivas, foram obtidos e apresentados resultados que comprovam a eficiência do IPSec.

Vale ressaltar que existem muitos textos que afirmam que o IPSec faz parte das funcionalidades do IPv6, ou seja, que o IPSec é mandatário no mesmo, porém não foram encontrados resultados de testes que comprovem esta afirmação e nem informações sobre a forma de utilização desde mecanismo de segurança no novo protocolo.

10. Referências

- [Silva, 2003] Silva, Lino Sarlo. Virtual Private Network (VPN), ED. Novatec.
- [Braghetto, 2003] Braghetto, Luis Fernando B; Silva Sirlei Cristina da. IPSec Segurança de Redes – INF542. Universidade Estadual de Campinas Unicamp. São Paulo, 2003. Disponível em <http://www.braghetto.eti.br/files/IPSec%20-%20Versao%20Final.pdf> acessado em maio de 2004.
- [Galiano, 1997] Galiano, Herbert Luna; Rochol, Juergen. Segurança em Sistemas de Comunicação Pessoal - Um Estudo Comparativo da Interconexão de Sistemas Heterogêneos. Artigo publicado XV Simpósio Brasileiro de Redes de Computadores. Disponível em http://labcom.inf.ufrgs.br/artigos/seguranca_em_sistemas.pdf, acesso em Junho de 2004.

