ATIVIDADE DE LABORATÓRIO V - SEGURANÇA IP (IPSEC)

Victor Dallagnol Bento
Universidade Federal de Santa Maria
Santa Maria - RS, Brasil
victor.bento@ecomp.ufsm.br

I. INTRODUÇÃO

Na quinta atividade de laboratório o professor nos apresentou conceitos sobre o protocolo de segurança IP, o IPSec. Posteriormente foram incumbidas tarefas como criar uma associação de segurança entre dois computadores, ativar a configuração IPSec para a interface de comunicação e verificar a segurança da comunicação utilizando um analisador de pacotes, no nosso caso, o WireShark.

II. DESENVOLVIMENTO TEÓRICO

Pela necessidade de proteger a infraestrutura de rede contra monitoramento e controle não autorizados de tráfego e pela necessidade de garantir tráfego de usuário para usuário final usando mecanismos de autenticação e criptografia, foram incluídas a autenticação e a criptografia como recursos de segurança necessários no IPv6. Estes recursos também são compatíveis com o IPv4, significando assim que os fornecedores podem começar a oferecer esses recursos e possuir os mesmos em seus produtos, tornando o IPsec um conjunto de padrões da Internet.

O IPsec oferece a capacidade de proteger as comunicações em uma LAN, nas WANs públicas e privadas e na Internet. Alguns exemplos do seu uso seriam: Conectividade segura de filiais pela Internet, acesso remoto seguro pela Internet, estabelecer conectividade de extranet e intranet com parceiros e melhorar a segurança do comércio eletrônico.

O principal recurso do IPsec que permite o suporte a esses aplicativos variados é que ele pode criptografar e/ou autenticar todo o tráfego no nível de IP. Fazendo com que todos os aplicativos distribuídos (incluindo login remoto, cliente/servidor, email, transferência de arquivos, acesso à Web, etc) possam ser protegidos. Quando o IPsec é implementado em um firewall ou roteador por exemplo, ele fornece uma segurança forte que pode ser aplicada a todo o tráfego que cruza o perímetro. Nesse caso o IPSec é resistente a desvios se todo o tráfego externo precisar usar IP e se o único meio de entrada for o firewall.

O IPsec está abaixo da camada de transporte (TCP, UDP) e, sendo transparente para os aplicativos, não havendo a necessidade de alterar o software em um sistema de usuário ou servidor quando o IPsec é implementado no firewall ou no roteador. Mesmo se o IPsec for implementado em sistemas finais, o software da camada superior, incluindo aplicativos, não será afetado. Além de oferecer suporte aos usuários finais e proteger sistemas e redes locais, o IPsec pode desempenhar um papel vital na arquitetura de roteamento necessária para a interconexão de redes.

O IPsec abrange três áreas funcionais: autenticação, confidencialidade e gerenciamento de chaves. A melhor maneira de compreender o escopo do IPsec é consultar a versão mais recente do roteiro do documento IPsec, que, até o momento, é o RFC 6071. Os documentos podem ser categorizados nos seguintes grupos:

- Arquitetura: Abrange os conceitos gerais, requisitos de segurança, definições e mecanismos que definem a tecnologia IPsec.
- Cabeçalho de Autenticação (AH): É um cabeçalho de extensão para fornecer autenticação de mensagem. Como a autenticação de mensagens é fornecida pelo ESP, o uso de AH é obsoleto.
- Encapsulating Security Payload (ESP): Tem por objetivo adicionar autenticação e confidencialidade, a fim de garantir que somente os destinatários autorizados possam acesso ao conteúdo do pacote
- Internet Key Exchange (IKE): Esta é uma coleção de documentos descrevendo os principais esquemas de gerenciamento para uso com o IPsec.
- Algoritmos de criptografia: essa categoria engloba um grande conjunto de documentos que definem e descrevem algoritmos criptográficos para criptografia, autenticação de mensagem, funções pseudo-aleatórias (PRFs) e troca de chave criptográfica.
- Outros: Há uma variedade de outros RFCs relacionados ao IPsec, incluindo aqueles que lidam com política de segurança e conteúdo de base de informações de gerenciamento (MIB).

O IPsec fornece serviços de segurança na camada IP, permitindo que um sistema selecione os protocolos de segurança necessários, determine o(s) algoritmo(s) a usar para o(s) serviço(s) e implemente as chaves criptográficas necessárias para fornecer os serviços solicitados. Dois protocolos são usados para fornecer segurança: O protocolo AH, que implementa os serviços de segurança de integridade e autenticação dos dados, garantindo que o pacote é o correto e que não houve nenhuma alteração nos dados enviados; o protocolo ESP, que é um protocolo combinado de criptografia/autenticação, implementando os serviços de autenticação dos dados e confidencialidade, assim só os destinatários autorizados teriam acesso a informação. O AH e o ESP suportam dois modos de uso: transporte e modo de túnel.

O modo de transporte fornece proteção principalmente para protocolos de camada superior. Normalmente, o modo de transporte é usado para comunicação de ponta a ponta entre dois hosts (por exemplo, um cliente e um servidor ou duas estações de trabalho). Quando um host executa AH ou ESP sobre IPv4, a carga útil é os dados que normalmente seguem o cabeçalho IP, o ESP no modo de transporte criptográfa e, opcionalmente, autêntica a carga útil do IP, mas não o cabeçalho IP. Já o AH no modo de transporte autêntica a carga útil do IP e as partes selecionadas do cabeçalho IP.

O modo de túnel fornece proteção para todo o pacote IP. Para conseguir isso, depois que os campos AH ou ESP são adicionados ao pacote IP, todo o pacote mais os campos de segurança são tratados como a carga útil do novo pacote IP externo com um novo cabeçalho IP externo. Todo o pacote original, interno, viaja através de um túnel de um ponto de uma rede IP para outro; Nenhum roteador ao longo do caminho é capaz de examinar o cabeçalho IP interno. Como o pacote original é encapsulado, o novo pacote maior pode ter endereços de origem e destino totalmente diferentes, aumentando a segurança. O modo de túnel é

usado quando uma ou ambas as extremidades de uma associação de segurança (SA) são um gateway de segurança, como um firewall ou roteador que implementa o IPsec.

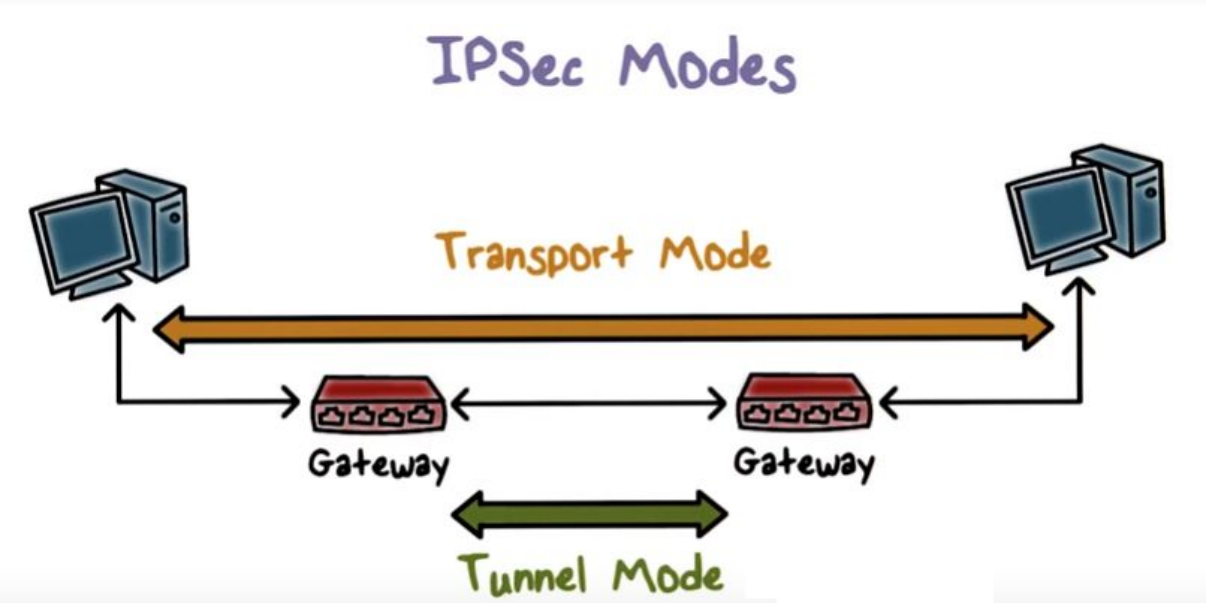

Figura 1: Demonstração do modo Transporte e do modo Túnel do IPSec.

III. DESENVOLVIMENTO PRÁTICO

Em um primeiro momento, executou-se o *prompt de comando* seguido do comando *mmc*, para abrir um console para que fosse possível a adição do IPSec, selecionando o mesmo para a ser adicionado no computador local.

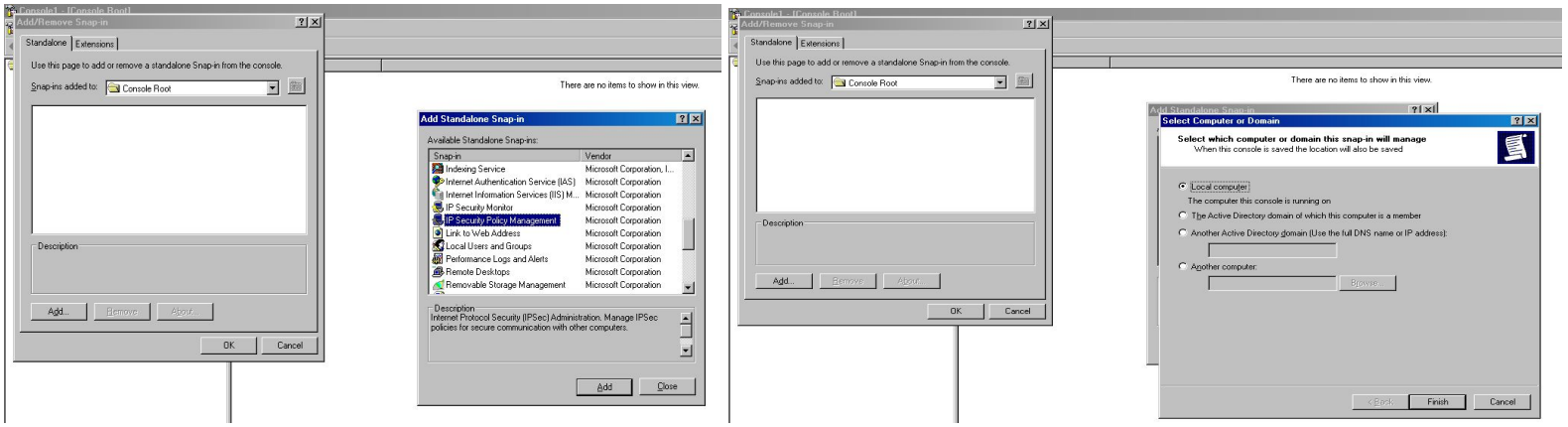

Figura 2: Adição do IPSec ao console.

Feita a adição do IPSec, partiu-se para a configuração do mesmo. Clicando com o botão direito do mouse, e selecionando a opção *Create IP Security Policy*, para criar uma política de segurança.

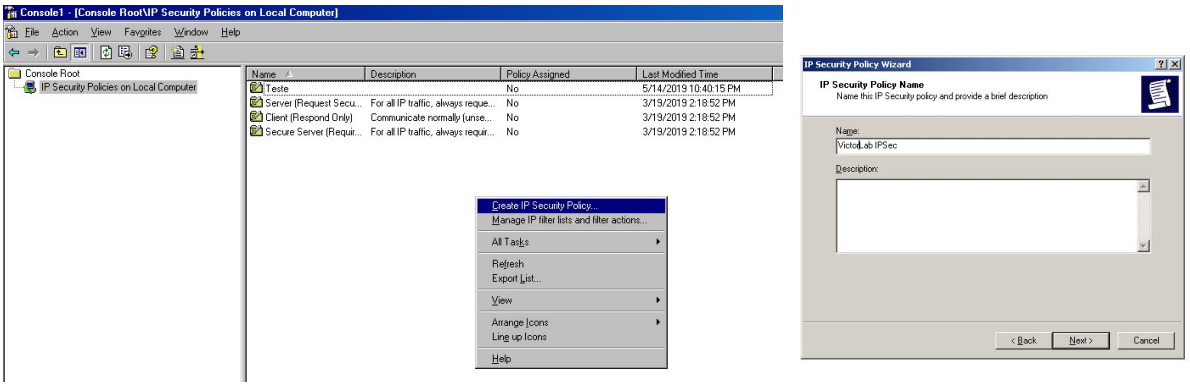

Figura 3: Criação de uma política de a segurança.

O nome adicionado para a política foi *VictorLab IPSec*, seguido dos passos e das marcações das caixas de diálogos, desativando as regras padrões e abrindo as propriedades, como informado pela **Figura 4**.

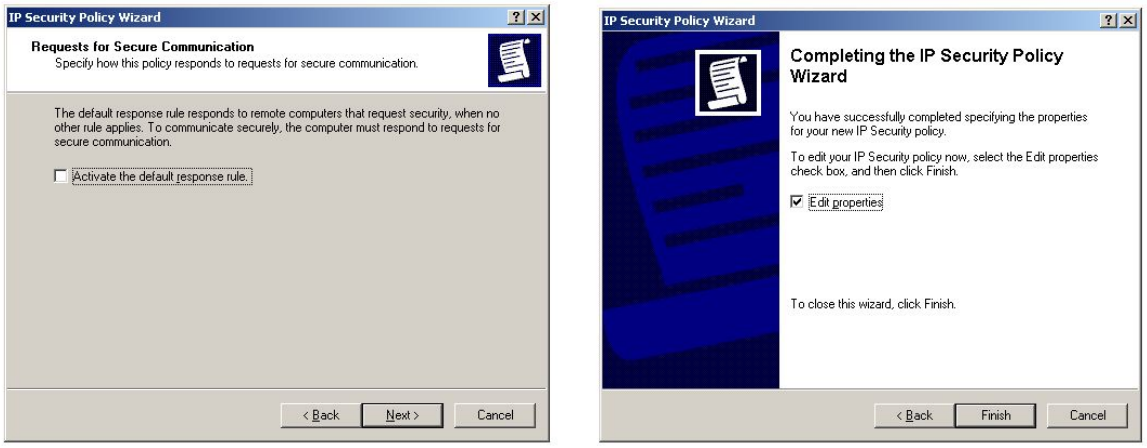

Figura 4: Finalizando a criação de uma política de a segurança.

Ao abrir as propriedades da política de segurança do IPSec criada, iremos adicionar um regra de segurança para o mesmo, clicando no botão *Add* da propriedade.

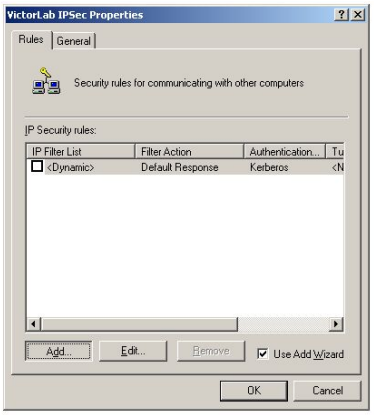

Figura 5: Propriedades e adição da regra para o IPSec.

Para criação da regra, selecionamos o modo de uso como *Transporte*, como já foi informado na parte teórica deste relatório.

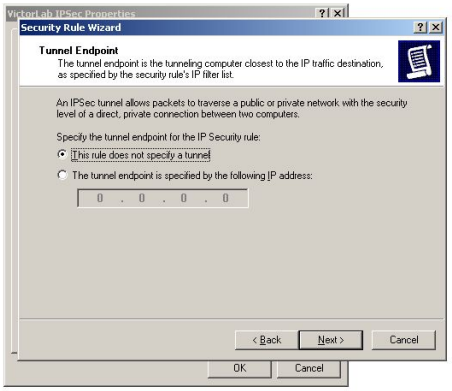

Figura 6: Configuração do modo de uso como *Transporte*.

Após a configuração do modo como *Transporte*, passamos para a configuração do tipo de rede que será utilizado, como usou-se uma conexão local, foi selecionada a opção *Local area network (LAN)*.

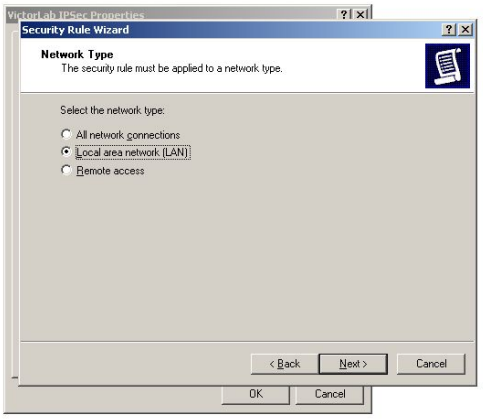

Figura 7: Configuração da rede para a regra.

Na próxima etapa da configuração da regra, precisou-se criar um filtro para o IP, para isso, clicamos na opção *Add*, apresentada na **Figura 8**.

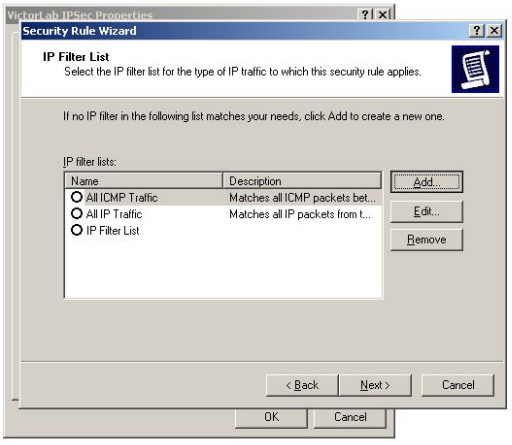

Figura 8: Criação de um filtro para um IP.

Para configurar o filtro adicionado, precisamos clicar novamente em na opção *Add* indicada na **Figura 9.**

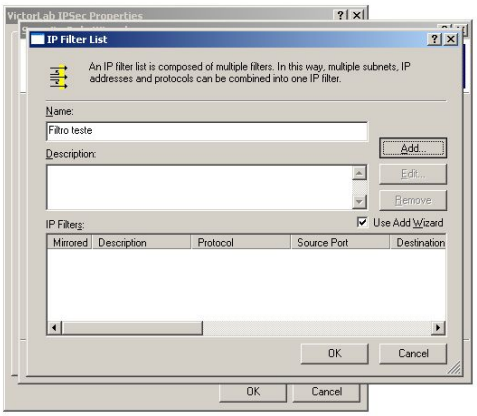

Figura 9: Configuração do filtro.

Feito isso, seguiu-se os passos da **Figura 10**, clicando em *next* em ambas as telas.

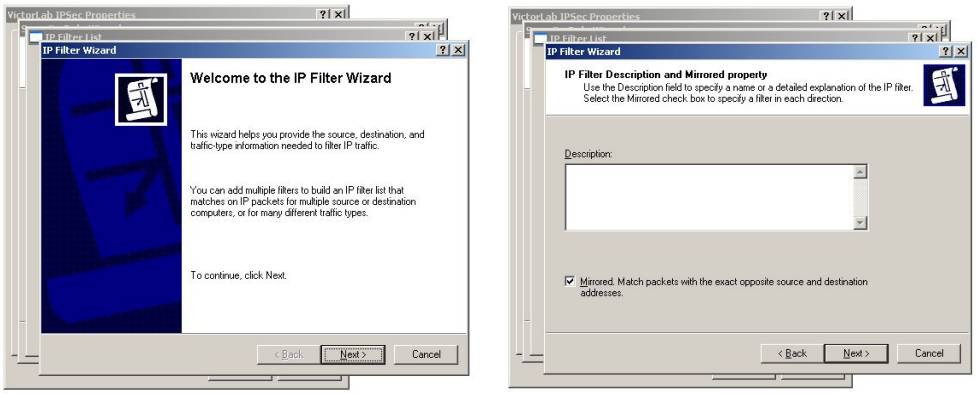

Figura 10: Configuração do filtro.

O próximo passo foi definir quem seria o "servidor" e quem seria o "cliente", em aula, foi combinado que o aluno Victor seria o servidor e o aluno Yuri seria o cliente que acessaria o site de Victor feito nos laboratórios passados. A próxima opção então foi definir o *Source address* sendo a opção *My IP Adress* (IP do Victor - 10.0.3.1).

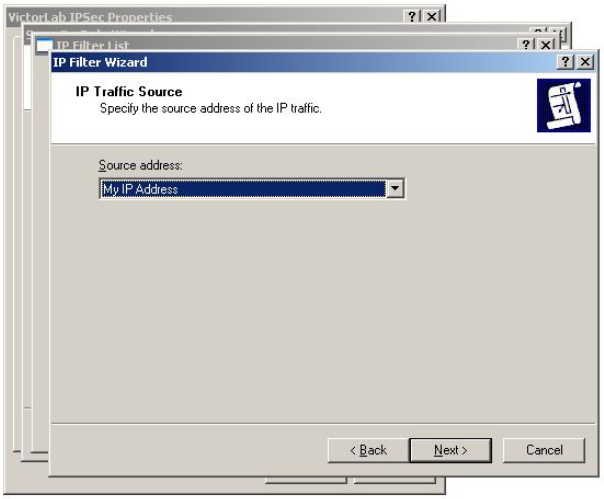

Figura 11: Configuração da fonte (servidor).

Agora necessitou-se fazer a configuração do cliente, para isso a opção selecionada foi *A Specific IP Addres*, e adicionou-se o IP de Yuri (10.0.2.1), como indica a **Figura 12**.

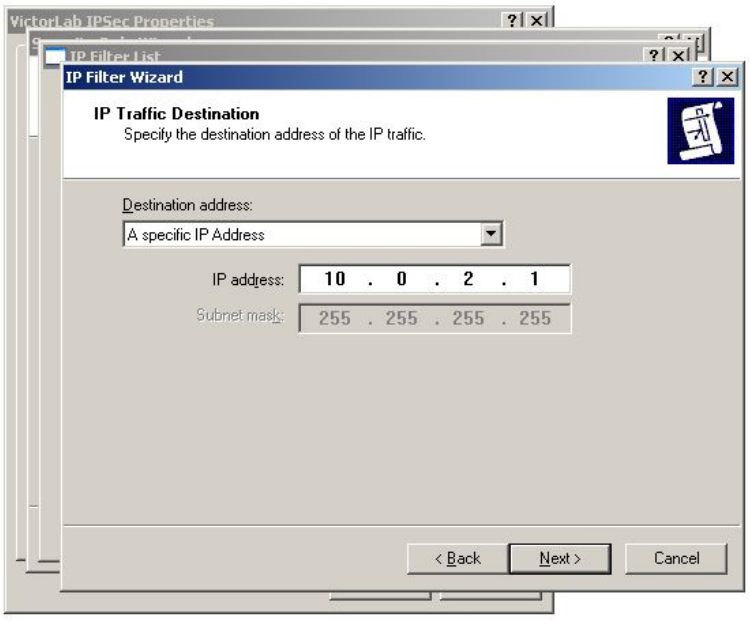

Figura 12: Configuração do destino (cliente).

Na próxima opção escolheu-se o tipo de protocolo, *TCP.*

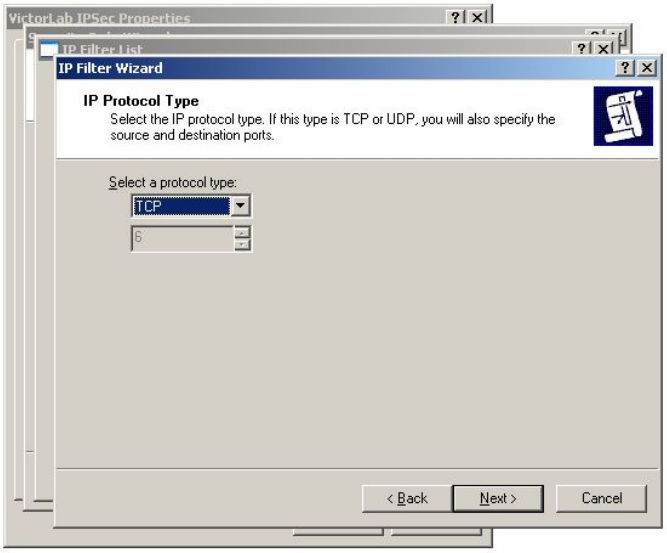

Figura 13: Configuração do destino (cliente).

Na próxima janela indicada pela **Figura 14,** precisou-se setar as portas que seriam usadas para a comunicação. O aluno Victor selecionou a porta definida nos laboratoŕios anteriores para acesso do servidor web, *Port 80*, e selecionou *To any port* para que qualquer porta pudesse receber a comunicação.

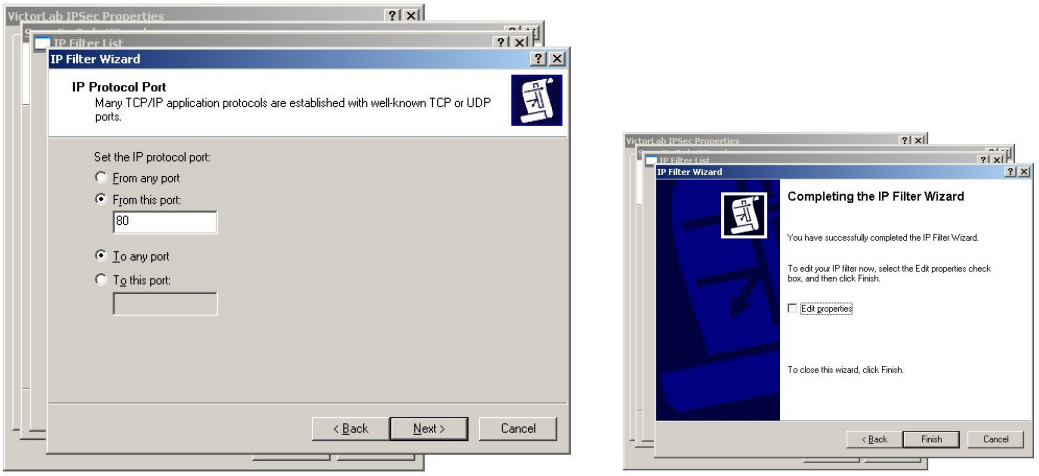

Figura 14: Configuração das portas e finalização da configuração do filtro.

Após a configuração do Filtro para o IP, clicou-se na opção *Ok* como indica a **Figura 15**.

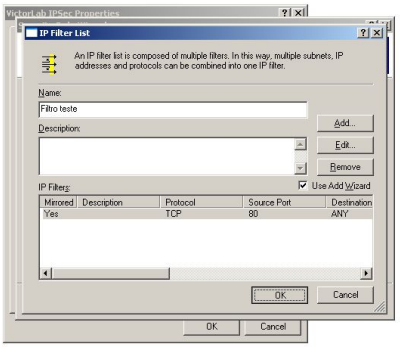

Figura 15: Finalização da criação e configuração do filtro para IP.

Finalizando-se a criação e configuração do filtro, precisou selecionar o mesmo, nas opções indicadas pela **Figura 16**, seguido do botão *next*.

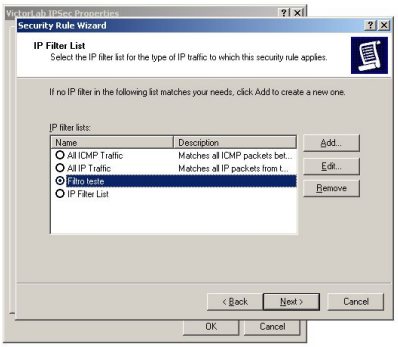

Figura 16: Seleção do filtro IP criado.

A próxima tela, representada pela **Figura 17**, nos dá 3 opções, sendo a primeira *Permit* que não utiliza IPSec na comunicação; seguida da opção *Required Secutiry (Optional)* que tenta efetuar a comunicação usando IPSec e caso não consiga, a comunicação é efetuada sem IPSec; e a última opção *Require Secutiry* que só efetua a comunicação com IPSec.

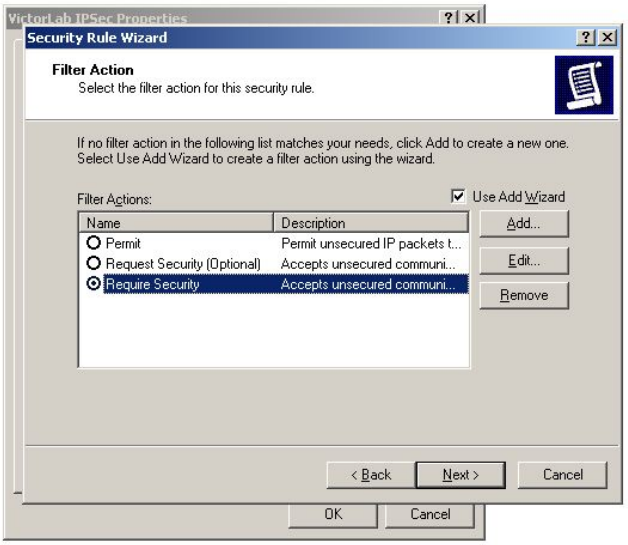

Figura 17: Seleção da ação do filtro (se usará ou não IPSec).

O próximo passo consiste no método de autenticação para a comunicação , possuindo também três opções, sendo a primeira *Active Directory default* que não apresenta autenticação, a segunda opção *Use a certificate from this CA* que é o mesmo método utilizado nos laboratórios passados envolvendo a Autoridade Certificadora; e por fim *Use this string to protect the key exchange* que é a utilização de uma frase como chave de autenticação. A opção escolhida foi a terceira, e para sua funcionalidade correta tanto o computador "servidor" quanto o "cliente" precisarão configurar com a mesma frase. No laboratório, a frase utilizada em ambos os computadores, do Victor e do Yuri, foi *123*.

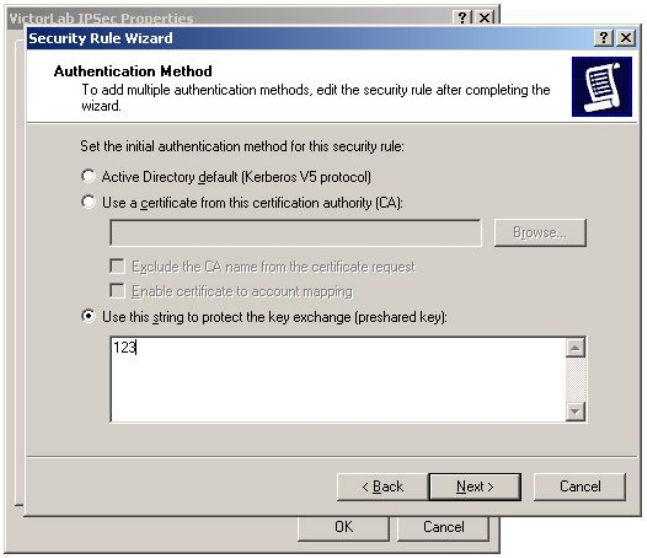

Figura 18: Configuração do método de autenticação.

Após a configuração do métodos de autenticação seguido da opção *Ok* da janela, indicada pela **Figura 18**, selecionou-se o filtro criado para que possa ser utilizado, seguido de *Ok*, como indica a **Figura 19.**

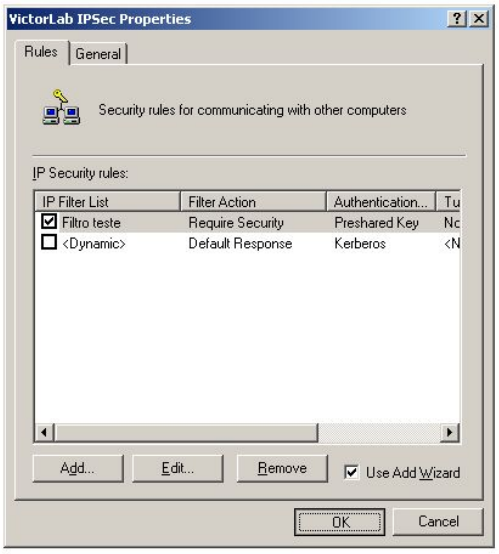

Figura 19: Ativação do filtro.

Por fim, selecionou-se a política, criada anteriormente, com o botão direito do mouse e clicou-se na opção *Assing*, para atribuir/ativar a política e testar seu funcionamento.

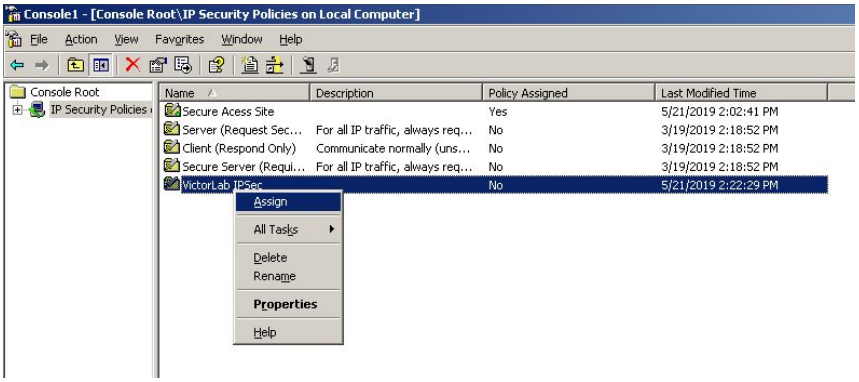

Figura 20: Assinatura da política.

IV. CONCLUSÃO

Como conclusão, fora da máquina virtual, no sistema nativo, executou-se o programa analisador de pacotes, o WireShark. Filtrou-se para obter somente pacotes do IP do cliente, no caso o IP do Yuri (10.0.2.1).

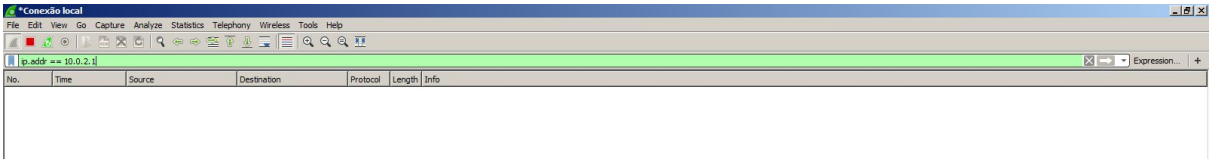

Figura 20: Filtragem da troca de pacotes com o IP específico.

Feita a filtragem com o IP, foi possível verificar a comunicação/troca de pacotes entre os dois alunos. Também é importante notar os protocolos utilizados, ESP que tem seu funcionamento explicado na parte teórica deste relatório, e o protocolo ISAKMP, como pode ser visto na **Figura 21**.

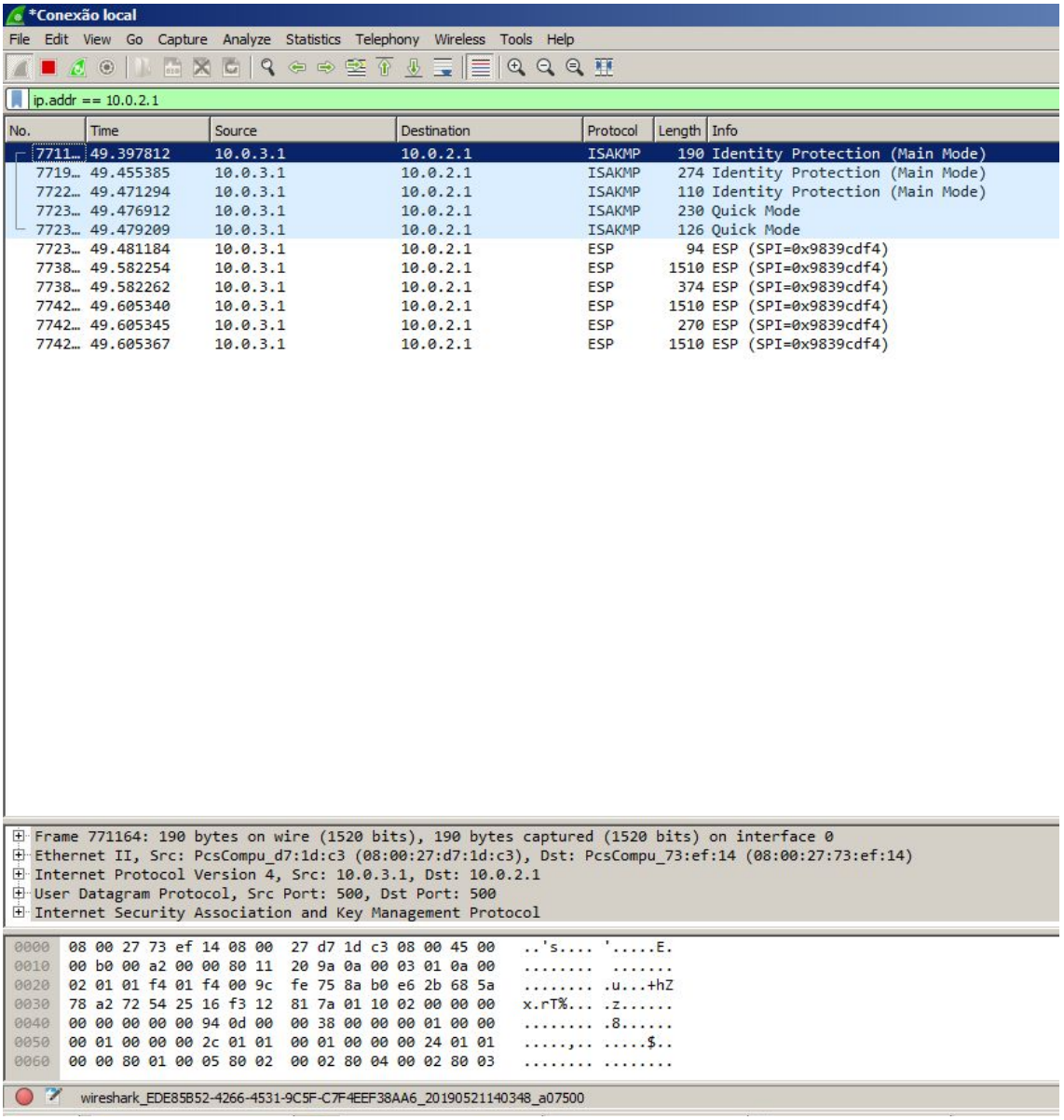

Figura 21: Análise da troca de pacotes entre alunos.

A parte de gerenciamento de chave do IPsec envolve a determinação e a distribuição de chaves secretas. Um requisito típico é quatro chaves para comunicação entre dois aplicativos: transmitir e receber pares para integridade e confidencialidade.

O protocolo de gerenciamento de chaves automatizado padrão para IPsec é referido como ISAKMP/Oakley e consiste nos seguintes elementos:

- Protocolo de Determinação de Chaves da Oakley: O Oakley é um protocolo de troca de chaves baseado no algoritmo Diffie-Hellman, mas fornecendo segurança adicional. A Oakley é genérica na medida em que não dita formatos específicos.
- Associação de Segurança da Internet e Protocolo de Gerenciamento de Chaves (ISAKMP): O ISAKMP fornece uma estrutura para o gerenciamento de chaves da Internet e fornece o suporte de protocolo específico, incluindo formatos, para negociação de atributos de segurança.

O ISAKMP por si só não dita um algoritmo de troca de chave específico; em vez disso, o ISAKMP consiste em um conjunto de tipos de mensagens que permitem o uso de

uma variedade de algoritmos de troca de chaves. O Oakley é o algoritmo de troca de chave específico obrigatório para uso com a versão inicial do ISAKMP.

V. REFERÊNCIAS

[1] STALLINGS, WILLIAM - **Cryptography and network security principles and practice.** 7th Edition.

[2] Material disponibilizado pelo professor.