FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

IPSEC: SEGURANÇA NA CAMADA DE REDE

ROBSON WENCESLAU ROSSI

AMERICANA / SP

2012

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

IPSEC: SEGURANÇA NA CAMADA DE REDE

ROBSON WENCESLAU ROSSI

robsonlp22@gmail.com

Monografia apresentada à Faculdade de Tecnologia de Americana como parte das exigências do curso de Segurança da Informação para obtenção do título de Tecnólogo em Segurança da Informação, sob a orientação do Profº Edson Roberto Gaseta.

AMERICANA / SP

2012

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

ROBSON WENCESLAU ROSSI - RA 0912229

IPSec: SEGURANÇA NA CAMADA DE REDE

Monografia aprovada como requisito parcial para obtenção do título de Tecnólogo em Segurança da Informação do curso de Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Prof. Edson Roberto Gaseta

Professor da Disciplina: _____
Prof. Carlos Henrique Rodrigues Sarro

Professor Convidado: _____
Prof. Marcus Vinicius Lahr Geraldi

Americana, 19 de Junho de 2012.

AGRADECIMENTOS

Agradeço a realização deste trabalho, primeiramente a Deus, meus pais, Valdir Rossi e Dalva Ap. Wenceslau Rossi, pela paciência e absolvição de algumas falhas.

Integrando a lista, minha namorada Cynthia P. Barbieri pela contínua cobrança do andamento do trabalho, a calma e carinho com qual me auxiliou a concretização do mesmo.

Reconheço também meus amigos, colegas de curso e trabalho que durante o curso na faculdade me auxiliaram de várias maneiras a concluir o mesmo, e meu professor durante a faculdade e posteriormente meu orientador pelos ensinamentos e conselhos dados para a realização do mesmo.

Dedico este trabalho de conclusão de curso a minha família, meus pais Valdir Rossi e Dalva Ap. Wenceslau Rossi, minha namorada Cynthia P. Barbieri e aos meus amigos.

“Se uma notícia secreta é divulgada por um espião antes da hora certa, ele precisa ser morto, juntamente com o homem a quem o segredo foi dito.”

A arte da guerra, Sun Tzu

RESUMO

O IPsec faz parte do protocolo IP para garantir a segurança de pacotes em redes não seguras, e é usado para conexão de computadores em uma rede segura com criptografia e sua principal função é assegurar que os dados cheguem ao destino da comunicação entre hosts de forma garantida, sendo estes dados confiáveis aos usuários.

Será abordado no decorrer do trabalho, conexões de redes virtuais privadas (VPNs), junto as estruturas que fazem parte do IPsec como cabeçalho AH e ESP e como atualmente é implementado o protocolo de segurança na versão IPV4. Ao fim do trabalho terá uma abordagem estabelecendo a teoria efetivamente em um exercício prático.

Palavras-chave: IPSec. Segurança. Protocolo. *IP*

ABSTRACT

IPsec is part of the IP protocol to ensure security area of data over unsecured networks, and is used for connecting computers on a secure, encrypted network and its main function is to ensure that the data arrives at the destination of the communication between hosts in a secure, reliable data for the users.

Will be addressed in this work, connections, virtual private networks (VPNs), with the structures that are part of IPsec such as ESP and AH header and how is it currently implemented in the protocol version IPv4. The end of the work will establish an approach to the effectively theory in a practical exercise.

Keywords: IPSec. Security. Protocol. *IP*

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

1. INTRODUÇÃO

Este trabalho tem como objetivo abortar sobre segurança de *IP* ou IPsec, que é um protocolo de segurança que trabalha na camada de rede, protegendo datagramas *IP* e comunicações por meio de redes locais (LAN) e de longas distancias (WANs) privadas ou públicas, compreendendo roteadores e hosts pela *Internet*.

O IPsec provê uma conexão segura, entre dois pontos de *Internet* como computadores e outros quaisquer dentro de uma rede, mesmo que esta rede não seja interligada a *Internet* por um meio seguro. Com isto empresas, órgãos do governo e outras organizações usam o protocolo a fim de criar redes virtuais privadas (VPNs).

O protocolo IPsec abrange três áreas funcionais:

- Autenticação, onde utiliza o código de mensagens HMAC;
- Confidencialidade utilizando um formato de criptografia chamado de encapsulamento de segurança do *payload*;
- Técnicas para gerenciamento de chaves.

Estas três áreas serão abordadas no transcorrer do trabalho.

2. O DATAGRAMA *IP*

O datagrama *IP* é implementado nas comunicações de uma rede, em dispositivos que oferecem conexão entre as redes, com o objetivo de interconectá-los e transferir dados. Utilizando dados de nível mais alto, encapsulados com a PDU (*Protocol Data Unit*) de *IP* para transmissão, possuem um tamanho entre 20 a 60 bytes, é composto por um cabeçalho de controle com diversas informações a fim de entregar os datagramas *IP* via roteamento e uma área de dados.

Devido às várias diferenças entre redes locais, públicas ou privadas, como endereços diferentes e outros problemas na *Internet* (vários tipos e tamanhos de pacotes de dados na rede, entre outros), há dificuldades na entrega dos datagramas para os equipamentos de rede como roteadores e suas respectivas redes locais.

O protocolo *IP* (*Internet Protocol*), que determina o datagrama *IP* estudado, possui duas versões, o IPv4 o qual será utilizado como base no andamento deste trabalho, que consiste em um número de 32 bits representados normalmente em forma decimal e indicando essencialmente o local da rede ou o nó do host na rede e o IPv6 que é o novo modelo que consiste basicamente em maior número de endereços, pois utiliza até 256^{16} endereços e possui 128 bits e um cabeçalho bastante complexo, por isso a opção de tomar como base no trabalho o IPv4.

Como será discutido, o protocolo *IP* não provê um serviço confiável, mantêm a política de "melhor esforço", pois não há certeza da entrega dos pacotes a rede destino, nem em ordem correta, portanto não existindo requisito de confiabilidade em nenhuma das redes. A figura 1 representa a composição do datagrama *IP*.

CABEÇALHO IPV4	CABEÇALHO TCP	DADOS TCP

Figura 1: Exemplo de datagrama *IP* (Própria autoria)

3. SERVIÇOS ORIENTADOS E NÃO ORIENTADOS A CONEXÃO

Em uma rede existem dois serviços distintos: o serviço orientado a conexão, que é o serviço no qual existe garantia de que os dados sejam entregues ao destino da mesma maneira que foram enviados, e o serviço não orientado a conexão, que ao contrário envia os dados, porém não garante a entrega.

3.1. Serviço orientado a conexão (TCP)

No momento em que o serviço orientado a conexão é usado, primeiramente, entre o cliente e o servidor em uma rede, é aberta uma espécie de canal de controle entre eles para que seja criada uma conexão, a fim de enfim enviar os dados. Assim que isto ocorre, a conexão está estabelecida, entretanto, como o nome diz apenas orientado a conexão, pois, somente os sistemas finais reconhecem esse canal, os comutadores - como switches e roteadores - de camada de rede que encaminham os pacotes na rede não possuindo a informação desta conexão. Um possível problema que esse serviço possui, é que como todos os dados enviados irão ser entregues ao destino, é enviado juntamente uma confirmação do remetente do pacote, o que em determinado momento pode causar uma sobrecarga de informações, causando lentidão não necessária, chamado de overhead.

O TCP, protocolo de controle de transmissão, também do conjunto TCP/IP, é o protocolo que garante a entrega dos datagramas *IP*. Um exemplo de serviço TCP na *Internet* é o envio de dados via FTP que é uma forma de transferir arquivos rapidamente na *Internet* com garantia de entrega dos datagramas.

3.2. Serviço Não Orientado a Conexão (UDP)

Utilizando este serviço, o canal de controle entre cliente e servidor não é criado, portanto os equipamentos em uma rede enviam pacotes um ao outro sem confirmação da entrega ou não, neste serviço, como não há este canal, os dados tendem a serem enviados mais rapidamente para o destino.

O UDP, Protocolo de Datagrama de Utilizador, igualmente do conjunto do TCP/IP, em alguns casos substitui o TCP, principalmente para transporte de dados mais rápido e simples, por isso, por exemplo, são usados em streaming de vídeo e musica.

3.3. Comparação entre UDP e TCP

A tabela 1 mostra a comparação entre os protocolos UDP e TCP

Tabela 1: Comparativo entre os protocolos UDP e TCP. (Fonte: Microsoft Technet, 2012)

UDP	TCP
Serviço sem ligações; não é estabelecida nenhuma sessão entre os anfitriões.	Serviço orientado a ligações; é estabelecida uma sessão entre os anfitriões.
O UDP não garante ou confirma a entrega, nem estabelece a sequência dos dados.	O TCP garante a entrega através da utilização de confirmações e a entrega sequencial dos dados.
Os programas que utilizam o UDP são responsáveis pelo fornecimento da fiabilidade necessária para o transporte dos dados.	Os programas que utilizam o TCP são fornecidos com a garantia da fiabilidade de transporte de dados.
O UDP é rápido, possui poucos requisitos de sobrecarga e pode suportar comunicações ponto a ponto ou ponto a multipontos.	O TCP é mais lento, possui mais requisitos de sobrecarga e apenas suporta a comunicação ponto a ponto.

4. O QUE É SEGURANÇA SOBRE *IP*

Como dito anteriormente e segundo Carissimi (2009), o protocolo *IP*, em função da época em que foi estabelecido não possuía segurança na troca de informações na rede. Após a explosão da *Internet* no mundo, a idéia de segurança, ou então a falta dela, tornou-se eminente, até que o IETF (*Internet* Engineering *Task Force*) criou o *Internet* IPSecurity (IPSec) em 1998 nas normas chamadas de RFCs de números 2401 e 2402, em meio de grandes discussões até estabelecer que a camada de rede fosse adequada para inserir a criptografia na *Internet*.

As principais vulnerabilidades do datagrama *IP,* o qual necessita do IPSec na questão de segurança na rede são: autenticidade, integridade e confidencialidade. Quando o *IP* de destino pode ser alterado por qualquer programa malicioso, ou não se pode confiar de que o *IP* de origem que consta no datagrama recebido está correto, temos um problema de autenticidade. Em um datagrama que chega ao *IP* de destino e não se pode verificar se o mesmo pacote de dados realmente chegou da mesma maneira de que foi enviado pela origem, há então problema de integridade dos dados. Os datagramas, por trafegarem em uma rede que outros têm acesso, ficam vulneráveis a captura deste pacote ou substituição do conteúdo, criando possíveis problemas de confidencialidade.

> Portanto, o IPSec oferece os meios necessários para garantir a confidencialidade, a integridade e a autenticidade dos pacotes IPs transmitidos e recebidos. Ele trabalha com uma variedade de esquemas padronizados e processo de negociação de criptografia bem como com vários sistemas de segurança. ***Guimarães (2006)***

Um administrador de rede, antes de utilizar criptografias próprias e que podem ser de alto valor e incompatíveis com toda a *Internet* fora de sua rede local, ou construir uma rede física a fim de prover uma segurança inquebrável e não viável economicamente, este usa o IPsec que resolve os problemas descritos e outros, como autenticação e privacidade, a fim de promover segurança na camada de rede.

Quando se configura uma VPN (Rede Privada Virtual), é utilizado o IPsec para garantir segurança na troca de informações entre uma conexão VPN cliente-a-servidor ou rede-a-rede, junto com mecanismos de criptografia e alguns protocolos, a rede pode ser considerada segura, tornando-a a escolha aceita pelos administradores de rede.

Ao criar o IPSec, o IETF teve o cuidado para que este seja implementado na camada *IP*, portanto com suporte tanto a IPv4 ou IPv6. A configuração de IPsec é bastante flexível, podendo ser configurado por criptografias, autenticações extras em específicos pontos da rede, ou apenas em um sentido de tráfego de rede e não no outro. É importante salientar que o IPSec, como um conjunto de protocolos, pode ser utilizado da melhor maneira possível e adequado aos ambientes de rede.

4.1. Redes privadas Virtuais (VPNs)

Uma empresa que possui filiais espalhadas em diferentes regiões é preciso que exista algum tipo de conexão entre elas, para possibilitar a troca de informações cotidianas ou secretas da empresa. A fim de criar uma conexão segura entre as empresas e filiais, é necessária uma rede própria privada, que antigamente (algumas empresas usam até atualmente) eram físicas, onde há cabos que as conectavam, o que gera um alto custo de implantação e manutenção. Assim, Tanenbaum (2003); Compartilha das afirmações acima.

A solução deste grande gasto e ainda se preocupando com a segurança na troca de seus dados foi estabelecida as VPNs, redes privadas virtuais, que conectam as empresas utilizando a rede pública de dados, a *Internet*. A opção de utilizar os serviços IPSec nas configurações de uma VPN torna a conexão mais segura, criptografando os dados e se utilizando de cabeçalhos extras nos pacotes enviados na rede publica, criando assim uma espécie de túnel no interior da *Internet* evitando que pessoas de fora da empresa não possam acessar os dados trafegados.

Alem da vantagem financeira, a VPN é interessante, pois, é transparente aos usuários finais que não precisam de orientação para utilizá-la. Para uma utilização mais adequada da VPN, é fundamental a utilização de firewalls, mas como descreve Peterson (2004), se todos os mecanismos de segurança, como exemplo o IPSec estivessem em uso, não haveria necessidade de firewalls, pois são basicamente filtros que ficam entre os hosts e o restante da rede a fim de validar os dados entregues e recebidos, e descartá-los quando preciso, e como é utilizado especificamente para segurança, o *firewall* será tanto ponto de partida quanto chegada desse túnel criado pela VPN. A figura 2 representa a utilização de uma VPN com *firewalls*.

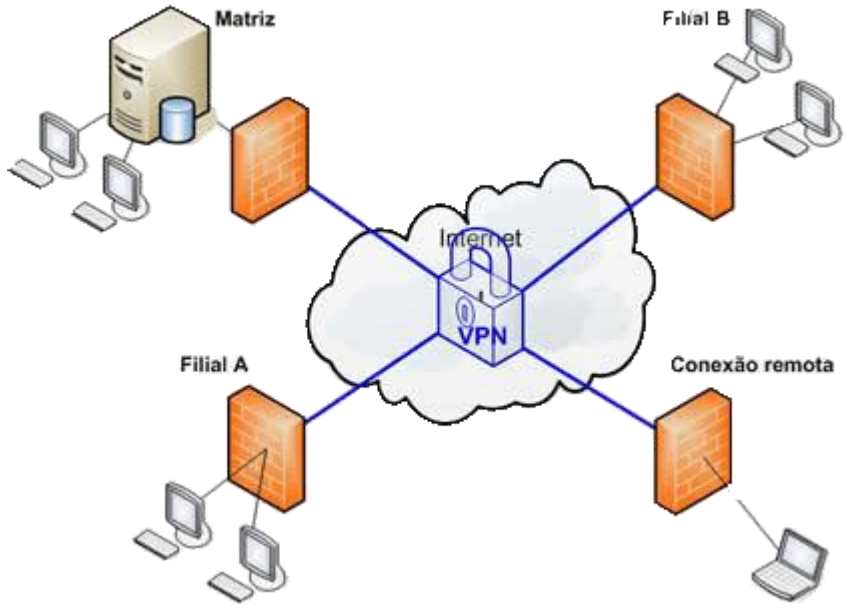


Figura 2: Exemplo de VPN com firewalls (Vulcanet, 2012)

Fonte: http://www.vulcanet.com.br/produtos/interconex-vpn/. Acessado 1 maio 2012

5. APLICAÇÕES DO IPSec

Para Stallings (2005), o IPSec em si protege as comunicações entre LANs, WANs públicas, redes privadas e públicas pela *Internet*. Algumas funções do protocolo de segurança são:

- **Conexão segura entre filiais e matriz de uma empresa através da *Internet*:** Com a possibilidade de segurança na *Internet* ou por WANs, as empresas podem utilizar do IPSec a fim de utilizar melhor os serviços da *Internet* por causa da criptografia da rede, barateando os custos com redes privadas, e reduzindo seu overhead.

- **Acesso remoto seguro via *Internet*:** Caso um funcionário que esteja em viagem de negócios ou fora da empresa, e que possua em seu equipamento um sistema que seja equipado com os protocolos de segurança *IP*, este pode utilizar seu computador para conectar na rede da empresa de forma segura.

- **Constituir conexão com terceiros:** Existe a alternativa de estabelecer conectividade segura de um local com outras organizações e de forma segura (privacidade e autenticação) e prover um mecanismo de troca de chaves.

- **Progresso na segurança em comercio eletrônico:** Enquanto as aplicações web e email já possuem segurança normalmente, o IPSec soma mais esta camada de segurança nos sistemas web.

5.1. Vantagens sobre o IPSec

Logo após apresentar as aplicações do IPSec, as vantagens na sua implementação são:

- Em um *firewall* ou roteador, quando o IPSec é implementado, esta rede é considerada em estado de segurança forte, e enquanto o tráfego é interno na rede, não gera overhead do processamento em relação a segurança.

- Caso o *firewall* seja a única porta de entrada da *Internet* na rede, e se os dados estiverem vindo com endereços IPs, uma configuração de IPSec irá impedir que seja realizado um *bypass*, que são os pacotes de dados não utilizarem portas alternativas para escapar do firewall.

- Devido o IPSec ser implementado na camada de rede, e não de aplicação, enquanto os roteadores ou firewall estiverem com IPSec, às aplicações ou sistemas finais podem ser modificados, que não haverá mudanças no protocolo de segurança, pois, este está abaixo da camada de transporte (TCP, UDP), portanto invisíveis para as aplicações.

- Semelhante com o beneficio anterior, como o IPSec não é visível aos sistemas finais, o usuário também não terá que se aprimorar para utilizar a segurança garantida nem se preocupar com senhas e/ou criptografia.

- A segurança remota pode ser resolvida quando um funcionário externo, por exemplo, utiliza seu computador fora da rede, com a necessidade de ter instalado um client no computador, e este terá os benefícios da rede segura da empresa.

5.2. Função do IPSec

No decorrer desse trabalho serão destacadas algumas funções do IPSec:

- Função de Autenticação, a Authentication Header (AH);
- Combinação de autenticação e criptografia, o Encapsulating Security Payload (ESP);
- Gerenciamento de chaves.

> IPSec não é um protocolo de segurança isolado. Em vez disso, IPSec oferece um conjunto de algoritmos de segurança e mais uma estrutura geral que permite que um par de entidades em comunicação utilize quaisquer algoritmos que ofereçam segurança apropriada para a comunicação. ***Comer (2006)***

Na função de autenticação, o protocolo AH fornece autenticação e integridade dos dados entre remetente e destinatário, porém, não provê sigilo. O protocolo ESP por outro lado, além de prover autenticação e integridade, também provê o sigilo. Portanto, como em uma VPN é importante assegurar segredo dos dados contidos nas conexões, o ESP é mais usado que o AH.

A função de troca de chaves entrega chaves secretas para seus sistemas, podendo essa distribuição ser manual ou automatizada.

Atualmente para se usar IPSec, é necessário que aceite criptografia DES (*Data Encryption Standard*), porém podem-se utilizar outros algoritmos de criptografia. Em especial neste trabalho será mostrado um esquema relativamente novo, conhecido com HMAC.

Será apresentado detalhadamente cada item destas funções do IPSec para uma rede.

6. ASSOCIAÇÃO DE SEGURANÇA

Os datagramas IPSec são transmitidos na rede entre todos os equipamentos, porem sem a utilização de NAT. Portanto, para que os datagramas sejam entregues seguros, antes é criada uma espécie de canal entre destinatário e remetente, essa conexão é chamada de associação de segurança (SA), que faz um caminho entre os equipamentos destinatário e remetente, e é unidirecional, ou seja, para que ambos enviem datagramas de um a outro é necessário duas SAs, uma para cada direção. Lembrando que somente é criada a SA quando for enviado datagramas seguros com IPSec. No caso de um host, por exemplo, queira somente utilizar da *Internet*, estará usando o IPv4 normalmente sem SAs.

Para esclarecer melhor, veremos em que consiste uma SA:

- Um identificador de 32 bits, chamado de Índice de Parâmetro de Segurança (SPI);
- As interfaces remetente e destinatário;
- A criptografia a ser usada;
- O tipo de constatação de integridade, como por exemplo, o HMAC;
- A chave de autenticação.

Os conteúdos necessários em uma SA são denominados de informações de estado da SA. Para que seja criado um datagrama IPSec e saber como será a autenticação e a criptografia, são essenciais os estados das SAs, para que o mesmo estado utilizado no destinatário seja usado para descriptografar os datagramas.

Como as informações podem ser usadas em outros datagramas IPSec diferentes, elas podem ser guardadas no Banco de Dados de Associação de Segurança (SAD).

7. MODOS DE TRANSPORTE E DE TÚNEL

Em uma associação de segurança (SA), o IPSec define dois modos, transporte e o túnel. No modo transporte é inserido o cabeçalho IPSec após o cabeçalho *IP*, não alterando o cabeçalho original. Este modo protege principalmente protocolos da camada superior a camada de rede, ou seja, inclui o cabeçalho *IP* e os dados do pacote. Geralmente o modo transporte é empregado em comunicação fim a fim entre hosts finais, por exemplo, cliente e servidor.

O modo túnel oferece proteção a todo o pacote *IP*, pois, o pacote é encapsulado e se torna a carga de um novo cabeçalho *IP* e o cabeçalho IPSec é inserido após o cabeçalho *IP* original. Portanto, no modo túnel, o endereço de quem envia e quem irá receber o pacote é protegido e também a quantidade de pacotes enviados nesta SA. O tunelamento (pode ser assim chamado) torna-se a melhor escolha para envio de pacotes que serão enviados a destinos físicos diferentes.

Guimarães (2006) explica que o modo túnel é empregado entre hosts finais e roteadores ou entre roteadores, e desta forma, quando há um roteador o IPSec pode ser ativo nele, não havendo, a necessidade de ativar todas as estações de trabalho de uma empresa.

Ambos os protocolos apresentados a seguir podem ser encapsulados em modo transporte ou túnel.

8. PROTOCOLOS IPSec

Existem diversas formas de implementar o IPSec, por exemplo, usando os protocolos principais:

- Cabeçalho de autenticação AH (*Authentication Header*);
- Carga de segurança de encapsulamento ESP (*Encapsulating Security Payload*).

Os dois protocolos resolvem problema de segurança no envio de datagramas na rede, e ambos serão apresentados, contudo devido ao sigilo oferecido, o ESP atualmente é usado com mais freqüência, o que simplifica a tabela 2 abaixo de Stallings (2008):

Tabela 2: Diferenças entre os cabeçalhos AH, ESP e ESP (com autenticação); (Stalling, 2008)

	AH	ESP (apenas criptografia)	ESP (criptografia mais autenticação)
Controle de acesso	✓	✓	✓
Integridade sem conexão	✓		✓
Autenticação da origem de dados	✓		✓
Rejeição de pacotes repetidos	✓	✓	✓
Confidencialidade		✓	✓
Confidencialidade limitada do fluxo de tráfego		✓	✓

8.1. Protocolo AH

No envio de um datagrama na rede, este possui segmentos, sendo um deles os dados que serão entregues. Dentre as partes do datagrama, há o cabeçalho. Como descreve Tanenbaum (2003), no AH, o IPSec usa um cabeçalho de autenticação, que fornece verificação de integridade e segurança contra reprodução, mas não há criptografia, portanto, não há sigilo nos dados do datagrama enviado.

Também para Peterson (2004), o Protocolo AH oferece:

> [...] Controle de acesso, integridade da mensagem sem conexões, autenticação e antireplay. ***Peterson (2004)***

O cabeçalho AH, é empregado para transportar informações que necessitam de autenticação no datagrama *IP*. Com IPv4, o AH pode optar pelo modo transporte ou modo túnel. No modo transporte, o cabeçalho AH é inserido logo após o cabeçalho *IP* original e antes de cabeçalho de transporte. É importante ressaltar que quando usa o modo transporte, os hosts finais de origem e destino, devem utilizar também o modo transporte.

No modo túnel é criado um novo cabeçalho *IP* que contem as informações do cabeçalho *IP* original, e em seguida alocado o cabeçalho AH. Desta maneira, o pacote *IP* original fica intacto e como já mencionado, gera proteção aos endereços de origem e destino do pacote.

A figura 3 mostra onde é inserido o cabeçalho AH nos diferentes modos de SA, e no campo do cabeçalho *IP* chamado de protocol, é inserido o número 51, indicando assim a presença de um cabeçalho de autenticação.

CABEÇALHO IPV4	CABEÇALHO TCP	DADOS TCP

Exemplo de formato de datagrama IPv4

CABEÇALHO IPV4	CABEÇALHO DE AUTENTICAÇÃO	CABEÇALHO TCP	DADOS TCP

O mesmo datagrama acima, após inserção do protocolo de autenticação AH, logo após o cabeçalho *IP* – Modo transporte

NOVO CABEÇALHO IPV4	CABEÇALHO DE AUTENTICAÇÃO	CABEÇALHO IPV4	CABEÇALHO TCP	DADOS TCP

O mesmo primeiro datagrama *IP*, após inserção do protocolo AH antes do cabeçalho *IP* original – Modo túnel

Figura 3: Pacote *IP* e os modos transporte e túnel no protocolo AH no IPv4. (Própria autoria)

Na figura 4, são mostrados os seis campos que compõem o cabeçalho AH que tem em seu total 32 bits.

- Próximo cabeçalho – Tipo de protocolo (seu código) que o datagrama carrega (ICMP, UDP, TCP...) e armazena o valor que o protocolo *IP* tinha antes.
- Tamanho da área de dados (*payload*) – Especifica o tamanho do cabeçalho de autenticação.
- Reservado – Reservado para uso futuro e para garantir a segurança
- Índice de parâmetro de segurança – Usado para garantir segurança e se mantêm fixo durante a conexão SA.

- Número de seqüência - Cria um número de seqüência para cada pacote enviado na conexão SA realizada. Este número serve para que não haja datagramas repetidos e se caso esgote os números de seqüência, ou seja, passe de 2^{32}, terá de ser estabelecida nova SA.
- Dados de autenticação – Dados de tamanho variável, que contem a assinatura digital da carga útil e pertencendo assim ao esquema de segurança do AH, onde qualquer alteração do endereço *IP* do remetente pode ser verificada. Neste campo é utilizado o algoritmo de autenticação HMAC.

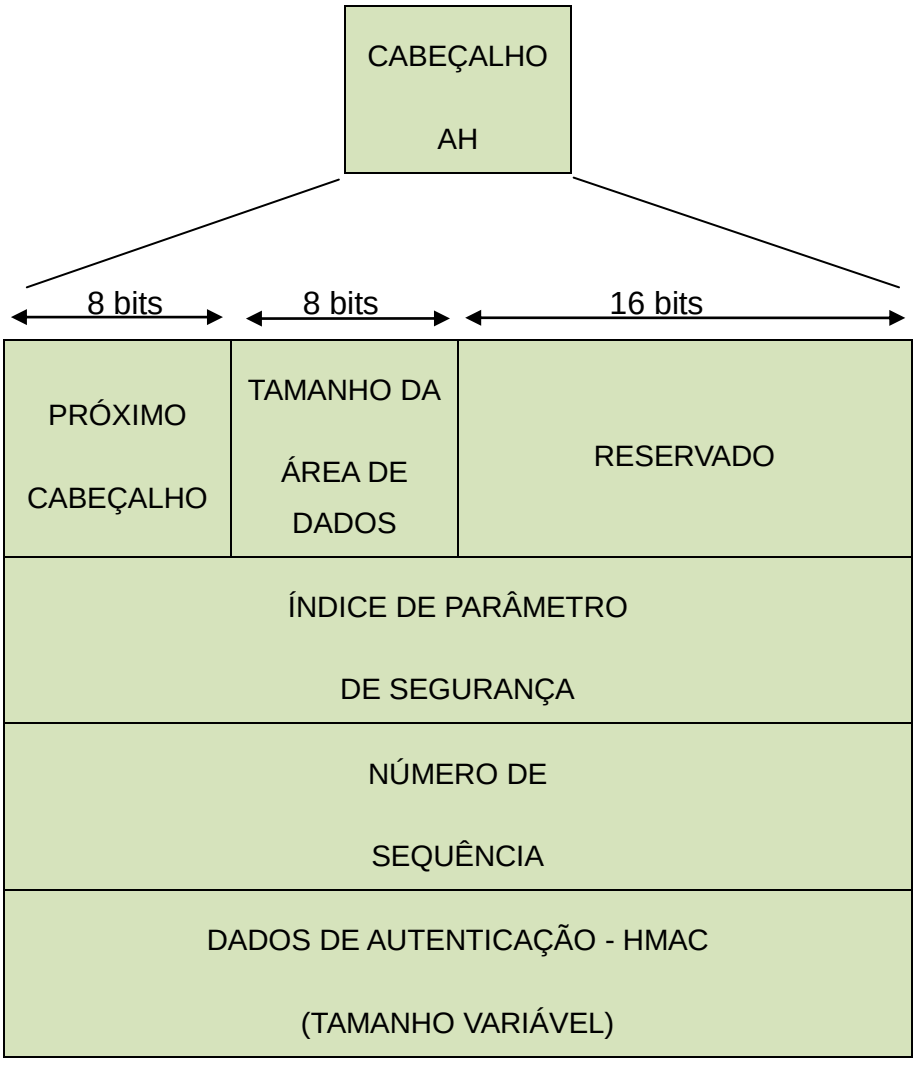


Figura 4: Segmentos do cabeçalho AH (Própria autoria)

No processo de integridade e autenticação, é usado um algoritmo hash que são seqüência de bits que transformam uma informação grande em pequena, normalmente utilizados para representar chaves criptografadas, no caso do AH é utilizado o HMAC (*Hashing Message Authentication*), que calculam um único valor, e este código de autenticação deve ser impossível de existir em outra mensagem.

Assim quando um host envia uma mensagem utilizando de SA, é associado a um código de autenticação e inserido no AH, e este quando chega ao destino é validado com outra função hash, e caso o código calculado não seja o mesmo, o pacote não é autenticado e então descartado, caso contrário, a autenticação é bem-sucedida.

8.2. Protocolo ESP

Como já mencionado, o protocolo ESP é mais empregado nas redes que se utilizam do IPSec, principalmente pelo fato de que este proporciona a privacidade, ou seja, confidencialidade. De forma geral, o ESP é mais complexo que o cabeçalho de autenticação, porém, pode ser trabalhado em conjunto com o AH para assim suprir a falta de autenticação dos datagramas *IP*.

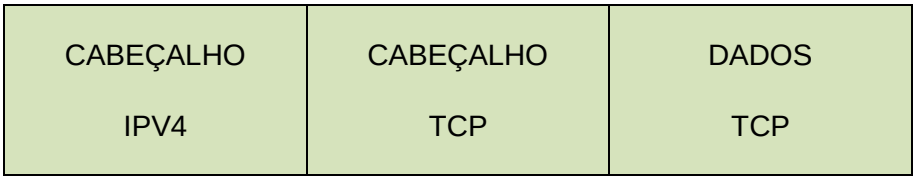
Novamente Peterson (2004) explica o que o protocolo ESP oferece:

> [...] ESP oferece confidencialidade, autenticação da origem dos dados, integridade sem conexões e um serviço antireplay [...] ***Peterson (2004)***

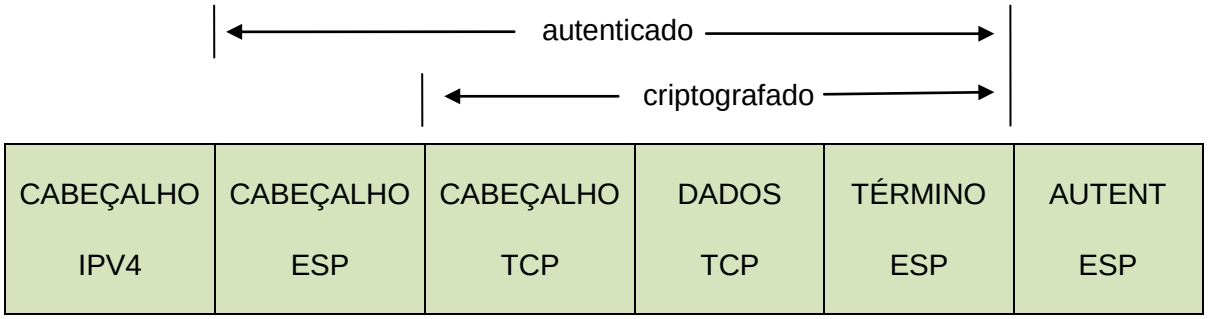
O ESP também opera nas formas transporte e túnel. No modo transporte o ESP é inserido como cabeçalho no datagrama *IP*, conforme a figura 5, antes da área de dados que será criptografada e opcionalmente autenticada, e logo após o cabeçalho *IP*, que neste mesmo é colocado um número 50 no campo protocol do

datagrama, revelando que o mesmo transporta o ESP. Entretanto, conforme Comer (2006), o protocolo acrescenta mais duas áreas no datagrama, o término ESP que acompanha na área criptografada e o campo autent ESP de tamanho variável que é alocado posterior a seção criptografada.

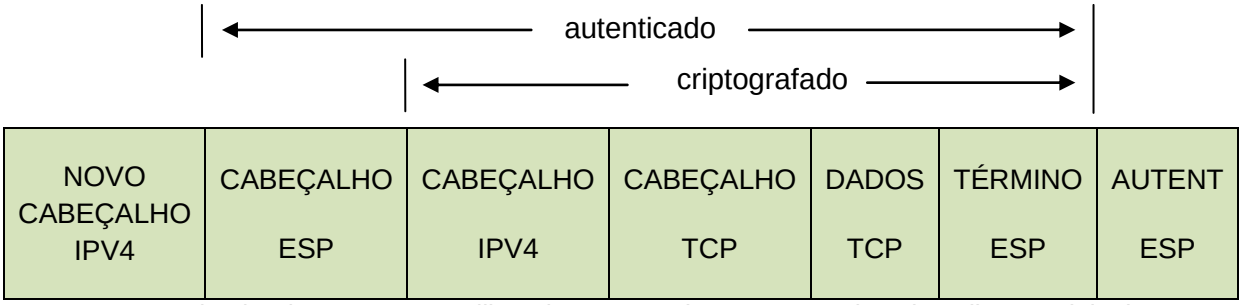
Em modo túnel, o ESP criptografa todo o pacote *IP*, e cria um novo cabeçalho *IP* externo, servindo, por exemplo, para ocultar os endereços de origem e destino reais, pois, no novo cabeçalho *IP* será armazenado os endereços dos roteadores (caso existam) da conexão, ficando assim os endereços originais dos cabeçalhos criptografados.



Datagrama *IP*



O mesmo datagrama acima, usando o ESP do IPSec e as partes criptografas e autenticadas – Modo transporte



O mesmo primeiro datagrama *IP*, utilizando o protocolo ESP antes do cabeçalho *IP* original e as partes criptografadas e autenticadas – Modo túnel

Figura 5: Pacote *IP* e os modos transporte e túnel no protocolo ESP no IPv4. (Própria autoria)

O ESP tem muitos itens iguais ao AH, porém reforma a ordem, por exemplo, no cabeçalho ESP, encontra-se o índice de parâmetro de segurança e o número de seqüência, ambos com 32 bits.

A área do término ESP consiste de um preenchimento opcional, um campo de tamanho de preenchimento que servem para determinar que o tamanho total do término ESP seja múltiplo de 4 bytes, e o próximo cabeçalho fazendo a mesma função que no AH. Acompanhado do término, o campo de dados de autenticação de quantidade variável que funciona como no AH, usando a função hash e autenticando desde o novo cabeçalho *IP* a todo o pacote *IP* criptografado, como pode ser observado na figura 6.

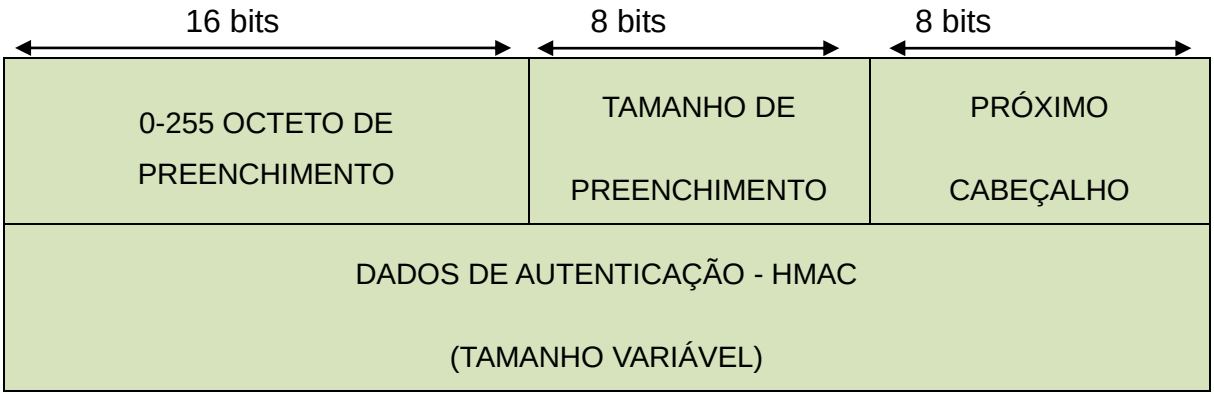


Figura 6: Área do término ESP e autenticação (HMAC). (Própria autoria)

Nos diferentes protocolos IPSec existe a dúvida de qual é melhor, com o ESP tendo a opção de autenticação, então não deveria existir o AH. Na função de autenticação o AH é melhor, pois verifica parte do cabeçalho que o ESP não faz, mas por tratar do sigilo e também a autenticação o ESP é mais usado. Contudo para aplicações críticas e que requerem muita segurança é recomendável utilizar o ESP em conjunto com o AH.

9. GERENCIAMENTO DE CHAVES

O gerenciamento de chaves do IPSec origina e difunde chaves secretas aos hosts ou roteadores. A distribuição das chaves pode ser manual ou automática, sendo que a manual envolve a configuração de cada sistema da rede, prático para ambientes estáticos e pequenos, e a distribuição automática que permite criar chaves quando é necessário, provocando melhor aproveitamento em ambientes grandes com sistemas distribuídos, o que gera configurações complexas e grande esforço.

Portanto, o mecanismo de chaves serve para criar, alterar e destruir chaves seguras e utiliza do protocolo hibrido IKE (*Internet Key Exchange*) que se originou pela união de três protocolos incompletos na visão do IETF e que fornece ao IPSec os seguintes serviços:

- Gera associação de segurança (SA) dinamicamente e sem o protocolo IKE é realizada manualmente toda a configuração;
- Troca de chaves quando estiverem por expirar são trocadas de forma dinâmica;
- Proteção contra ataques de repetição;
- Permite autenticação da origem através de certificados digitais.

O IKE pode estabelecer SAs para diferentes aplicações de segurança e protocolos, realizando assim um processo em que há diversos mecanismos de segurança e não são envolvidos os destinos e origens da conexão.

> É importante ressaltar que quando dois dispositivos IPSec necessitam se comunicar usando IPSec, eles primeiramente se autenticam, usando o IKE, e assim estabelecem uma Associação de Segurança IKE, também chamada SA IKE. ***Guimarães (2006)***

Esta associação de segurança do IKE apresentado por Guimarães (2006) é diferente da SA do IPSec, pois tem a finalidade de estabelecer o canal seguro para a conexão, para após configurar a interligação entre os dispositivos que desejam a conexão segura.

10. PRÁTICA DE IPSec

O IPSec foi fundamentado de forma teórica durante todo o andamento do trabalho, e explicado onde é possível implementá-lo, um exemplo é bloqueando o tráfego do protocolo ICMP, o “ping”, para máquinas que não possuem a segurança de *IP* implementada. Contudo a parte prática de como o IPSec pode ser utilizado pode ser demonstrado de uma maneira simples.

Em uma rede local interna, já é suficiente demonstrar a segurança de *IP* na prática. Neste exemplo foram utilizados três computadores, que são:

- MS-Windows 7 (chamado de Seven)
  - *IP* 192.168.0.123
- MS-Windows XP SP2 (chamado de XP 01)
  - *IP* 192.168.0.115
- MS-Windows XP SP2 (chamado de XP 02)
  - *IP* 192.168.0.118

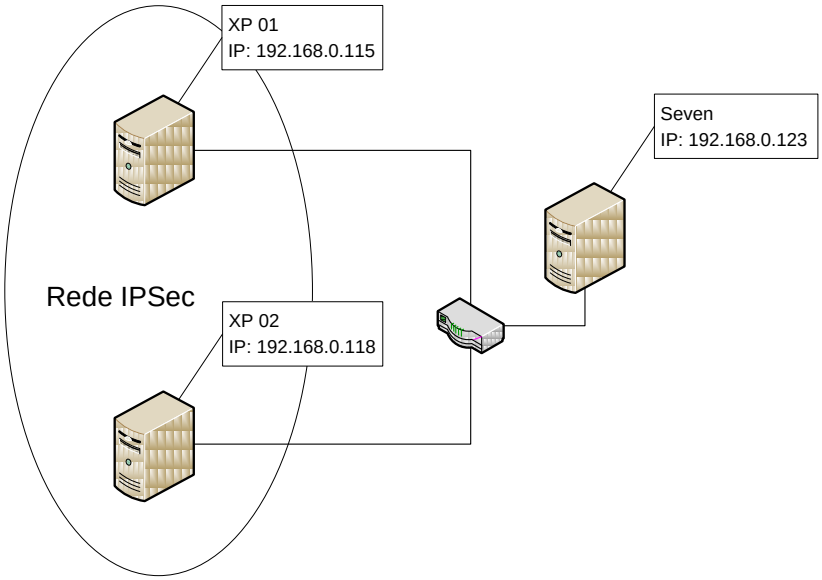


Figura 7: Esquema da rede IPSec na prática. (Própria autoria)

Nesta demonstração, será apresentado um exemplo em que três computadores da mesma rede que se conectam, foi implementado um canal IPSec em duas máquinas, afim de que possam trocar informações seguras de forma que algum terceiro computador, mesmo dentro da rede não seja capaz de identificar se essas estão ligadas, pois não obtêm resposta ao protocolo ICMP usado no ping.

Primeiramente vemos como as máquinas estão conectadas, utilizando o comando “ping”, usado para testar a conexão entre equipamentos em uma rede, e que usa o protocolo ICMP.

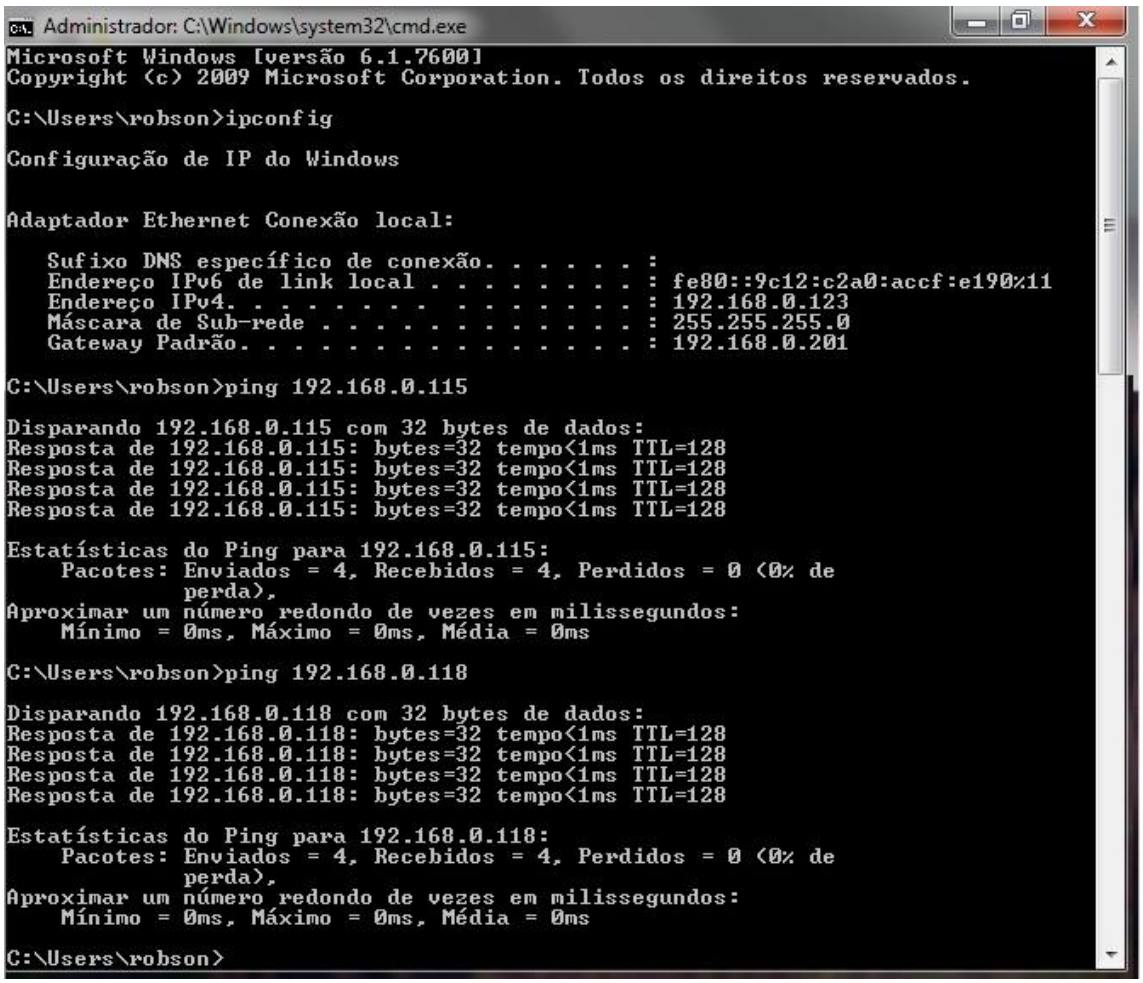


Figura 8: Seven efetuando ping em XP 01 e XP 02. (Própria autoria)

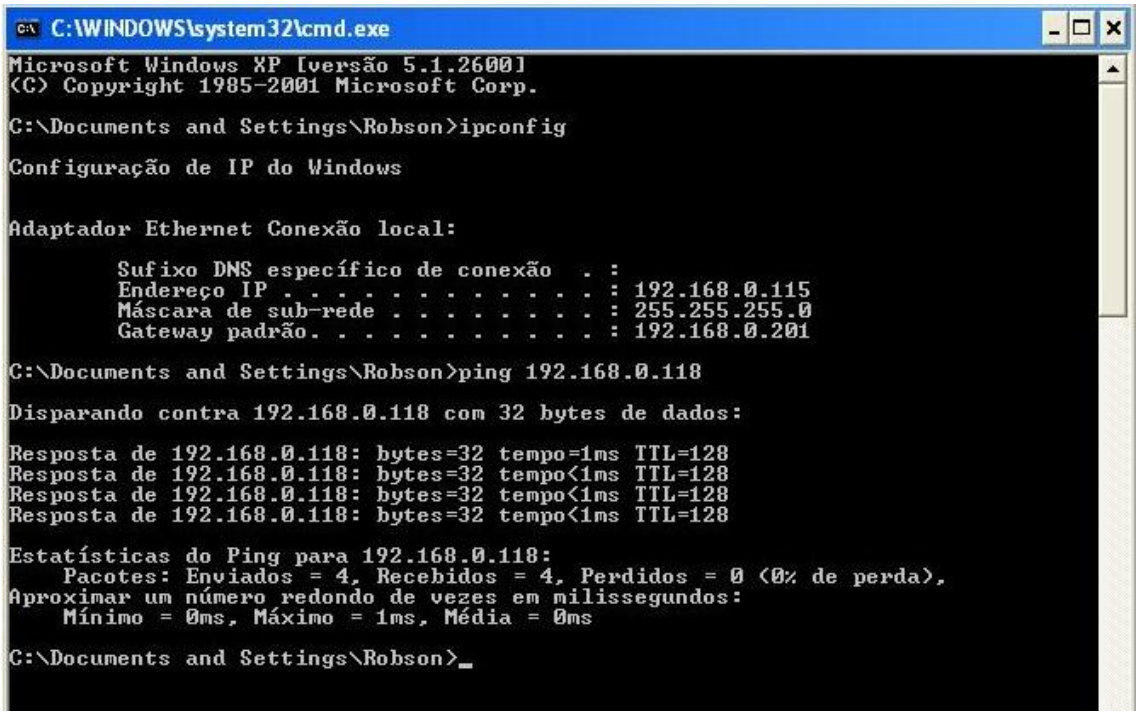


Figura 9: XP 01 efetuando ping em XP 02. (Própria autoria)

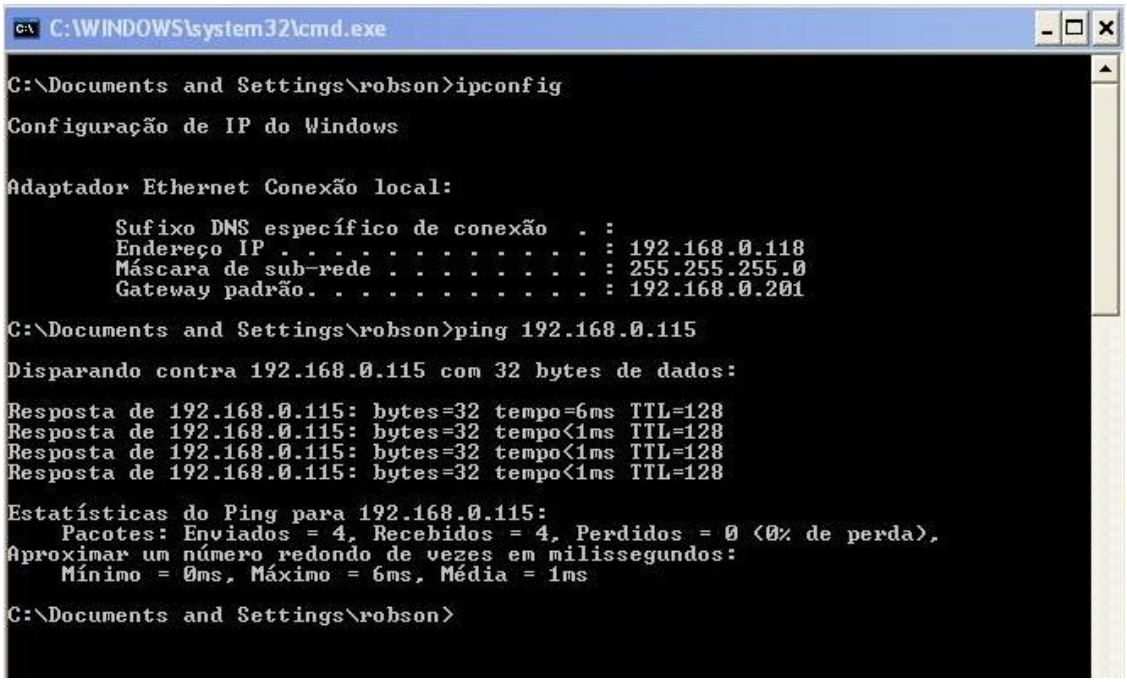


Figura 10: XP 02 efetuando ping em XP 01. (Própria autoria)

Para que o IPsec realmente funcione nesta rede, foram necessários alguns passos:

Passo 1. Em **Iniciar > Executar**, digita **secpol.msc**, que é o mesmo que **Iniciar > Configurações > Painel de Controle > Ferramentas Administrativas > Diretiva de segurança local.**

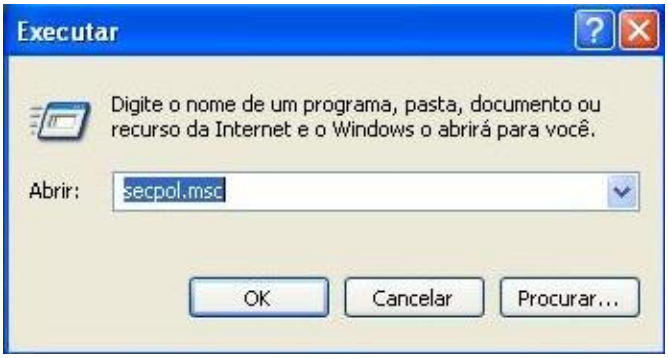


Figura 11: Janela Executar (Windows XP). (Própria autoria)

Passo 2. Na janela **Configurações locais de segurança**, clique com o botão direito do mouse em **Diretivas de segurança *IP*** em computador local e **Criar diretiva segurança *IP*.**

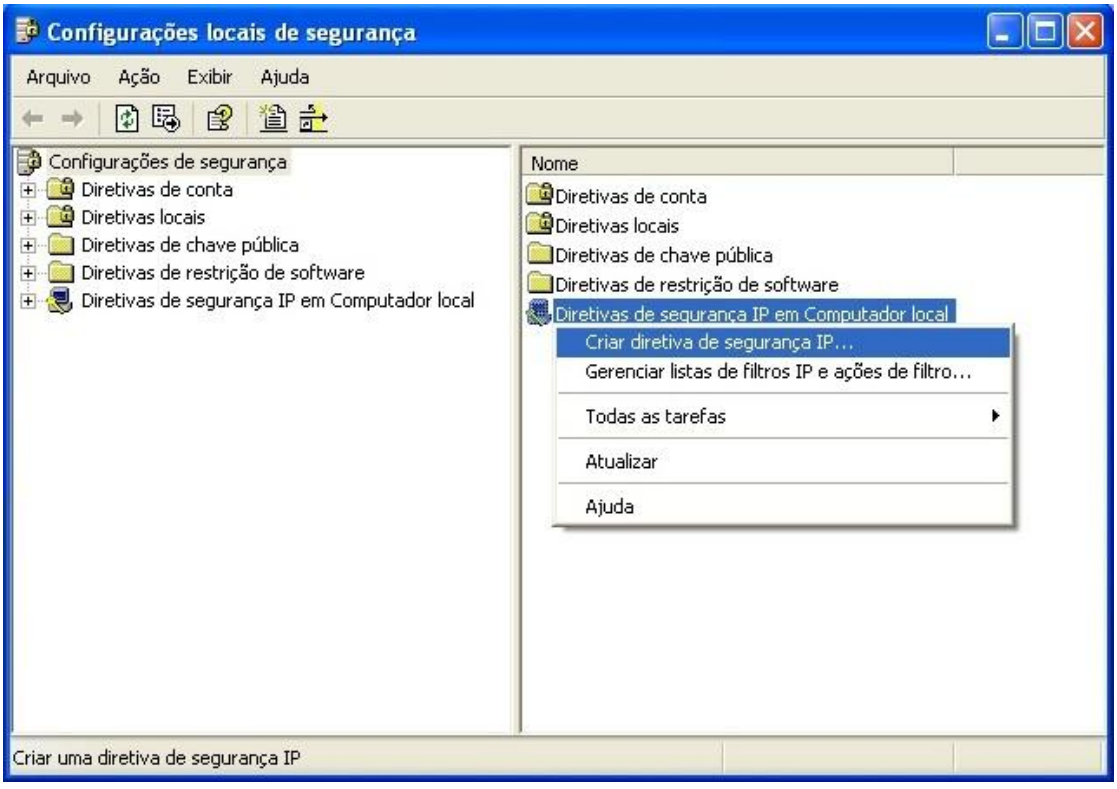


Figura 12: Janela Configurações locais de segurança. (Própria autoria)

Passo 3. Na janela **Assistente de diretiva de segurança *IP*** clicar em **Avançar** e escolher um nome e uma breve descrição para sua diretiva e clicar em **Avançar** novamente.

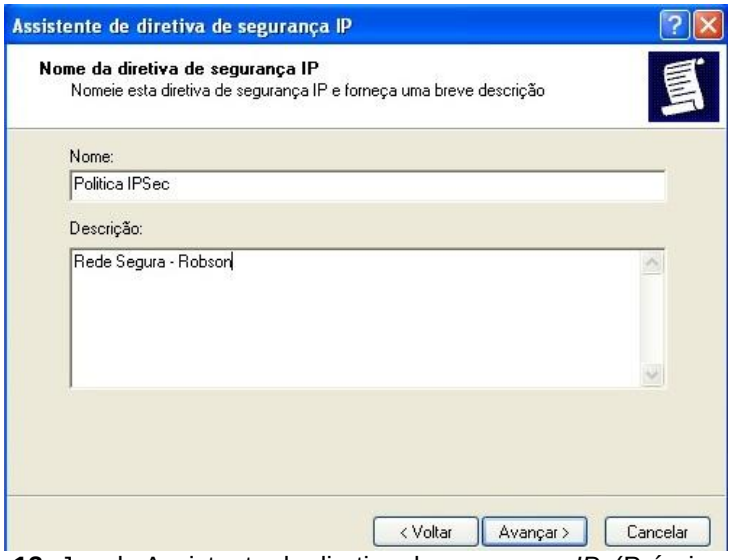


Figura 13: Janela Assistente de diretiva de segurança *IP*. (Própria autoria)

Passo 4. Desmarcar a opção **Ativar a regra de resposta padrão**, pois, só queremos a nossa regra em ação clicar em **Avançar** e em seguida **Concluir**. Não foi usado nenhum tipo de assistente do Windows, portanto, desmarque qualquer caixa que sugere a usar o assistente.

Passo 5. Em **Propriedades de <nome da diretiva>** clica em adicionar.

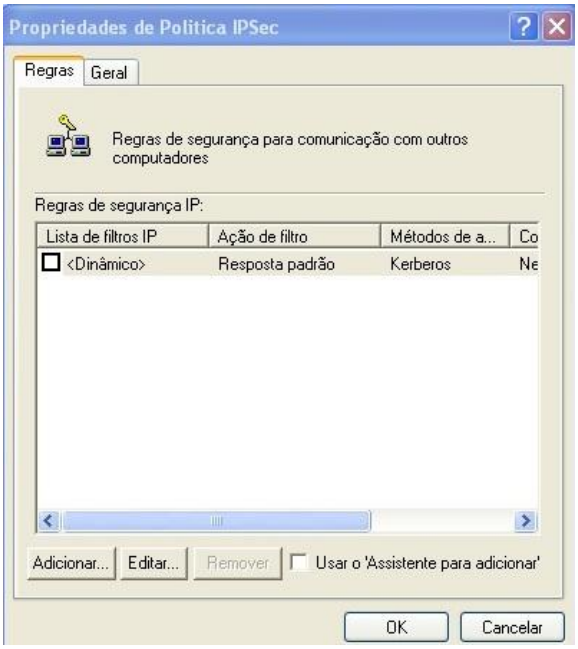


Figura 14: Janela Propriedades de <nome da diretiva>. (Própria autoria)

Passo 6. Na janela **Propriedades de nova regra**, ignore os filtros já existentes e clique para criar novo filtro utilizando o botão **Adicionar**.

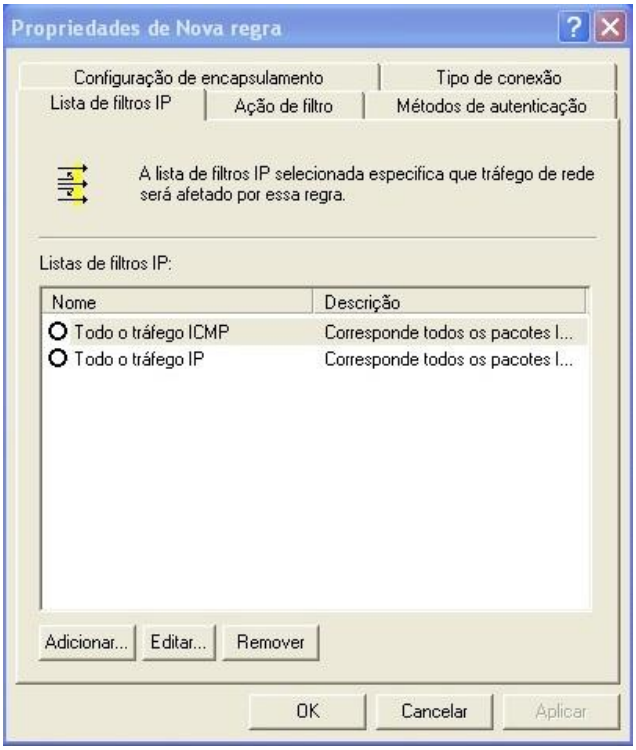


Figura 15: Janela Propriedades de nova regra. (Própria autoria)

Passo 7. Em **Lista de filtros *IP***, colocar um nome e uma descrição para o filtro e clicar no botão **Adicionar**.

Figura 16: Janela Lista de filtros *IP*. (Própria autoria)

Passo 8. Na janela **Propriedades de filtro**, na guia **Endereçamento**, colocar endereço de origem: **Meu endereço *IP*** e em destino deixar **Qualquer endereço *IP***.

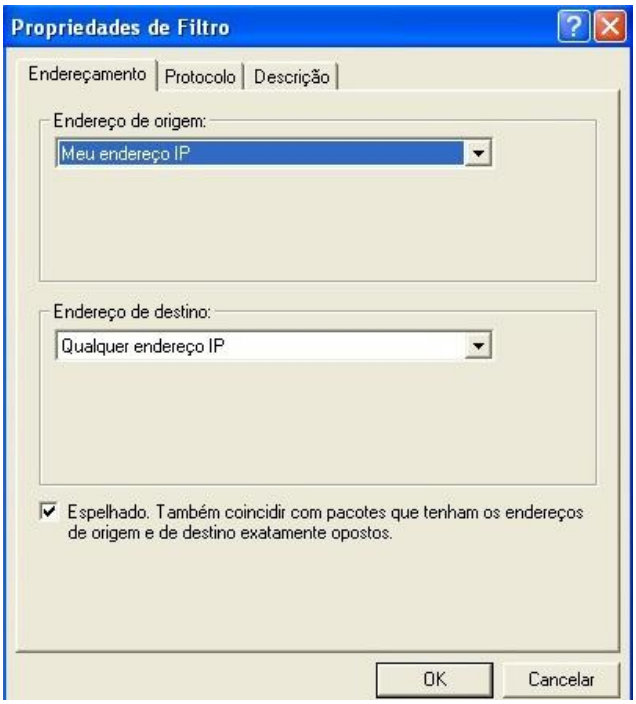


Figura 17: Janela Propriedades de filtro; Guia Endereçamento. (Própria autoria)

Passo 9. Na guia **Protocolo** selecionar **ICMP** e breve descrição na seguinte guia. Clicar em **OK** e **OK** novamente.

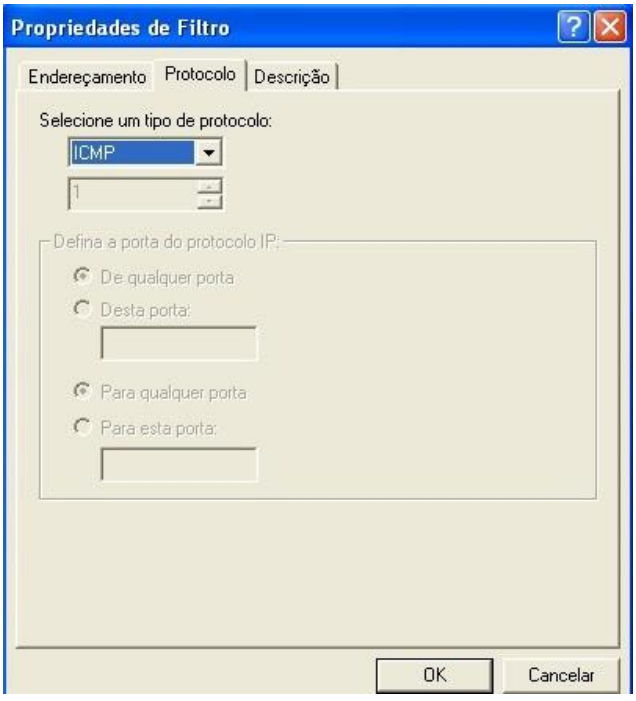


Figura 18: Janela Propriedades de filtro; Guia Protocolo. (Própria autoria)

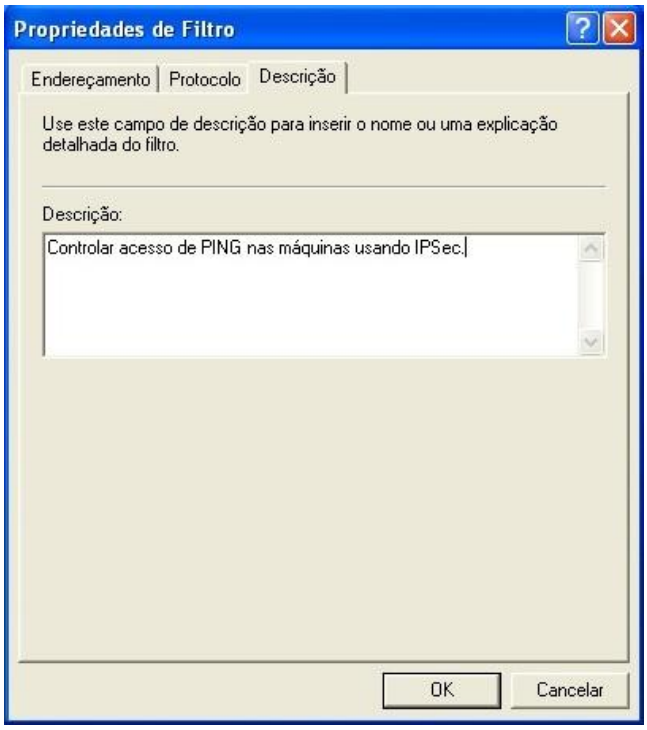


Figura 19: Janela Propriedades de filtro; Guia Descrição. (Própria autoria)

Passo 10. Voltando na janela **Propriedades de nova regra**, abrir na guia **Ação de filtro** e clicar no botão **Adicionar** para selecionar qual ação o filtro criado anteriormente irá realizar.

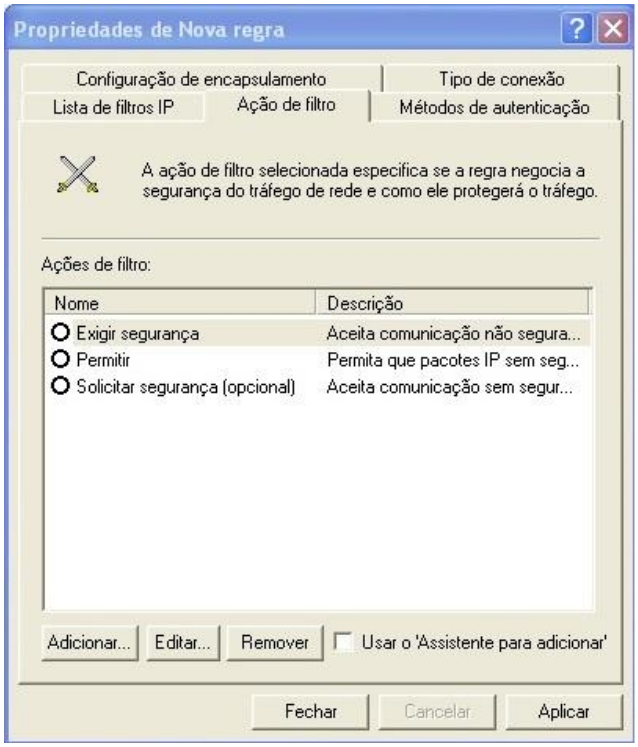


Figura 20: Janela Propriedades de Nova regra; Guia Ação de filtro. (Própria autoria)

Passo 11. Entre as opções:

- Permitir
- Bloquear
- Negociar segurança

Selecionar a última opção, pois, assim será possível verificar o IPSec em funcionamento e bloqueando o protocolo ICMP para máquinas que não tem acesso.

Figura 21: Janela Propriedades de Ação de filtro; Guia Método de segurança. (Própria autoria)

Passo 12. Clicar no botão **Adicionar** e selecionar **Criptografia e integridade** e clicar no botão **OK**. Na guia geral poderá ser descrita a tarefa do filtro.

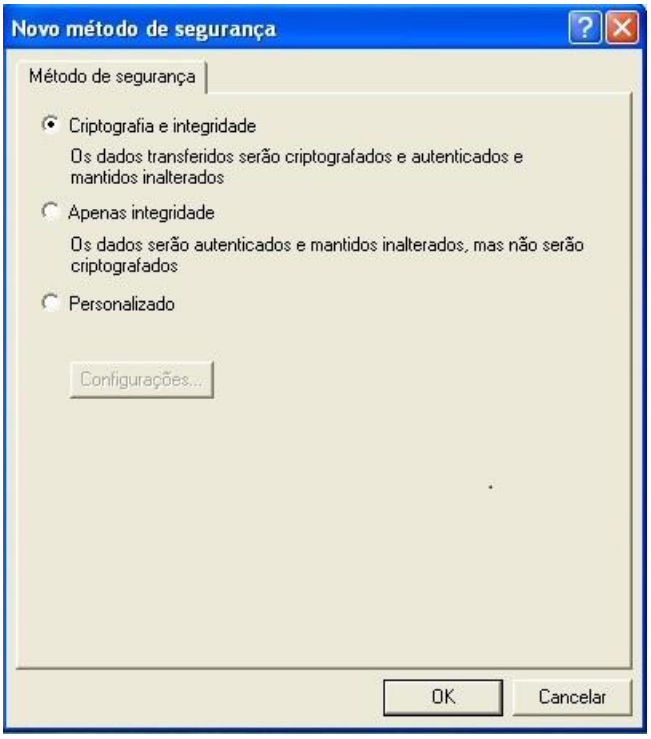


Figura 22: Janela Novo método de segurança. (Própria autoria)

Passo 13. Retornando outra vez na janela **Propriedade de nova regra** e na guia **Métodos de autenticação**, clicar no botão **Adicionar** e abrirá uma nova janela onde será criado um novo método de autenticação além do Kerberos.

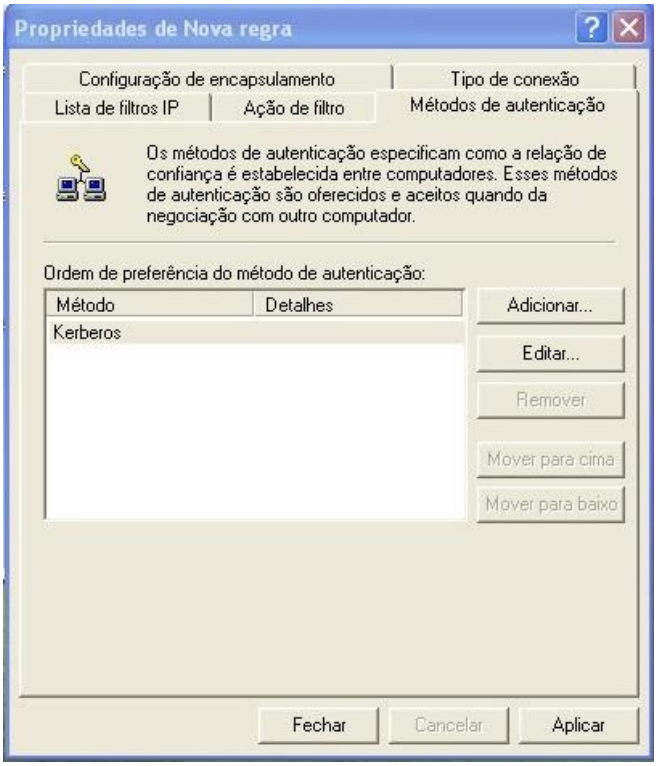


Figura 23: Janela Propriedades de Nova regra; Guia Métodos de autenticação. (Própria autoria)

Passo 14. Na janela **Propriedades de Novo método de autenticação**, selecionar **Usar esta seqüência de caracteres (chave pré-compartilhada)** e digitar a palavra ou frase desejada.

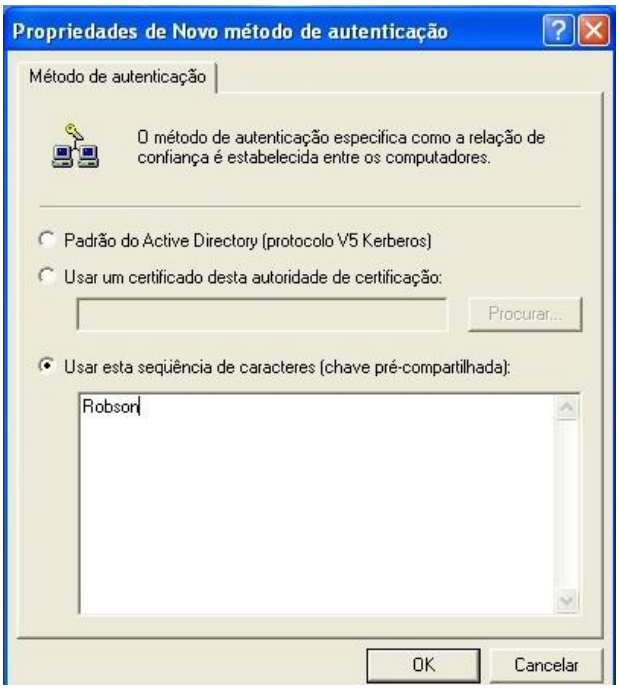


Figura 24: Janela Propriedades de Novo método de autenticação. (Própria autoria)

Passo 15. Novamente na janela **Propriedades de nova regra**, e nas guias **Configuração de encapsulamento** e **Tipo de conexão** deixar o padrão. Na guia **Lista de filtro *IP*** selecionar o filtro criado e aplicar e então clicar em **OK**.

Passo 16. Na janela principal, aparecerá a política criada, clicar com o botão direito do mouse sobre ela e selecionar **Atribuir** para habilitar a política.

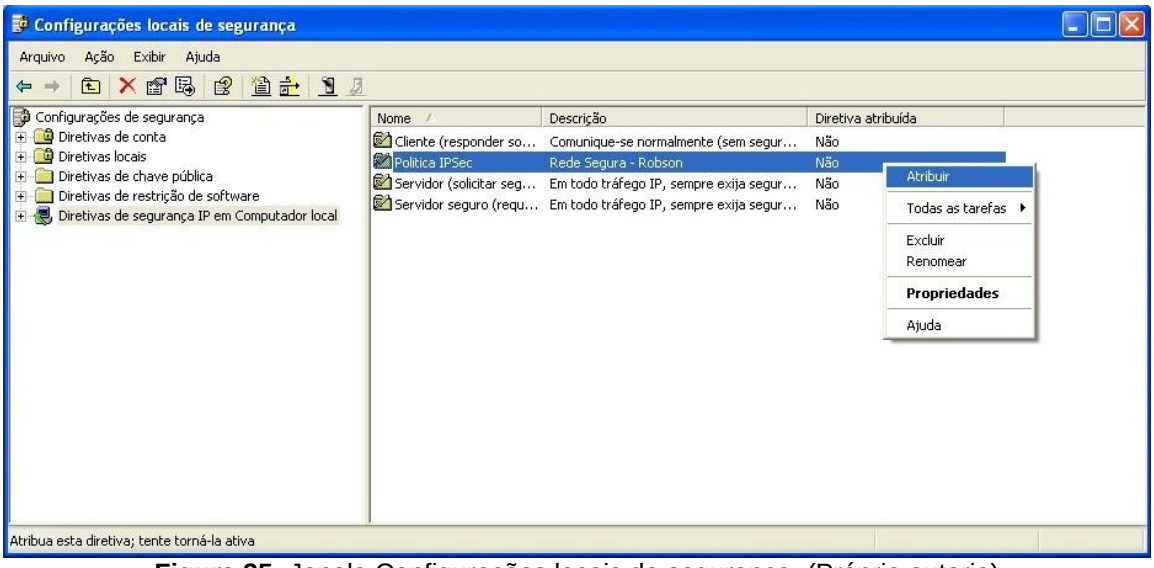


Figura 25: Janela Configurações locais de segurança. (Própria autoria)

Passo 17. Para que seja efetiva a criação desta diretiva de segurança *IP*, o mesmo processo declarado acima deve ser realizado nas outras máquinas da rede, criando assim o canal seguro IPSec.

10.1. IPSec em Funcionamento

Após criar as diretivas de IPsec, vejamos como funciona aplicada na rede local descrita acima.

Etapa 1. Depois de atribuir a diretiva política IPSec em nosso exemplo prático, no caso a XP 02, vemos que esta continua realizando o ping na XP 01 e na Seven, porém está negocia a segurança e não mostra efetivamente os disparos, mas sim que os pacotes foram realmente enviados.

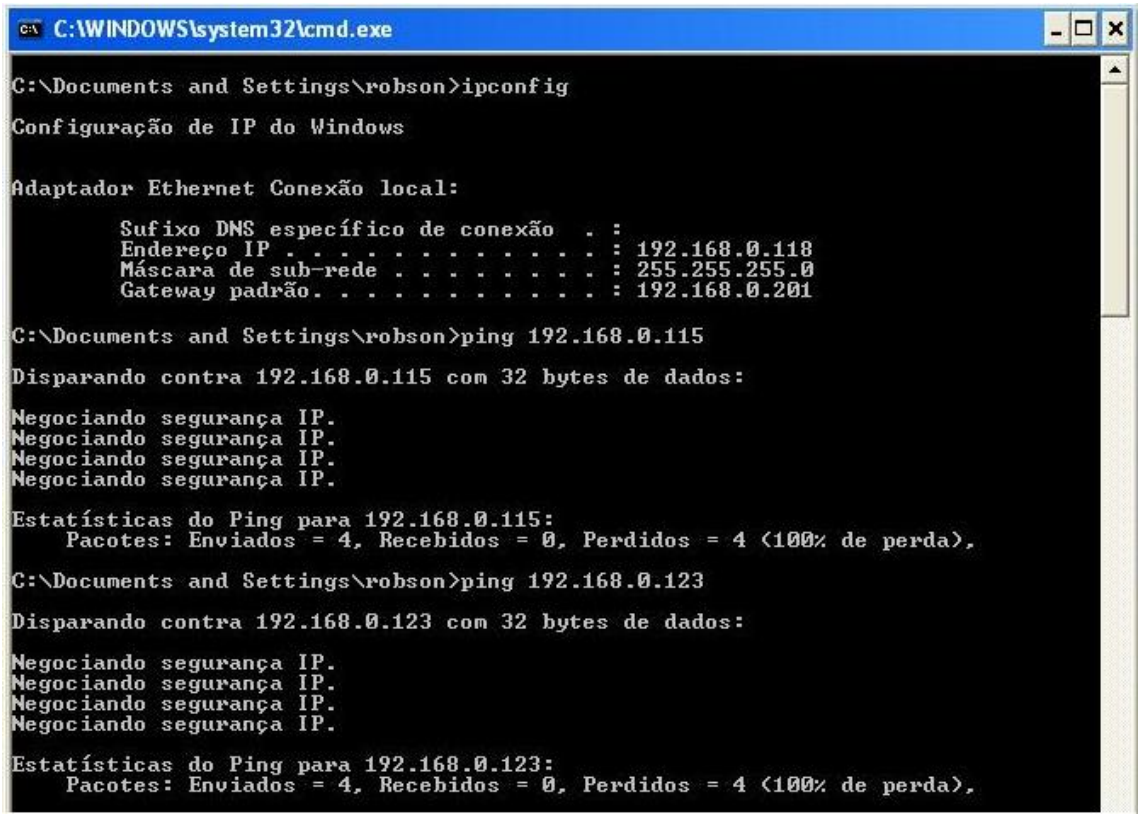


Figura 26: Prompt de comando da Maquina XP 02. (Própria autoria)

Etapa 2. Com a diretiva na XP 02 atribuída, a máquina XP 01 não consegue realizar o ping na XP 02, o que se entende que está desligada, fora da rede, ou não existe na rede. Contudo na Seven continua normalmente.

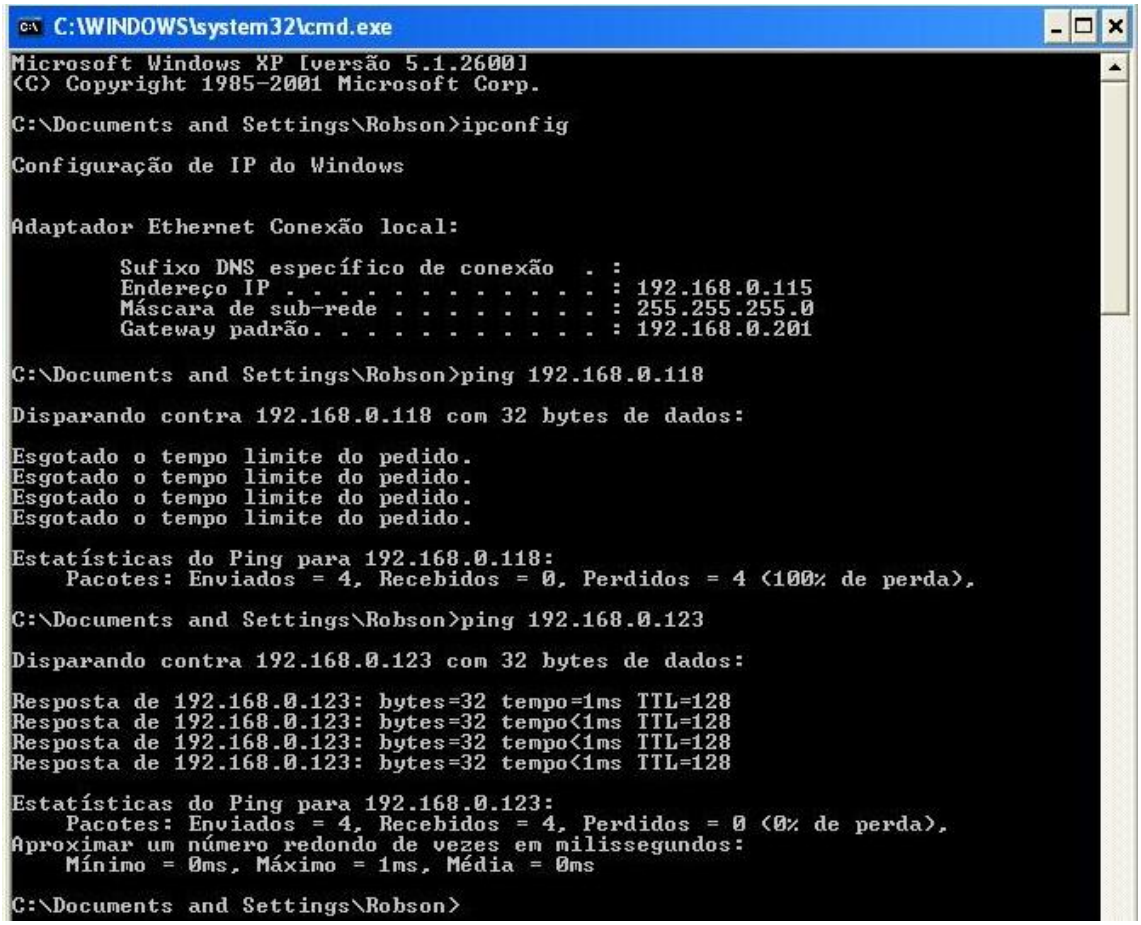


Figura 27: Prompt de comando da Maquina XP 01. (Própria autoria)

Etapa 3. O próximo passo é atribuir a mesma diretiva para XP 01, com isso, as máquinas XP 01 e XP 02 estariam em um canal IPSec de comunicação. Observa-se que a partir deste momento os computadores realizam o ping normalmente entre elas, mas a Seven que está fora da diretiva IPSec não “enxerga” mais elas.

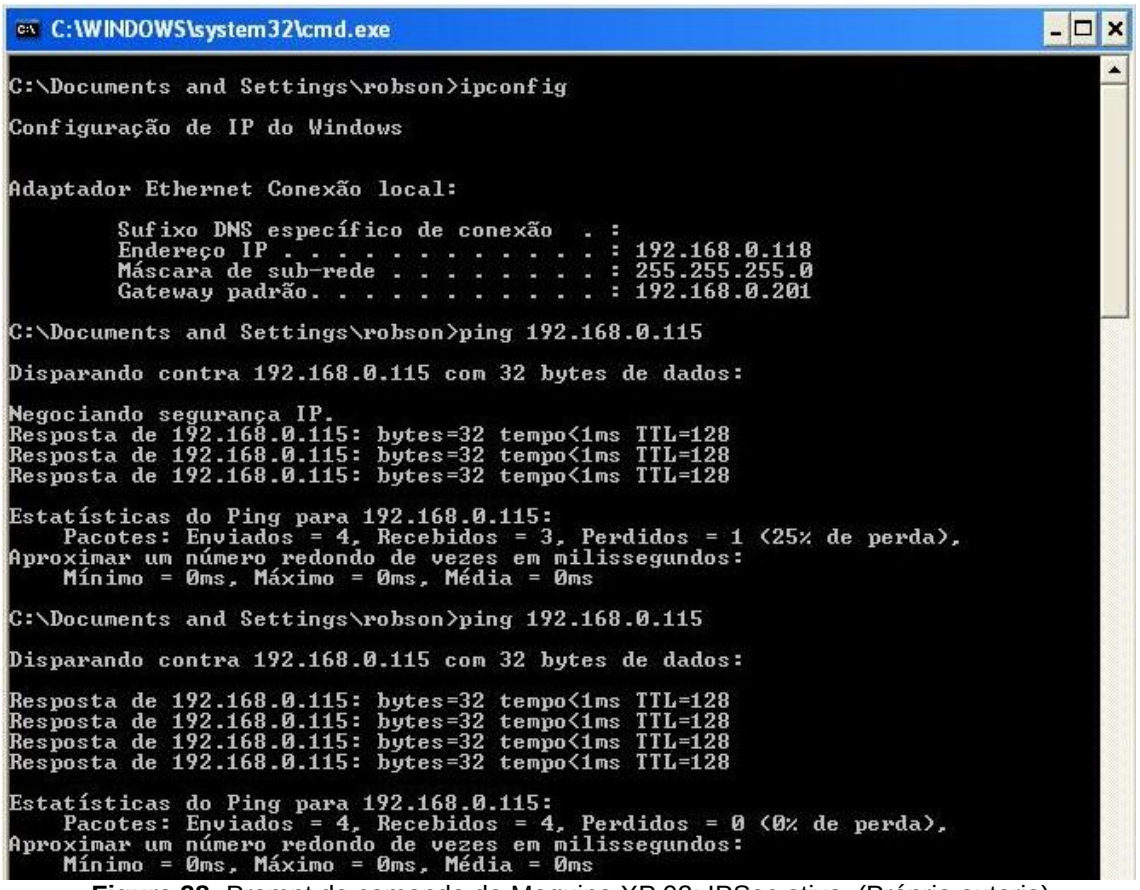


Figura 28: Prompt de comando da Maquina XP 02; IPSec ativo. (Própria autoria)

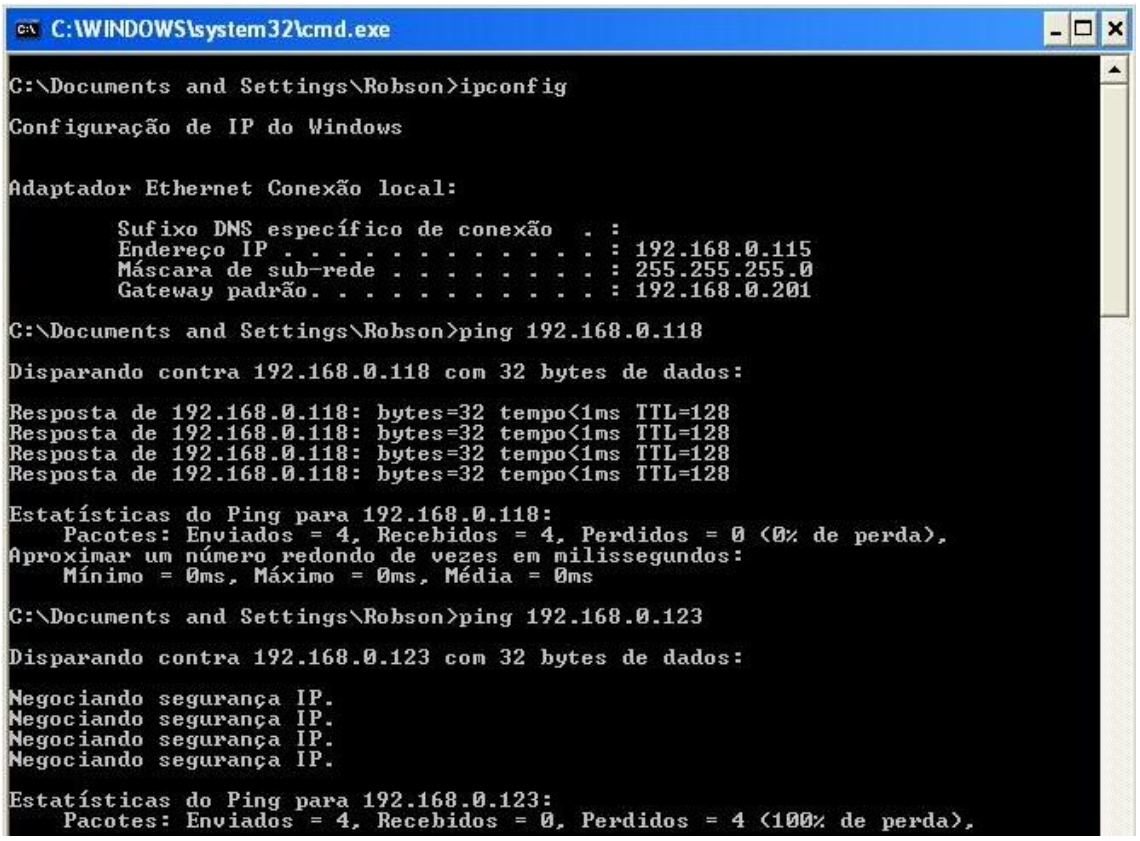


Figura 29: Prompt de comando da Maquina XP 01; IPSec ativo. (Própria autoria)

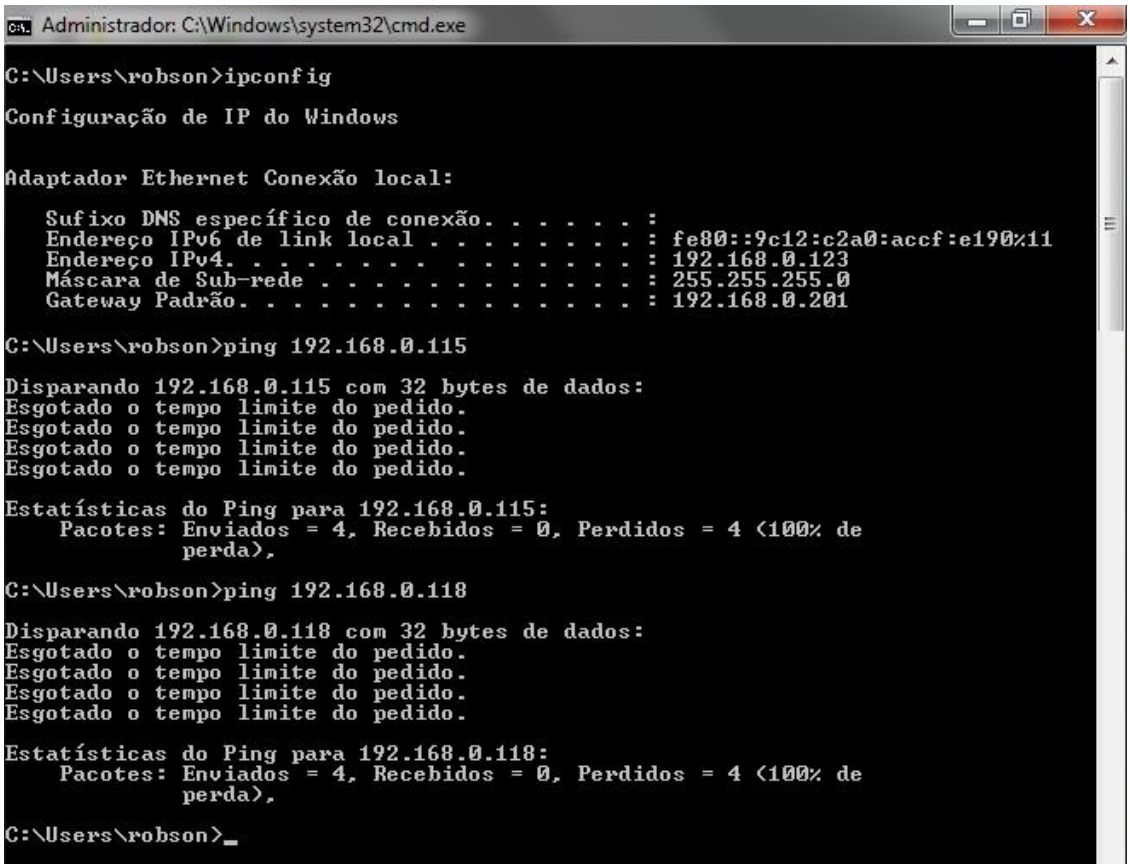


Figura 30: Prompt de comando da Maquina Seven; IPSec ativo. (Própria autoria)

Etapa 4. Com esse exemplo, comprova-se que o IPSec é funcional ao que promete, mesmo neste caso prático básico do protocolo ICMP. A segurança de *IP* garante o filtro ativo para computadores permitidos e o não acesso aos que tentam “invadir” a rede que se enquadra na política de segurança de *IP*.

11. CONSIDERAÇÕES FINAIS

Observou-se que durante o andamento deste trabalho, um pouco da história é resgatada. O porquê de o IPSec ser criado e o que essa união de protocolos de segurança traz de vantagens para a evolução das redes seguras com criptografia no mundo todo.

Conclui-se neste trabalho que o IPSec implementado em uma rede privada provê muitas vantagens, entre elas, a empresa conter gastos, como alugar uma linha de *Internet* dedicada para se conectar com suas filias. Com a vantagem da possível criptografia existente na rede, torna-se mais difícil a quebra de sigilo e divulgação dos dados para a rede aberta.

A implementação de modo prático do IPSec é simples, apenas definir uma política de segurança IPSec na rede, e ainda é possível utilizar de diversos filtros e modos de negociar a segurança e a autenticação, gerando uma rede de tráfego altamente segura.

Os objetivos da segurança de IPSec são basicamente proteger os dados dos pacotes *IP* e garantir a defesa contra ataques de redes. Para que isso seja efetivo, alem dos pacotes autenticados na rede, é indispensável o uso da criptografia, utilizando, por exemplo, o ESP em modo túnel e o gerenciamento de chaves, para assim proteger de forma geral os hosts de redes privadas, extranets, domínios, sites e outros.

Espera-se que a idéia da rede privada utilizando o IPSec continue a se espalhar e que cada vez mais seja aplicada, tornando assim, as redes mais seguras e diminuindo o número de ataques de tantos diferentes tipos que as empresas sofrem atualmente.

REFERÊNCIAS BIBLIOGRÁFICAS

AUGUSTO Fabio. **Configurando o IPSec no Windows Server 2008**. Disponível em: <*http://fabiozibiani.wordpress.com/2011/01/04/configurando-o-ipsec-no-windows-server-2008/#comment-3388*>. Acessado em 09 de fevereiro de 2012.

BATTISTI, Júlio. **Tutorial de TCP/*IP* – Parte 18 – Introdução ao IPSec**. Disponível em: <*http://www.juliobattisti.com.br/artigos/windows/tcpip_p18.asp*>. Acessado em 28 de janeiro de 2012.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de computadores**. Porto Alegre: Bookman, 2009. p. 366-368.

COMER, Douglas E. **Interligação de redes com TCP/*IP*, vol. 1 princípios, protocolos e arquitetura**; Tradução Daniel Vieira. Rio de Janeiro: Elsevier, 2006 – 6ª reimpressão. p. 358-363.

DIAS, Diego Sousa. **Serviços Orientados à Conexão e Sem Conexão**. Disponível em: <*http://pt.scribd.com/diego_dias_30/d/49637772/27-Servicos-Orientados-a-Conexao-e-Sem-Conexao*>. Acessado em 22 de abril de 2012.

GUIMARÃES, Alexandre Guedes. **Segurança com VPNs.** Rio de Janeiro: Brasport, 2006. p. 100-122.

KUROSE, James F.; ROSS, Keith W. **"Redes de computadores e a *Internet*: uma abordagem top-down"**. São Paulo: Pearson Addison Wesley, 2010 – 5ª reimpressão. p. 526-531.

MARTINS, Dêner Lima Fernandes. **Redes privadas virtuais com IPSec**. Disponível em: <*http://www.cic.unb.br/~pedro/trabs/vpn.pdf*>. Acessado em 06 de maio de 2012.

PETERSON, Larry L. **Redes de computadores: uma abordagem de sistemas;** Tradução de Daniel Vieira. Rio de Janeiro: Elsevier, 2004 – 3ª reimpressão. p. 448-450

SHINDER, Deb. **Get IT Done: Create custom IPSec configurations for Windows XP**. Disponível em: <*http://www.techrepublic.com/article/get-it-done-create-custom-ipsec-configurations-for-windows-xp/5034335*>. Acessado em 29 de abril de 2012.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Prática**. 4ª Edição. São Paulo: Pearson Prentice-Hall, 2008 –. p. Cap. 16 p. 348-377.

STALLINGS, William. **Redes e sistemas de comunicação de dados: teoria e aplicações corporativas.** Rio de Janeiro: Elsevier, 2005 – 4ª reimpressão. p. 397-401.

TANENBAUM, Andrew S. **Redes de Computadores**; Tradução Vanderberg D. de Souza. Rio de Janeiro: Elsevier, 2003 – 17ª reimpressão. p. 820-829.

TECHNET Microsoft. **IPSec (*Internet* Protocol Security)**. Disponível em: <*http://technet.microsoft.com/pt-br/library/cc783420(WS.10).aspx*>. Acessado em 08 de abril de 2012.

TECHNET Microsoft. **Protocolos de Núcleo de TCP/*IP***. Disponível em: <*http://technet.microsoft.com/pt-pt/library/cc781096(v=ws.10)*>. Acessado em 08 de abril de 2012.

TECHNET Microsoft. **User Datagram Protocol (UDP).** Disponível em: <*http://technet.microsoft.com/pt-pt/library/cc785220(v=ws.10)*>. Acessado em 22 de maio de 2012.

TS'O, Theodore; FRASER, Barbara Y. ***IP* Security Protocol (IPSec)**. Disponível em: <*http://datatracker.ietf.org/wg/ipsec/charter/*>. Acessado em 22 de maio de 2012.

GLOSSÁRIO

Banco de dados de associação de segurança (SAD). Banco de dados do IPSec que contêm conjuntos de parâmetros de associações de segurança, com o objetivo de manter as informações para usos futuros em entras SAs.

By-pass. Desvio dos pacotes na rede para encontrar um caminho diferente a fim de encontrar o mesmo destino.

Certificados digitais. Arquivo de computador que contêm os dados da empresa, pessoa física ou entidade a qual gerou o certificado. Serve para saber se a pessoa que o emite é mesmo quem diz ser, através da chave pública. Esta chave pública é a responsável por criptografar dados para enviar ao dono do certificado e a chave privada é aquela que descriptografa a informação enviada.

Datagrama. Unidade de transmissão de dados que contem um cabeçalho com informações dos endereços de origem e destino e a real parte dos dados que serão entregues para o destinatário.

DES (Data Encryption Standard). Método de criptografia. Entre os primeiros algoritmos de criptografia aberto no mercado, atualmente dado com inseguro, porém melhor na forma 3DES.

Host. Hospedeiro. Qualquer computador ou dispositivo conectado a uma rede, que oferecer informações, recursos ou serviços. Obrigatoriamente todo host tem de ser representado por um endereço *IP* na rede.

IETF (*Internet* Engineering Task Force). Comunidade internacional que se preocupa com a arquitetura da *Internet* e seu funcionamento de forma perfeita. Ela propõe soluções para problemas na utilização da *Internet* e padronizações dos protocolos e tecnologias nelas abrangidas.

Kerberos. Protocolo de rede. Permite em uma rede insegura, comunicação identificada, individual e segura. Garante a integridade dos dados e utiliza da criptografia simétrica.

LAN (Local Area Network). Rede local, uma rede de computadores com a finalidade de troca de dados, se conectando entre si. Cobrem um espaço de no máximo km.

Overhead. Sobrecarga de informações, incluindo, de memória, processamento e outros. Como conseqüência o desempenho do host é diminuído drasticamente.

PDU (Protocol Data Unit). Bloco de dados que recebem outros blocos da camada superior e adiciona seus cabeçalhos, gerando o processo de encapsulamento. O PDU pode ser chamado de pacote, entretanto, apenas na camada de rede.

Roteador. Encaminhador. Equipamento de informática que serve para conduzir os pacotes em quais caminhos da rede deve percorrer para chegar ao destino.

Streaming. Conteúdo multimídia, vídeo e som.

WAN (Wide Area Network). Rede de longa distância compreende uma rede de computadores que estabelece em grande área geográfica, como um país ou continente.