

UNIVERSIDADE DE CUIABÁ
ESPECIALIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

**ESTUDO DE CASO DO PROTOCOLO IPSEC EM REDES IPV4 E
IPV6**

RAUL NERIS DOS SANTOS

CUIABÁ-MT
OUTUBRO/2014

ESTUDO DE CASO DO PROTOCOLO IPSEC EM REDES IPV4 E IPV6

RAUL NERIS DOS SANTOS

Monografia apresentada ao Curso de Especialização em Segurança da Informação do Programa de Pós-Graduação da Universidade de Cuiabá, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. M.e. Edson Shin-Iti Komatsu

CUIABÁ-MT

OUTUBRO/2014

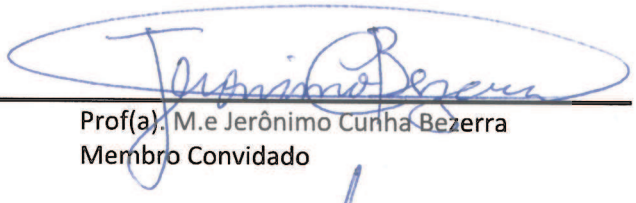
RAUL NERIS DOS SANTOS
ESTUDO DE CASO DO PROTOCOLO IPSec EM REDES IPv4 E IPv6

Monografia de Especialização apresentada à
União para o Desenvolvimento da Pós-
Graduação - UNIPÓS da Universidade de
Cuiabá, para obtenção do título de
Especialista em Segurança da Informação.
Orientador(a): M.e. Edson Shin-Iti Komatsu

BANCA EXAMINADORA



Prof(a). M.e. Edson Shin-Iti Komatsu
Orientador(a)



Prof(a). M.e. Jerônimo Cunha Bezerra
Membro Convidado



Prof(a). M.e. Maximillian Mayolino Leão
Membro Convidado

Cuiabá, 26 de novembro de 2014

Nota final:

10,0 (DEZ)

DEDICATÓRIA

Eu dedico este trabalho a todos os meus familiares, a meus pais Maria Geni dos Santos e Pedro Neris dos Santos, a minha irmã Rafaela Neris dos Santos, a minha noiva Juciane Antonio de Souza e em especial a meu avô paterno Augusto dos Santos que nos deixou no dia 13/10/2014.

AGRADECIMENTOS

Eu agradeço primeiramente a Deus pela força que tem me concedido durante toda minha vida acadêmica e a meus familiares pela paciência. Agradeço também a todos os professores deste curso em especial a meu orientador Prof. M.e. Edson Shin-Iti Komatsu que de longa data contribui com a minha formação acadêmica e aperfeiçoamento profissional.

SUMÁRIO

INTRODUÇÃO.....	12
JUSTIFICATIVA.....	13
OBJETIVOS.....	14
METODOLOGIA.....	15
FUNDAMENTAÇÃO TEÓRICA	16
ORGANIZAÇÃO DA MONOGRAFIA.....	19
1 - PROTOCOLO IPV4	20
1.1 - CABEÇALHO IPV4.....	20
1.2 - ENDEREÇAMENTO IPV4.....	21
1.3 - SEGURANÇA IPV4.....	23
2 - PROTOCOLO IPV6	24
2.1 - CABEÇALHO IPV6.....	24
2.2 - ENDEREÇAMENTO IPV6.....	27
2.3 - FUNCIONALIDADES BÁSICAS DO IPV6.....	29
2.4 - ICMPV6	29
2.5 - NEIGHBOR DISCOVERY PROTOCOL	30
2.6 - SEGURANÇA IPV6.....	32
2.6.1 - IPSEC	33
2.6.2 – <i>SECURITY ASSOCIATION</i> (SA)	34
2.6.3 – <i>INTERNET KEY EXCHANGE</i> (IKE)	34
2.6.4 – CABEÇALHOS DE SEGURANÇA IPV6	35
3 – ESTUDO DE CASO	40
3.1 – REQUISITOS DE SOFTWARE.....	40

3.2 – REQUISITOS DE HARDWARE	40
3.3 – AMBIENTE DE TESTE	41
3.3.1 – CONFIGURAÇÃO IPSEC	41
3.3.2 – TESTES.....	56
3.3.2.1 – ANÁLISE PROTOCOLO IPV4.....	57
3.3.2.2 – ANÁLISE PROTOCOLO IPV4 COM IPSEC.....	57
3.3.2.3 – ANÁLISE PROTOCOLO IPV6.....	59
3.3.2.4 – ANÁLISE PROTOCOLO IPV6 COM IPSEC.....	59
4 – CONCLUSÃO.....	61

LISTA DE FIGURAS

Figura 1 - Cabeçalho do Protocolo IPv4	20
Figura 2 - Faixa de Endereços IPv4.....	22
Figura 3 - Cabeçalho do Protocolo IPv6	25
Figura 4 - Encadeamento dos Cabeçalhos de Extensão	27
Figura 5 - Estrutura do Endereço IPv6	28
Figura 6 - Cabeçalho do ICMPv6.....	30
Figura 7 - Cabeçalho AH.....	36
Figura 8 - Cabeçalho ESP.....	37
Figura 9 - IPSec Modo Transporte	38
Figura 10 - IPSec Modo Túnel	38
Figura 11 - Cabeçalho ESP encapsulado pelo AH	39
Figura 12 - Topologia de Rede <i>host-to-host</i>	41
Figura 13 - Iniciando a Diretiva de Segurança Local.....	42
Figura 14 - Diretiva de Segurança Local.....	42
Figura 15 - Assistente de Diretiva de Segurança IP	43
Figura 16 - Nome de Diretiva de Segurança IP	43
Figura 17 - Solicitação de Comunicação Segura.....	44
Figura 18 - Concluindo o Assistente de Diretiva de Segurança IP	44
Figura 19 - Propriedades de IPSec	45
Figura 20 - Propriedades de Nova Regra	46
Figura 21 - Lista de Filtros IP.....	46
Figura 22 - Propriedades de Filtro IP	47
Figura 23 - Propriedades de Filtro IP – Protocolo.....	48

Figura 24 - Propriedades de Filtro IP – Descrição	48
Figura 25 - Concluindo Lista de Filtro IP	49
Figura 26 - Propriedades de Editar Regra	49
Figura 27 - Ação de Filtro	50
Figura 28 - Método de Ação de Filtro	51
Figura 29 - Integridade e criptografia.....	51
Figura 30 - Nome e Descrição para a Ação de Filtro	52
Figura 31 - Métodos de Autenticação	53
Figura 32 - Definindo um Método de Autenticação.....	53
Figura 33 - Configuração de Túnel	54
Figura 34 - Tipo de Conexão.....	55
Figura 35 - Propriedades de IPSec após Configuração	55
Figura 36 - Diretiva de Segurança Local após Configuração.....	56
Figura 37 - Topologia Física	56
Figura 38 - Protocolo IPv4 sem IPSec.....	57
Figura 39 - Protocolo ISAKMP IPv4	58
Figura 40 - Protocolo IPv4 com IPSec	58
Figura 41 - Protocolo IPv6 sem IPSec.....	59
Figura 42 - Protocolo ISAKMP IPv6	59
Figura 43 - Protocolo IPv6 com IPSec	60

LISTA DE TABELAS

Tabela 1 - Faixa de Endereço Privada do IPv4	23
Tabela 2 - Ordem dos Cabeçalhos de Extensão	26
Tabela 3 - Mensagens ICMPv6 do NDP	31

LISTA DE SIGLAS

ARPANET	Advanced Research Project Agency Network
AH	Authentication Header
AS	Autonomous System
CIDR	Classless Inter-Domain Routing
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MIPv6	Mobile Internet Protocol version 6
MTU	Maximum Transmission Unit

NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
OSI	Open Systems Interconnect
RFC	Request for Comments
SA	Security Association
SO	Sistema Operacional
SPI	Security Parameter Index
UDP	User Datagram Protocol
VM	Virtual Machine
VPN	Virtual Private Network

RESUMO

Estamos vivendo na era da informação, precisamos cada vez mais trocar informações de forma rápida e isso hoje é possível graças a Internet, notícias de qualquer parte do mundo estão bem a nossa frente, a um click de distância, além de serviços como transações bancárias e *e-commerce*. Porém quando a Internet foi criada não foi previsto essa gama de serviços, tanto que a segurança não fazia parte do projeto inicial do protocolo IPv4. Além da necessidade de segurança, atualmente a Internet necessita de mais endereços IP, o protocolo IPv4 foi projetado com um espaço de 32 bits para endereçamento, atualmente esse espaço está escasso.

O protocolo IPv6 surgiu com o principal objetivo de suprir a escassez de endereços IPv4, o IPv6 possui 128 bits para endereçamento, número absurdamente grande, ainda aproveitando a oportunidade de desenvolvimento de um novo protocolo os engenheiros que participaram da elaboração do projeto decidiram que era necessário que o protocolo IPv6 possuísse novas funcionalidades para que fosse possível suporte a novas tecnologias. Dentre as novas funcionalidades uma voltada para a segurança é bastante citada pelos autores, que o IPv6 passa a ter segurança nativa através do protocolo IPSec fazendo parte da pilha de protocolo TCP/IPv6, esse aspecto será abordado e discutido neste trabalho através de estudo de caso.

O presente trabalho apresenta o novo protocolo de Internet o IPv6 mostrando as suas principais funcionalidades e mudanças em relação ao protocolo IPv4.

ABSTRACT

We are living in the information age, we increasingly need to exchange information quickly and this is now possible thanks to the Internet, news from anywhere in the world are well ahead in our one click away, plus services such as banking and e-commerce. But when the Internet was not created such a range of services was provided, so that the security was not part of the initial design of IPv4 protocol. Besides the need for security, currently the Internet requires more IP addresses, the IPv4 protocol was designed with space for 32-bit addressing, currently this space is scarce.

The IPv6 protocol came up with the main objective of meeting the shortage of IPv4 addresses, IPv6 has 128 bits for addressing, absurdly large number, even taking the opportunity to develop a new protocol engineers who participated in the elaboration of the project decided that it was necessary the IPv6 protocol possess new features to make it possible to support new technologies. Among the new features a forward security is often quoted by the authors, who shall be native IPv6 security through IPSec protocol part of the stack TCP / IPv6 protocol, this aspect will be addressed and discussed in this paper through a case study of.

This paper presents the new Internet protocol IPv6 showing its main features and changes compared to IPv4.

INTRODUÇÃO

Com o advento da internet a humanidade passou a utilizá-la para diversos fins, como exemplo, comunicação com familiares e colegas, correio eletrônico, comércio eletrônico, serviços bancários, pesquisas, estudo a distância, redes sociais, etc. Porém o projeto inicial da Internet não previa o seu uso comercial e doméstico, apenas militar e acadêmico.

Segundo Tanenbaum (2011), o projeto inicial de elaboração da Internet começou no final da década de 1950, o Departamento de Defesa dos Estados Unidos queria uma rede capaz de resistir a ataques, onde se uma linha de transmissão ou central de comutação fosse atingida a comunicação continuaria por uma rota alternativa.

Brito (2013, p.19) disse que: [...] Em 1969 foram instalados os primeiros quatro nós da rede que, naquela época, era denominada ARPANET. Com o passar dos anos a Internet cresceu substancialmente, atingindo números de usuários jamais imaginados.

Visando subsidiar este crescimento, nasce o protocolo base da Internet, o IP (*Internet Protocol*), que é responsável pelo endereçamento dos *hosts* e roteamento dos pacotes na Internet. Em sua versão atual, o protocolo IPv4 (*Internet Protocol version 4*) é composto por 32 bits para endereçamento dos *hosts*, com isso são possíveis 4.294.967.296 endereços. Parece muito, não? Naquela época sim, porém hoje não. Diante disso, serviços como CIDR (*Classless Inter-Domain Routing*) e NAT (*Network Address Translation*) foram criados visando otimizar a alocação de endereços IPv4.

Tanenbaum (2011) comenta que: “Até mesmo com CIDR e NAT usando endereços com mais cautela, os últimos endereços IPv4 deverão ser atribuídos pela ICANN antes do final de 2012”.

Segundo Brito (2013, p.26): [...] Em 2011, o estoque de endereços disponíveis na IANA atingiu seu esgotamento, ou seja, todos os endereços IPv4 disponíveis já haviam sido distribuídos para as autoridades regionais e, assim que os estoques locais chegarem ao fim, a Internet não poderá mais crescer.

A solução para a escassez dos endereços IPv4 já foi desenvolvida a quase duas décadas com a padronização do protocolo IPv6 (*Internet Protocol version 6*), a versão 6 do protocolo IP. Segundo Tanenbaum (2011), o protocolo IPv6 foi padronizado em 1998.

O novo protocolo de Internet, o IPv6 utiliza 128 bits para endereçamento com isso é possível 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) de endereços.

Ainda segundo Tanenbaum (2011), o IPv6 é um protocolo bastante diferente da camada de rede e não se interliga com o IPv4, apesar de suas semelhanças, com isso atualmente apenas um por cento da Internet está utilizando o IPv6.

É indiscutível a adoção do protocolo IPv6 devido ao esgotamento dos endereços IPv4, porém o IPv6 não foi concebido apenas para resolver o problema de escassez de endereços, mas também para trazer novas funcionalidades ao IP. Os ISPs (*Internet Service Providers*) ou mesmo ASs (*Autonomous Systems*) devem adotar o protocolo de Internet IPv6, não só pelo fato da escassez de endereços IPv4, mas pelo nível de segurança que pode ser obtida e novas funcionalidades que o IPv6 tem.

Nos dias atuais a segurança da informação é algo indispensável não só para grandes corporações, porém também para usuários domésticos, pelo fato que a Internet hoje não é só utilizada para troca de mensagens, mas também para transações bancárias e e-commerce o que exige que as informações que são trafegadas pela Internet sejam confidenciais a quem é de interesse.

Atualmente estamos vivendo a era da “Internet das Coisas”, onde qualquer tipo de equipamento pode ser conectado à Internet, por exemplo, cafeteira, geladeira, micro-ondas, aparelho de ar-condicionado, televisor, automóvel, lâmpada e entre outros. Com isso não há somente a necessidade de mais endereços IP, mas também, a necessidade de melhorar as funcionalidades e segurança do protocolo IP versão 4.

Justificativa

O projeto justifica-se porque, a evolução do protocolo IPv4 para o IPv6 é inevitável. Com a utilização do protocolo IPv6, a camada de rede passa a ter nativamente mecanismo de segurança. O rastreamento de *hosts* na Internet será possível, porque o IPv6 não faz uso de NAT, pois o projeto do IPv6 prevê que os *hosts* que conectarem-se a Internet não deverão utilizar o NAT. Esse é um dos muitos benefícios que o protocolo IPv6 oferece em nível de segurança.

Como dito, estamos vivendo na era da “Internet das Coisas”, onde os mais variados tipos de equipamentos estão sendo conectados à Internet.

Brito (2013, p.36) afirma que: [...] todo esse avanço ubíquo na conectividade somente será realmente viável quando tivermos o IPv6 efetivamente operacional na Internet, afinal, será necessário muito mais endereços do que os poucos 4,3 bilhões do IPv4, além de outros requisitos como segurança[...]

Com o avanço por toda parte na conectividade, não há somente a necessidade de mais endereços IP, mas a necessidade de melhorar as funcionalidades e segurança do protocolo IPv4, por isso a adoção do protocolo IPv6 se faz necessária.

Objetivos

Este trabalho tem como objetivo realizar um estudo das principais funcionalidades do protocolo IPv6, visando desenvolver um estudo de caso prático que realize uma análise do protocolo IPSec em redes IPv4 e IPv6.

Visando atingir o objetivo geral do trabalho pretende-se:

- Realizar um estudo teórico sobre segurança da informação, auditoria em redes, análise de vulnerabilidades e os protocolos IPv4 e IPv6;
- Fazer um levantamento de requisitos de software (sistema operacional, serviços de redes, máquina virtual) e hardware para o projeto;
- Especificar a arquitetura de rede a ser utilizada no estudo de caso;
- Implantar e configurar a arquitetura de rede;
- Configurar a arquitetura com o protocolo ipv4;
- Definir testes de vulnerabilidades;
- Executar os testes de vulnerabilidades;
- Analisar os resultados obtidos;
- Reconfigurar a arquitetura com o protocolo IPv6;
- Reaplicar os testes de vulnerabilidades;
- Analisar os testes obtidos;
- Confrontar os dois resultados (Ipv4 e Ipv6);
- Apresentar as conclusões com base nos resultados;
- Escrever a monografia.

Metodologia

A metodologia utilizada para a elaboração deste projeto é qualitativa, será realizado um estudo de caso do protocolo IPSec em redes IPv4 e IPv6.

Será realizado um levantamento bibliográfico sobre os temas: Segurança da informação, análise de vulnerabilidades e os protocolos IPv4 e IPv6. Esse levantamento será realizado através de consultas a livros e Internet.

Em seguida será feito um levantamento de requisitos de software (sistema operacional, serviços de redes, máquina virtual) e hardware.

Após realização do levantamento de requisitos, será montado um laboratório através de máquinas virtuais para realização dos testes.

Os testes serão realizados aplicando as ferramentas de vulnerabilidade no protocolo IPv4 e em seguida analisar os resultados obtidos. Em seguida será aplicado o mesmo teste no protocolo IPv6 e analisado os resultados obtidos. Após realizado os testes serão confrontados os dois resultados obtidos (IPv4 e IPv6) e será apresentada as conclusões com base nos dois resultados.

Fundamentação Teórica

Assim se Faz: “A fundamentação teórica é uma etapa fundamental para a execução da pesquisa, pois se trata de um segmento em que as teorias encontradas que dialogam e comprovam o teor e a credibilidade do estudo realizado são veiculadas em forma de texto. [...] se o embasamento teórico é bem fundamentado, provavelmente a pesquisa que se apresenta também o é [...]”

Segurança da Informação

A Segurança da Informação é de fundamental importância desde as grandes corporações até os usuários domésticos. O que muda é o quanto custa a informação em cada contexto.

Moraes (2010 p.19) “A Segurança da Informação pode ser definida como um processo de proteger a informação do mau uso tanto acidental como intencional, por pessoas internas ou externas à organização, [...]”

Integridade

Moraes (2010) explica que: A integridade tem como função garantir que uma mensagem não seja alterada durante sua transmissão ou armazenamento.

Moraes (2010 p.26): “O objetivo da garantia de integridade dos dados é prevenir a existência de fraude ou erros de processamento. Nenhum usuário deve ter a capacidade de alterar os dados de forma a corrompê-los, ou causar perda financeira, tornando a informação não confiável.”

Tanenbaum (2009): A integridade tem o objetivo de não permitir que usuários não autorizados realizem alterações nos dados, exclusões e inserir dados falsos.

Confidencialidade

Kurose (2006): A confidencialidade permite que somente o destinatário e o remetente de uma comunicação leiam a mensagem transmitida, isso é possível através da criptografia.

Tanenbaum (2009) afirma que: A confidencialidade dos dados é assegurar que os dados secretos serão mantidos em segredo. Os dados só podem ser acessados por pessoas previamente autorizadas.

Disponibilidade

A disponibilidade é muito importante principalmente em corporações que disponibilizam serviços pela rede. Imaginemos uma operadora de cartão de créditos, o sistema fica indisponível por alguns segundos, quantas transações deixaram de ser realizadas neste curto espaço de tempo? Acredito que milhares. A disponibilidade se faz necessária para os serviços de rede.

Tanenbaum (2009 p.380) explica que a disponibilidade: “[...] significa que ninguém pode perturbar o sistema para deixá-lo inutilizável.”

Autenticidade

Moraes (2010 p.29): “A autenticidade consiste em mecanismos que verificam se a mensagem é mesmo de quem diz ser o remetente.”

Kurose (2006) disse que: A autenticação se faz necessária para que duas entidades (remetente e destinatário) possam verificar ambas as identidades.

Auditoria

Para Moraes (2010), a auditoria é um importante serviço utilizado para registrar atividades em uma rede, com isso é possível realizar uma verificação a procura de irregularidades no futuro. Moraes (2010 p.30) ainda explica que a auditoria: “Consiste na capacidade de verificação das atividades do sistema e determinação do que foi feito, por quem, quando e o que foi afetado [...]”

Análise de Vulnerabilidades

Moraes (2010) disse que: Uma vulnerabilidade pode ser definida como uma falha no sistema, um colaborador que não mantém sua senha em segurança, um colaborador que altera a base de dados ou uma pessoa contratada para roubar dados da empresa.

Organização da Monografia

Este trabalho monográfico está organizado da seguinte forma:

Capítulo 1 – Protocolo IPv4, cabeçalho IPv4, endereçamento IPv4 e segurança IPv4.

Capítulo 2 – Protocolo IPv6, cabeçalho IPv6, endereçamento IPv6, funcionalidades básicas do IPv6, ICMPv6, neighbor discovery protocol e segurança IPv6.

Capítulo 3 – Estudo de Caso, requisito de software, requisito de hardware, ambiente de teste, configuração IPsec, testes, análise protocolo IPv4, análise protocolo IPv4 com IPsec, análise protocolo IPv6, análise protocolo IPv6 com IPsec.

Capítulo 4 – Conclusão.

1 - PROTOCOLO IPv4

O protocolo IPv4 é o protocolo base usado atualmente pela Internet, o IPv4 é responsável pelo roteamento dos pacotes e é de suma importância pelo funcionamento da rede mundial de computadores. Afirma Tanenbaum (2011, p.274): “O elemento que mantém a Internet unida é o protocolo da camada de rede, o IP (*Internet Protocol*).”

1.1 - Cabeçalho IPv4

Tanenbaum (2011) disse que, o cabeçalho do protocolo IPv4 é formado por duas partes, uma parte de tamanho fixo contendo 20 bytes e uma parte de tamanho variável. Os bits são transmitidos da esquerda para a direita e de cima para baixo. Brito (2013) disse também que, o cabeçalho do protocolo IPv4 possui 12 campos fixos e seu tamanho varia entre 20 e 60 bytes devido existir o campo opções e complemento.

A figura 1 mostra o formato do cabeçalho IPv4.

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)			Flags	Deslocamento do Fragmento (Fragment Offset)
Tempo de Vida (TTL)		Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Figura 1 - Cabeçalho do Protocolo IPv4

Fonte: <http://ipv6.br/entenda/cabecalho>

Tanenbaum (2011) explica os campos do cabeçalho IPv4: O campo Versão define a versão do protocolo que está sendo usado. O campo Tamanho do Cabeçalho informa o tamanho total do cabeçalho. O campo Tipo de Serviço é utilizado para marcar os pacotes com sua classe de serviço. O campo Tamanho Total é utilizado para informar o tamanho total do datagrama, cabeçalho mais dados. O campo Identificação é utilizado pelo *host* de destino para identificar a qual datagrama pertence um determinado fragmento. O campo *Flags* é utilizado como parte do processo para descobrir a MTU (*Maximum Transmission Unit*) do caminho e para saber quando chegaram os fragmentos de um determinado datagrama. O campo Deslocamento do Fragmento informa a posição do fragmento dentro do datagrama atual. O campo Tempo de Vida permite restringir o número de saltos que o pacote pode alcançar. O campo Protocolo aponta para qual protocolo de camada superior o pacote será entregue. O campo Soma de Verificação do Cabeçalho possibilita verificar se existe erros no cabeçalho. Os campos Endereço de Origem e Endereço de Destino identificam os endereços dos *hosts*. O campo Opções foi criado para que novos protocolos pudessem utilizá-lo para adicionar novas informações sem ter que realocar bits de outros campos.

1.2 - Endereçamento IPv4

O endereçamento do protocolo IPv4 faz uso de 32 bits, são possíveis 4.294.967.296 de endereços. O endereço é representado por números decimais que variam de 0 a 255, são quatro octetos separados por ponto.

Os blocos de endereços de tamanho fixo são separados por cinco classes: A, B, C, D e E.

Tanenbaum (2011, p.281) afirma que: Os formatos das classes A, B e C permitem até 128 redes com 16 milhões de *hosts* cada uma, 16.384 redes com até 65.536 *hosts* cada uma e 2 milhões de redes (por exemplo, LANs) com até 256 *hosts* cada uma (embora algumas dessas sejam especiais).

Ainda Tanenbaum (2011), a classe D é para endereço *multicast* e a classe E está reservada para uso futuro.

A figura 2 mostra as faixas dos endereços IPv4.



Figura 2 - Faixa de Endereços IPv4

Fonte: http://www.teleco.com.br/tutoriais/tutorialmplscam/pagina_2.asp

Com a escassez de endereços IPv4 que estamos enfrentando, ainda existe a faixa de endereço classe E reservada para uso futuro? Por que não utilizamos a classe E? Tanenbaum (2011, p.281), explica que “Infelizmente, muitos *hosts* não aceitarão esses endereços como válidos, pois têm ficado fora dos limites por tanto tempo que é difícil ensinar novos truques a *hosts* antigos”.

Para tentar conter a escassez dos endereços IPv4 foi criado o CIDR (*Classless Inter-Domain Routing*). Com o CIDR os bits que identificam a rede e o *host* podem estar em qualquer posição, sendo assim é possível adequar o tamanho do bloco de endereço as necessidades das organizações.

Brito (2013 p.29) afirmou que: O CIDR (acrônimo de *Classless Inter-Domain Routing*) foi definido em setembro de 1993, na RFC 1519, com o intuito de propor flexibilização das classes padrões originalmente projetadas no IPv4, de maneira que a fronteira dos bits reservados para identificar redes e *hosts* poderia estar localizada em qualquer posição.

Dentro das faixas de endereços disponíveis no IPv4, existem três faixas de endereços reservada para uso privado como mostra a tabela 1.

Tabela 1 - Faixa de Endereço Privada do IPv4

Classe	Faixa de Endereço	Número de <i>Hosts</i>
A	10.0.0.0 – 10.255.255.255/8	16.777.216
B	172.16.0.0 – 172.31.255.255/12	1.048.576
C	192.168.0.0 – 192.168.255.255/16	65.536

Fonte: Adaptado de Tanenbaum (2011, p.283)

A faixa de endereço privada não pode ser roteável na Internet, seu uso é aplicado apenas na rede LAN (*Local Area Network*).

1.3 - Segurança IPv4

O projeto inicial do protocolo IPv4 não previa qualquer meio de segurança na camada de rede, as aplicações que necessitassem de autenticidade, confidencialidade e integridade deveriam prover tudo isso na sua própria camada. O protocolo IPSec (*Internet Protocol Security*) foi adaptado para funcionar com o IPv4, porém existem restrições ao funcionamento entre os dois protocolos. Brito (2013 p.133): “[...] segurança não era um requisito de projeto na concepção do IPv4 [...]”.

Kurose (2010, p.269): “[...] O IPv4 foi projetado em uma era (anos 1970) em que a Internet era utilizada primordialmente, entre pesquisadores de rede mutuamente confiáveis.”

2 - PROTOCOLO IPv6

O protocolo IPv6, definido pela RFC (*Request for Comments*) 2460, foi projetado com a principal finalidade de resolver o problema de escassez de endereços IPv4. Aproveitando o desenvolvimento do novo protocolo os projetistas adicionaram novos recursos que antes não existiam no IPv4.

Brito (2013) afirma que, as principais vantagens que o IPv6 oferece são: Espaço quase “ilimitado” de endereços, cabeçalho simplificado e de tamanho fixo, processamento simplificado nos roteadores, recomendações internacionais de agregação de prefixos, dispensa adoção de NAT, segurança embutida (nativa) com o IPSec e suporte à mobilidade MIPv6 (*Mobile IPv6*).

2.1 - Cabeçalho IPv6

Tanenbaum (2011) disse que, o cabeçalho do protocolo IPv6 foi simplificado e possui oito campos contra os treze do protocolo IPv4. Com essa simplificação os roteadores são capazes de processar os datagramas com agilidade, melhorando o *throughput* (vazão) e o atraso.

Brito (2013) também disse que, o cabeçalho do protocolo IPv6 foi reestruturado para possibilitar maior otimização, o cabeçalho foi reduzido para oito campos. Os campos excluídos foram: Tamanho do Cabeçalho (IHL), Identificação, *Flags*, Deslocamento do Fragmento, Soma de Verificação no Cabeçalho (*Checksum*) e Opções + Complemento. Agora o IPv6 possui tamanho de cabeçalho fixo em 40 bytes, com isso os roteadores não precisam analisar o extinto campo IHL otimizando o repasse dos pacotes. A figura 3 mostra o cabeçalho do protocolo IPv6.

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)		
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				

Figura 3 - Cabeçalho do Protocolo IPv6

Fonte: <http://ipv6.br/entenda/cabecalho>

Tanenbaum (2011) afirma que: O campo Versão indica o tipo de pacote, para o IPv6 o valor é 6 e para o IPv4 o valor é 4. O campo Classe de Tráfego tem a mesma função que no protocolo IPv4, que é de marcar o pacote de acordo com a classe de serviço. O campo Identificador de Fluxo permite que os *hosts* de origem e destino marquem grupos de pacotes que necessitam de mesmo tratamento especial pela rede. O campo Tamanho dos Dados indica o tamanho da carga útil que segue o cabeçalho. O campo Próximo Cabeçalho informa, se houver, qual cabeçalho de extensão segue o cabeçalho IPv6, se não houver, o pacote é encaminhado para a camada de transporte. O campo Limite de Encaminhamento tem a mesma função que o campo TTL do IPv4, decrementando um campo a cada salto. Os campos Endereço de Origem e Endereço de Destino contêm 16 bytes, ou seja, 2^{128} endereços.

Brito (2013 p.44): No IPv6, as funcionalidades que anteriormente eram utilizadas por meio do campo de opções estão a cargo de novos cabeçalhos adicionais denominados cabeçalhos de extensão, sendo que esses cabeçalhos não precisam ser verificados pelos roteadores intermediários na comunicação entre

dois nós, o que reflete em melhor desempenho na rede decorrente de menor processamento nos roteadores.

Brito (2013) disse que, os cabeçalhos de extensão são anexados ao cabeçalho base do IPv6 de forma encadeada através do campo próximo cabeçalho de cada cabeçalho de extensão. A tabela 2 mostra a ordem que os cabeçalhos de extensão devem seguir e o seu respectivo código, a figura 4 mostra o seu encadeamento.

Tabela 2 - Ordem dos Cabeçalhos de Extensão

Ordem	Nome do cabeçalho	Código no campo “Nex Header”
01	Cabeçalho IPv6 convencional	-
02	Hop-by-Hop	0
03	Destination Options	60
04	Routing Header	43
05	Fragment Header	44
06	Authentication Header (AH)	51
07	Encapsulation Security Payload (ESP)	50
08	Destination Options	60
09	Mobility	135
-	Ausência de próximo cabeçalho	59
Camada superior	ICMPv6	58
Camada superior	UDP	17
Camada superior	TCP	6

Fonte: Adaptado de Brito (2013, p.45)

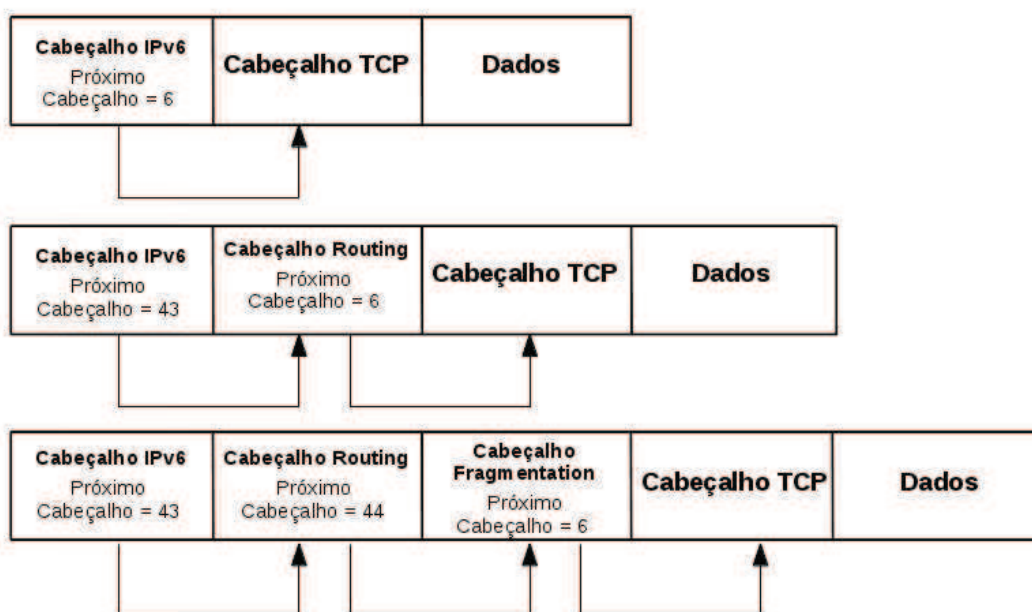


Figura 4 - Encadeamento dos Cabeçalhos de Extensão

Fonte: <http://ipv6.br/entenda/cabecalho>

2.2 - Endereçamento IPv6

O protocolo IPv6 possui 128 bits disponíveis para endereçamento, com esses bits são possíveis 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) de endereços.

Florentino (2012, p.35) disse que “[...] se convertêssemos cada IPv6 possível em um cm^2 , poderíamos envolver toda a superfície do planeta Terra com 7 camadas de endereços.” Brito (2013) também disse que, se considerarmos que o planeta Terra tenha 10 bilhões de habitantes, cada habitante poderia ter 3,4 oitilhões de endereços o equivalente a $3,4 \times 10^{27}$ endereços. Ainda Tanenbaum (2011, p.288): “Se o planeta inteiro, terra e água, fosse coberto de computadores, o IPv6 permitiria 7×10^{23} endereços IP por metro quadrado.”

Bruto (2013) e Florentino (2012), o endereço IPv6 é representado por símbolos hexadecimais, são 8 blocos de 16 bits separados pelo caractere “:”, os valores variam de 0000 a FFFF. Um exemplo de endereço IPv6 é 2001:0DB8:CAFE:B01A:C0CA:BE00:B0B0:B0CA.

Para facilitar a nomenclatura e entendimento algumas regras de escrita do endereço foram definidas. Brito (2013) e Florentino (2012), zeros à esquerda podem ser omitidos e zeros contínuos podem ser substituídos pelos caracteres “::”.

O endereço 2001:0DB8:00AD:000F:0000:0000:0000:0001 pode ser representado de duas formas como mencionado, omitindo os zeros à esquerda 2001:DB8:AD:F:0:0:0:1 e substituindo os zeros contínuos pelos símbolos “::” 2001:DB8:AD:F::1.

No IPv6 devido ao tamanho de seu endereço não é usada a máscara de rede, usa-se a notação CIDR como em: 2001:0DB8:00AD:000F:0000:0000:0000:0001/64.

Brito (2013 p.56) afirmou que: [...] é mandatório a utilização da notação CIDR. Isso faz todo sentido, porque os endereços são grandes e as máscaras seriam muito extensas, imaginem ter que escrever a máscara de um prefixo /64: ffff:ffff:ffff:ffff:0000:0000:0000:0000.

Brito (2013 p.56) disse que: Era comum determinar o prefixo das redes IPv4 a partir da quantidade de *hosts* necessários em cada sub-rede para fins de economia de endereços. Acontece que, com o IPv6, todas as redes locais devem ser necessariamente /64 (RFC 4291).

Conforme Brito disse, um usuário doméstico terá no mínimo um bloco de endereço /64, ou seja, são 64 bits fixo para a rede e 64 bits para trabalhar o endereçamento dos *hosts*, com isso um usuário doméstico terá 18,4 quintilhões de endereços globais válidos roteáveis na Internet disponíveis em sua rede local. A figura 5 ilustra a estrutura do endereço IPv6.



Figura 5 - Estrutura do Endereço IPv6

Fonte: Brito (2013, p.56)

Segundo Florentino (2012 p.35) “Com o IPv6, é necessário pensar somente na quantidade de redes que podem ser oferecidas ao usuário final.”

Kurose (2006): Além dos endereços *multicast* e *unicast*, o IPv6 introduziu um novo endereço o *anycast*, que permite que um pacote IP seja entregue a qualquer *host* de um determinado grupo, por exemplo, uma mensagem HTTP GET pode ser enviada ao site mais próximo de um grupo de sites espelhados que contenham um determinado documento.

2.3 - Funcionalidades Básicas do IPv6

Brito (2013) afirma que: O ICMPv6 (*Internet Message Control Protocol version 6*) é de suma importância para o funcionamento do protocolo IPv6. Ainda Brito (2013), o ICMPv6 não é somente responsável pelo diagnóstico de rede como ocorria com o ICMPv4 (*Internet Control Protocol version 4*), agora o ICMPv6 assume funções de extrema importância para o funcionamento do IPv6 que antes eram realizadas por outros protocolos no IPv4.

2.4 - ICMPv6

Brito (2013) disse que: O ICMPv6 é responsável por funcionalidades de comunicações entre *hosts* vizinhos, essas funcionalidades são importantes para o bom funcionamento da rede, as mensagens ICMPv6 não podem ser bloqueadas pelos firewalls como era feito com o protocolo ICMPv4. Brito (2013) também afirma que: Os protocolos ARP (*Address Resolution Protocol*), RARP (*Reverse Address Resolution Protocol*) e IGMP (*Internet Group Management Protocol*) não existem mais no IPv6.

Brito (2013, p.77) O ICMPv6 é integrado ao IPv6 por meio da sinalização do código 58 no campo “Próximo Cabeçalho” do cabeçalho convencional do IPv6. [...] Ele contém dois campos de tipo/código para representar o formato das mensagens de controle, um campo de verificação de erros para checar a integridade das mensagens de controle e um campo de tamanho variável com a mensagem propriamente dita.

A figura 6 ilustra o cabeçalho do protocolo ICMPv6.

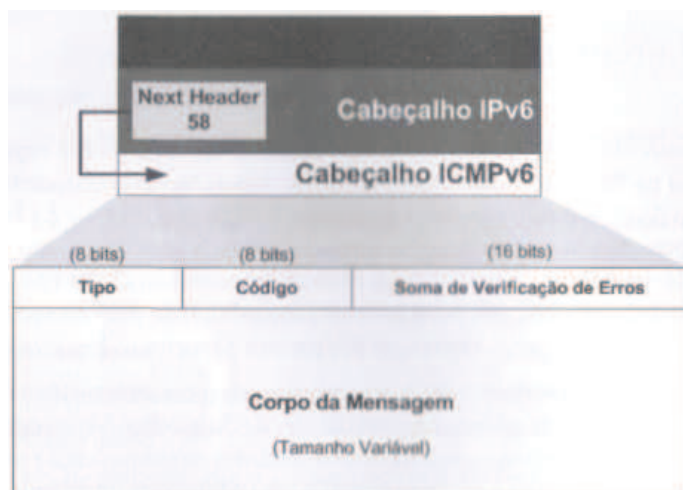


Figura 6 - Cabeçalho do ICMPv6

Fonte: Brito (2013, p.78)

2.5 - Neighbor Discovery Protocol

Brito (2013) afirmou que: O NDP (*Neighbor Discovery Protocol*) é responsável por muitas funcionalidades, por isso ele é parte importante do protocolo IPv6. O NDP opera a partir do ICMPv6.

Equipe IPv6.br (2012): O protocolo NDP atua sobre duas formas na comunicação IPv6, na autoconfiguração de nós e a na transmissão de pacotes. No caso da autoconfiguração de nós o NDP oferece suporte a três funcionalidades:

- *Parameter Discovery* (Descoberta de Parâmetros do Enlace): Atua na descoberta por um nó de informações sobre o enlace (como MTU) e sobre a Internet (como *hop limit*);
- *Address Autoconfiguration* (Autoconfiguração de Endereços): Trabalha na autoconfiguração *stateless* de endereços na interface de um nó;
- *Duplicate Address Detection* (Detecção de Endereços Duplicados): Utilizado para descobrir se o endereço que se deseja atribuir a uma interface já está sendo usado por um outro nó na rede.

Já no caso da transmissão de pacotes o suporte é dado a seis funcionalidades:

- *Router Discovery* (Descoberta de Roteadores): Trabalha com a descoberta de roteadores pertencentes ao enlace;
- *Prefix Discovery* (Descoberta de Prefixo): Realiza a descoberta de prefixos de redes no enlace;
- *Address Resolution* (Resolução de Endereços): Descobre um endereço físico (MAC) através de um endereço lógico IPv6;
- *Neighbor Unreachability Detection* (Detecção de Atividade no Vizinho): Permite que os nós descubram se um vizinho é ou se continua alcançável.
- *Redirect* (Redirecionamento de Roteadores): Permite ao roteador informar ao nó uma rota melhor a ser utilizada para enviar pacotes a determinado destino.
- *Next-Hop Determination* (Determinação do Próximo Salto): Algoritmo para mapear um endereço destino em um endereço IP de um vizinho para onde o tráfego deve ser enviado.

A tabela 3 mostra os tipos de mensagens ICMPv6 do protocolo NDP utilizadas para descoberta de vizinhança.

Tabela 3 - Mensagens ICMPv6 do NDP

Tipo	Mensagem	Descrição
133	RS – Router Solicitation	Enviada pelos <i>hosts</i> para encontrar roteadores
134	RA – Router Advertisement	Enviada periodicamente pelos roteadores
135	NS – Neighbor Solicitation	Enviado para obter informações de vizinhança
136	NA – Neighbor Advertisement	Enviada por um <i>host</i> como resposta à solicitação
137	Redirect	Enviado por roteadores para redirecionar rota

Fonte: Adaptado de Brito (2013, p.82)

2.6 - Segurança IPv6

O protocolo IPv6 oferece segurança nativa graças ao protocolo IPSec fazer parte da pilha de protocolos TCP/IPv6.

Brito (2013): O IPv6 é mais robusto que o IPv4. No projeto do protocolo IPv4 não foi proposto nenhum método de segurança, ao contrário do IPv6 onde a segurança foi um dos principais motivos pela concepção do novo protocolo.

Brito (2013 p.133): “[...] a segurança foi um dos critérios mais relevantes na escolha da proposta que daria origem ao [...] IPv6.”

O IPv6 não faz uso do NAT, isso é possível graças a abundância de endereços IPv6 disponíveis.

Um grande problema que os ISPs têm desde muitos anos é a identificação de *hosts* que fazem uso do NAT. Com o uso do NAT fica difícil identificar os *hosts* na Internet. Imaginemos um ISP com milhares de *hosts* em sua rede utilizando NAT, um desses *hosts* está infectado e gerando um ataque a um servidor qualquer na Internet. De onde está saindo esse ataque? A resposta é: De um endereço IP público. Se essa empresa for notificada sobre esse incidente ela deverá fazer uma verificação árdua em sua rede para verificar qual *host* é o responsável pelo incidente.

Para Tanenbaum (2011), NAT é a tradução de endereços privados em endereços públicos, cada usuário ou corporação recebe um único ou poucos endereços IPs públicos para se conectarem a Internet, internamente na rede local os *hosts* recebem um endereço para uso exclusivo em redes locais para roteamento de tráfego interno, quando um *host* precisa se conectar a Internet, deve acontecer à tradução desse endereço privado em endereço público. O NAT está descrito na RFC 3022.

Kurose (2006) disse que: Alguns membros da IETF (*Internet Engineerig Task Force*) têm restrições ao NAT dizendo que a finalidade dos números de portas é endereçar processos e não *hosts*. Argumentam ainda que roteadores tenham que processar apenas pacotes da camada de rede. O protocolo NAT viola o modelo fim-a-fim. Ainda afirmam que deveríamos deixar de utilizar soluções para postergar a implantação do protocolo IPv6.

2.6.1 - IPSec

O IPSec é um protocolo capaz de prover segurança na camada três do modelo OSI (*Open Systems Interconnect*), ele já era utilizado sobre IPv4 porém, com o IPv6 o IPSec se torna nativo. Brito (2013): O IPv6 possui segurança nativa onde o protocolo IPSec faz parte da suíte de protocolos TCP/IPv6. Com isso qualquer equipamento que tenha suporte ao IPv6 automaticamente também terá suporte ao IPSec, o que não ocorre com o IPv4, onde o profissional responsável pela configuração do equipamento tem de verificar o suporte ao IPSec.

Brito (2013): O IPSec (RFC 4301) é um protocolo que opera na camada de rede provendo segurança, o IPSec pode também operar diretamente nos *hosts*, isso é possível graças a eliminação do NAT.

Equipe IPv6.br (2012): O IPSec foi desenvolvido para funcionar com IPv6, porém mesmo não sendo compatível com NAT ele foi adaptado para funcionar também com o IPv4, mas sendo pouco utilizado devido essa incompatibilidade.

Equipe IPv6.br (2012) ainda afirma que: Mesmo o IPSec não sendo compatível com o NAT, existe a possibilidade de utilizar o NAT encapsulando todo o pacote IPv4 em um novo pacote não alterando o endereço do pacote original, o pacote deverá ser desencapsulado no destino. Devemos sempre lembrar que, essas são medidas paliativas, o que devemos fazer é adotar o novo protocolo de Internet IPv6.

Brito (2013), afirma que: Com o IPv6 a comunicação fim-a-fim volta a funcionar devido a não implementação do NAT, com isso o IPSec passa a funcionar melhor, porque os cabeçalhos de extensão são manipulados apenas pela origem e destino, toda informação criptografada ficará inacessível para os roteadores intermediários.

Kurose (2010, p.526): “O IPSec protege os datagramas IP entre quaisquer entidades da camada de rede, incluindo hospedeiros e roteadores.”

A grande vantagem de prover segurança na camada de rede é que a segurança é transparente para o usuário, o usuário não precisa realizar nenhum tipo de configuração. Outra vantagem, nas camadas superiores não é realizada qualquer tipo de alteração, sendo assim, não a necessidade de alteração no código das aplicações.

Tanenbaum (2011): Realizar a codificação na camada de rede não impediria que usuários preocupados com a segurança a implementasse também na camada de aplicação, isso também beneficiaria os usuários sem consciência da segurança.

Kurose (2010) afirma que: O IPSec oferece mecanismos para sigilo, autenticação da fonte, integridade dos dados e prevenção do ataque de repetição.

2.6.2 – *Security Association (SA)*

Segundo Moraes (2010): Uma SA é um acordo estabelecido entre dois *hosts* antes da comunicação IPSec. Nesse acordo são negociados os parâmetros IPSec.

Na SA são negociados os seguintes mecanismos de segurança:

- Modo do túnel IPSec: ESP ou AH;
- Algoritmo de criptografia;
- Método de Autenticação;
- Função hashing;
- Método de autenticação do usuário: RADIUS, SecurID;
- Escolha das chaves criptográficas e chaves de autenticação.

2.6.3 – *Internet Key Exchange (IKE)*

Moraes (2010) disse que: A função do protocolo IKE é negociar e fornecer segurança para as SAs IPSec. Os pacotes IKE são transportados sobre UDP (*User Datagram Protocol*) e fazem uso das portas de origem e destino número 500.

Ainda Moraes (2010): O protocolo IKE define duas fases:

- Fase 1: Para definir uma associação de segurança IP, os dois pontos devem primeiro estabelecer um canal seguro, devendo assim:

Acordar o método de autenticação;

Selecionar os algoritmos de autenticação e encriptação;

Trocar as chaves;

Verificar as identidades de cada uma das partes.

O canal de segurança é estabelecido a partir de uma associação de segurança chamada ISAKMP (*Internet Security Association and Key Management Protocol*).

- Fase 2: Após estabelecimento do canal seguro ISAKMP a SA é negociada. Todo pacote trocado na fase 2 é autenticado e encriptado de acordo com as chaves e algoritmos definidos na fase 1

2.6.4 – Cabeçalhos de Segurança IPv6

O protocolo IPv6 faz uso dos cabeçalhos de extensão AH (*Authentication Header*) e ESP (*Encapsulating Security Payload*), como vimos na tabela 2.

Brito (2013, p.49): “[...] os cabeçalhos de extensão AH e ESP são importantes para viabilizar as soluções de autenticação, integridade e confidencialidade (criptografia).”

Brito (2013): Os protocolos AH e ESP são responsáveis pelo suporte nativo do IPsec ao IPv6. Ainda Brito (2013): O suporte nativo ao IPsec trouxe funcionalidades de segurança que com o IPv4 dependiam de soluções externas. Os protocolos de roteamento dinâmico implementavam soluções de segurança independentes, porém com a utilização dos protocolos AH e ESP, essas funcionalidades foram removidas da estrutura interna dos protocolos de roteamento.

Tanenbaum (2011): O cabeçalho AH fornece verificação de integridade e segurança contra ataques de reprodução, porém não oferece criptografia. A verificação do AH inclui alguns campos do cabeçalho IP, como o campo endereço de origem, o que torna impossível um atacante falsificar a origem de um pacote.

A figura 7 mostra o cabeçalho de extensão AH.

Próximo Cabeçalho	Comprimento do Payload	Reservado
SPI		
Sequence Number		
Dados de Autenticação		

Figura 7 - Cabeçalho AH

Fonte: Adaptado de <http://www.rnp.br/newsgen/9907/ipsec3.html>

Conforme a figura 7, os campos que constituem o cabeçalho AH são:

- Próximo Cabeçalho: Informa qual o próximo cabeçalho na cadeia de cabeçalhos de extensão;
- Comprimento do *Payload*: Indica o comprimento do conteúdo do cabeçalho;
- Reservado: Reservado para extensão do protocolo, uso futuro;
- SPI (*Security Parameter Index*): Este índice em conjunto com o endereço origem, identifica unicamente uma AS para um determinado pacote;
- *Sequence Number*: Contador que identifica unicamente os pacotes de uma determinada AS (usado contra ataques de reprodução);
- Dados de Autenticação: Campo de comprimento variável que contém o ICV (*Integrity Check Value*) para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela AS.

Silva; Teixeira (1999), afirmam que: O uso do AH previne os seguintes tipos de ataques:

- *Replay*, quando um atacante captura um pacote, duplica e reenvia. A utilização do campo *Sequence Number* ajuda a prevenir este tipo de ataque enumerando os pacotes trafegados;
- *Spoofing*, a autenticação previne esse ataque;
- Roubo de Conexões, quando um atacante captura pacotes numa conexão e passa a participar da comunicação. A autenticação previne esse ataque.

Ainda Silva; Teixeira (1999): O protocolo ESP provê autenticação e confidencialidade, permitindo que somente quem estiver autorizado terá acesso ao conteúdo do pacote. A figura 8 mostra o cabeçalho de extensão ESP.

SPI
Sequence Number
Dados Cifrados e Parâmetros
Dados de Autenticação

Figura 8 - Cabeçalho ESP

Fonte: Adaptado de <http://www.rnp.br/newsgen/9907/ipsec3.html>

Conforme a figura 8, os campos que constituem o cabeçalho ESP são:

- **SPI** (*Security Parameter Index*): Este índice em conjunto com o endereço origem, identifica unicamente uma AS para um determinado pacote;
- **Sequence Number**: Contador que identifica unicamente os pacotes de uma determinada AS (usado contra ataques de reprodução);
- **Dados Cifrados e Parâmetros**: Contém os dados cifrados e os parâmetros utilizados pelo algoritmo de criptografia usado, definido pela AS.
- **Dados de Autenticação**: Campo de comprimento variável que contém o ICV para este pacote, que é calculado seguindo o algoritmo de autenticação usado, definido pela AS.

O ESP previne ataques como:

- **Replay**, através da utilização do campo *Sequence Number*;
- **Particionamento de Pacotes Cifrados**, acontece quando um invasor captura pacotes cifrados e consegue montar pacotes que podem ser aceitos por membros da conexão;

- *Sniffer*, acontece quando um atacante captura pacotes que trafegam na rede, pode ser evitado utilizando a criptografia, mesmo que o atacante capture o pacote ele não conseguirá decifrar o seu conteúdo.

O IPSec pode operar em dois modos, transporte e túnel.

Brito (2013): No modo transporte a criptografia acontece apenas nos dados do datagrama, o cabeçalho da camada de rede continua sem alteração (não é criptografado), com isso é possível o roteamento do pacote na Internet. O modo de operação transporte é comum em comunicações *host-to-host*. A figura 9 mostra a operação do IPSec em modo transporte.

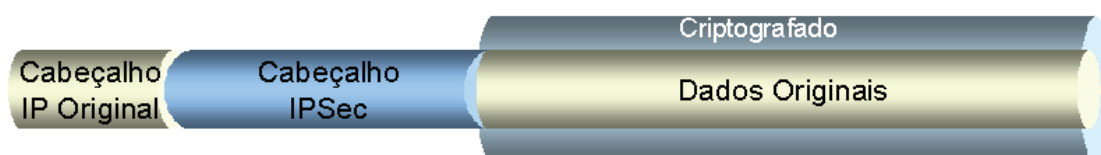


Figura 9 - IPSec Modo Transporte

Fonte: http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana

Brito (2013): No modo túnel, todo o datagrama é cifrado desde o cabeçalho IP até os dados. Um novo cabeçalho é inserido ao datagrama para que seja possível o roteamento na Internet. O modo túnel é utilizado em comunicações *site-to-site*, onde os roteadores de borda estabelecem uma VPN (*Virtual Private Network*). A figura 10 mostra a operação do IPSec em modo túnel.



Figura 10 - IPSec Modo Túnel

Fonte: http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana

Silva; Teixeira (1999): Em ambiente onde é exigida apenas autenticação o uso do AH é indicada. O indicado é a utilização do AH com ESP ou ainda, a utilização do ESP

encapsulado pelo AH, como mostra a figura 11, permitindo que o remetente verifique a autenticidade do pacote antes de ser descriptografado, ou ainda verifique a autenticidade e descriptografe o pacote paralelamente.

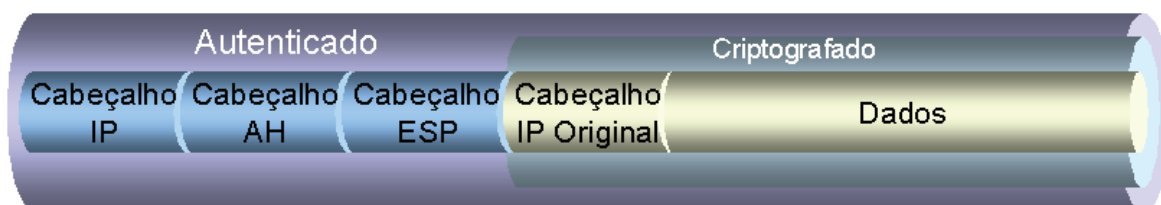


Figura 11 - Cabeçalho ESP encapsulado pelo AH

Fonte: http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana

3 – ESTUDO DE CASO

O estudo de caso tem o objetivo de analisar a implementação do protocolo IPSec em redes IPv4 e IPv6, possibilitando uma discussão acerca do assunto.

No estudo de caso foi implementado o protocolo IPSec em redes IPv4 e IPv6 através de laboratório, utilizando-se VMs (*virtual machines*). Foi definida a escolha do protocolo IPSec devido os autores referenciados neste trabalho e entre outros defenderem que o IPSec é nativo ao protocolo IPv6 e que devido a isso o IPv6 passa a ter segurança nativa na camada de rede.

3.1 – Requisitos de Software

Os softwares utilizados foram:

- SO (Sistema Operacional) Microsoft Windows 8.1, x64;
- SO Microsoft Windows 7, Service Pack 1, x86;
- Emulador de SO em VMs Oracle VirtualBox, Versão 4.3.14;
- IIS (*Internet Information Services*) versão 7.5.7600.16385 com o serviço FTP (*File Transfer Protocol*) configurado;
- Analisador de Protocolo de Rede Wireshark, Versão 1.12.0.

3.2 – Requisitos de Hardware

O hardware utilizado foi um notebook, cujas as especificações são:

- Marca e modelo DELL Inspiron 14 Série 3000;
- Memória 4GB, Single Channel DDR3, 1600MHz (1x4Gb);
- Placa de vídeo Intel® HD Graphics Integrada;

- Disco Rígido de 1TB, SATA (5400 RPM);
- 4ª Geração do Processador Intel® Core™ i5-4210U (até 2.7 GHz, 3Mb Cache).

3.3 – Ambiente de Teste

No notebook com o SO Microsoft Windows 8.1 foi instalado a aplicação de virtualização Oracle Virtual Box. Na aplicação de virtualização foi configurado duas VMs com o SO Microsoft Windows 7.

As duas VMs foram conectadas pela rede interna do software de virtualização através da topologia de rede *host-to-host*. A figura 12 mostra a topologia de rede utilizada.



Figura 12 - Topologia de Rede *host-to-host*

3.3.1 – Configuração IPSec

O protocolo IPSec foi configurado em modo transporte nas duas VMs utilizando-se o snap-in “Diretiva de Segurança Local”. O modo transporte é utilizada em topologia de rede *host-to-host*.

No menu “Iniciar” na caixa de pesquisa devemos digitar “diretiva de segurança local” e teclar “Enter” conforme a figura 13.

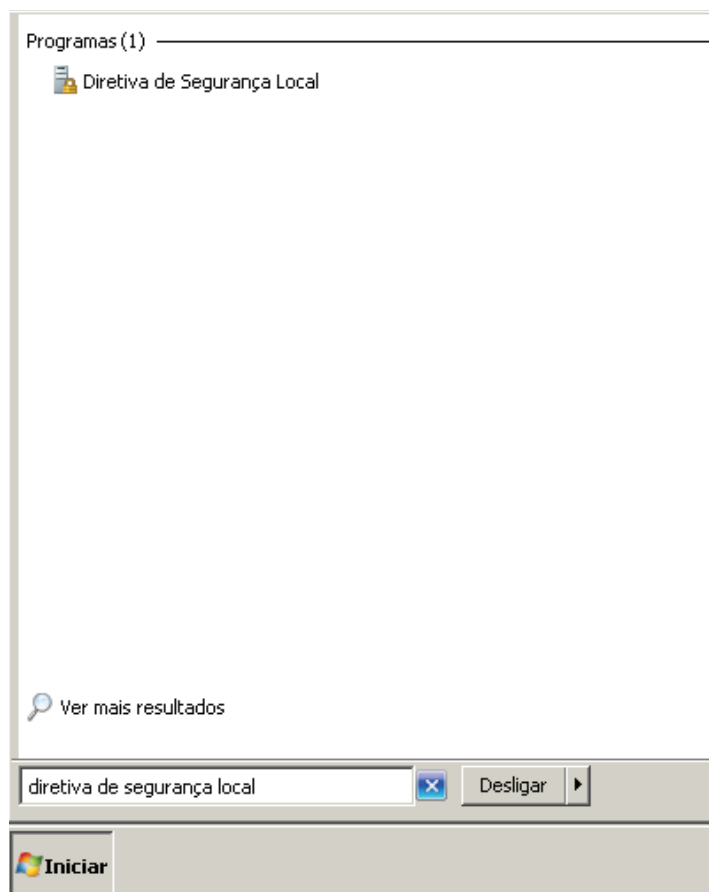


Figura 13 - Iniciando a Diretiva de Segurança Local

Em “Diretivas de segurança IP em Computador local” clicamos com o botão direito do *mouse* e selecionamos “Criar diretiva de segurança IP...”, ver figura 14.

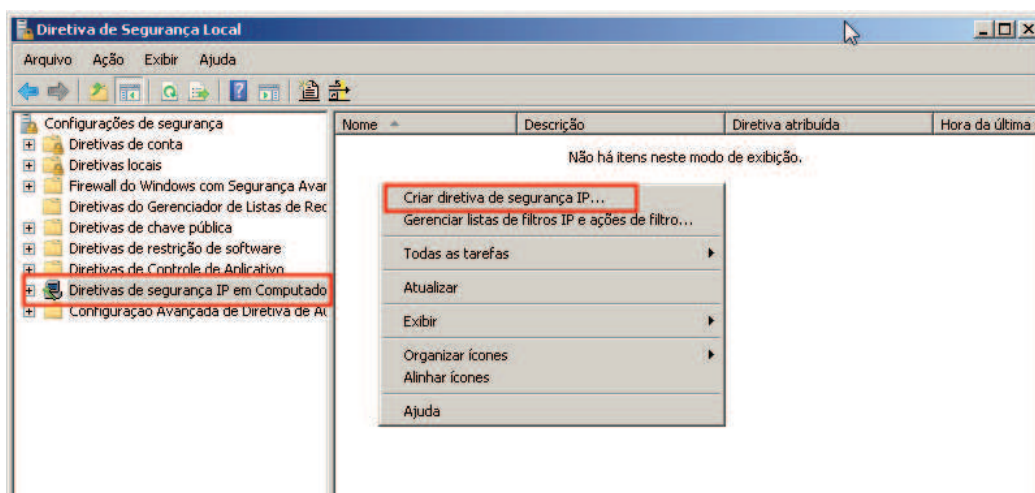


Figura 14 - Diretiva de Segurança Local

Na tela seguinte clicamos em “Avançar”, ver figura 15.

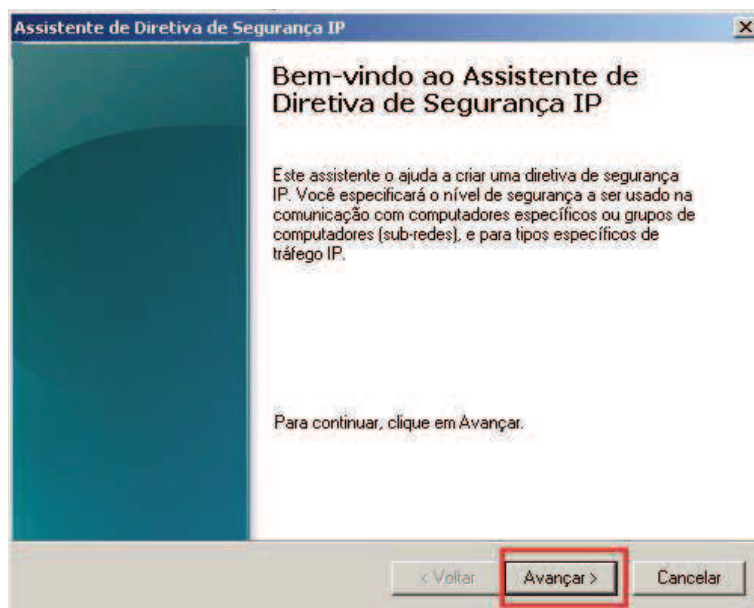


Figura 15 - Assistente de Diretiva de Segurança IP

Na figura 16 devemos fornecer o nome e a descrição da política e clicar em “Avançar”.

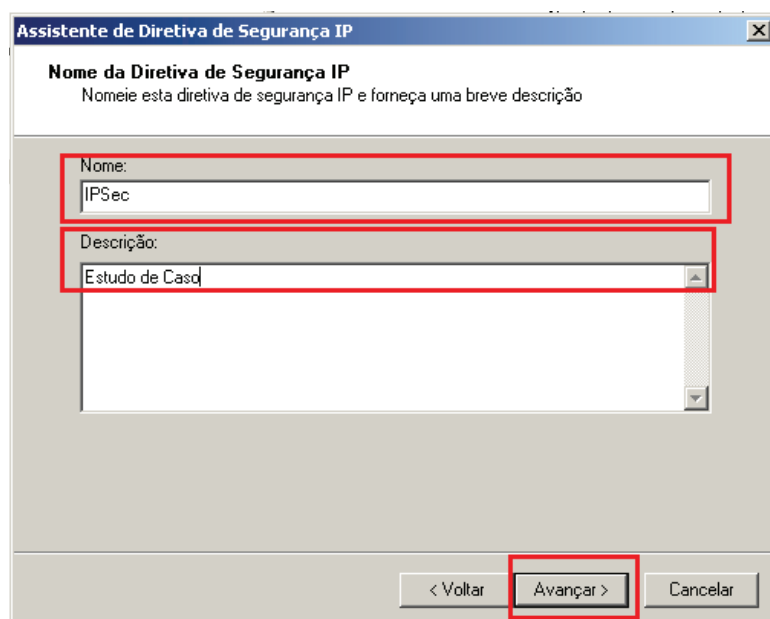


Figura 16 - Nome de Diretiva de Segurança IP

Na tela seguinte não marcamos nada, porque queremos que apenas as regras que criemos entre em vigor, clicamos apenas em “Avançar”, ver figura 17.

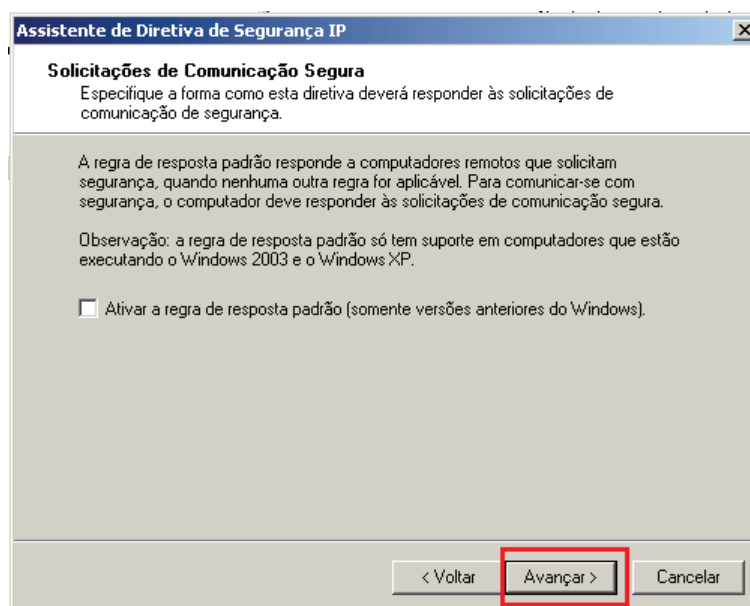


Figura 17 - Solicitação de Comunicação Segura

Na tela seguinte deixamos marcado a opção “Editar propriedades” e clicamos em “Concluir”, ver figura 18.

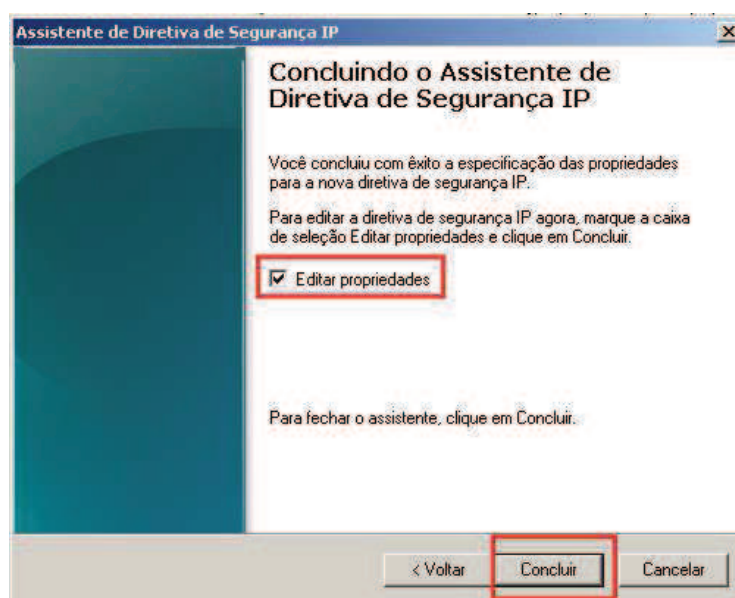


Figura 18 - Concluindo o Assistente de Diretiva de Segurança IP

Devemos agora criar um filtro IPSec, em regras desmarcamos a opção “Usar Assistente para Adicionar” e em seguida clicamos em “Adicionar...”, ver figura 19.

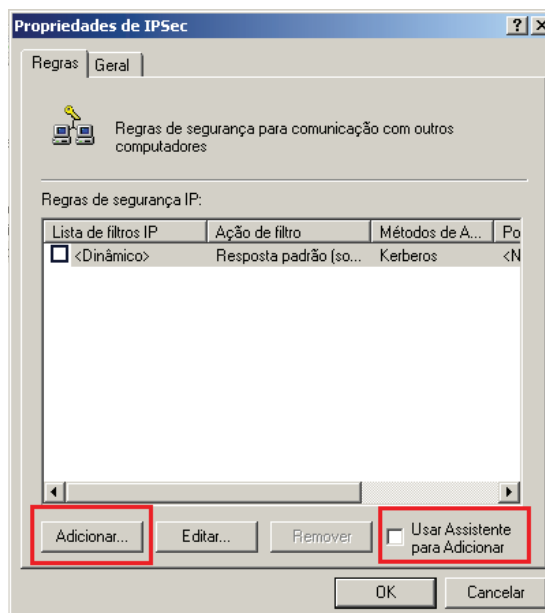


Figura 19 - Propriedades de IPSec

A figura 20 mostra onde iremos configurar as regras IPSec, através desta janela também é possível criar uma lista de filtros e definir a ação. Vamos criar um filtro clicando em “Adicionar...”.

Na próxima janela (figura 21) devemos dar nome ao filtro e realizar uma descrição, devemos desmarcar a opção “Usar Assistente para Adicionar” e clicar em “Adicionar...”.

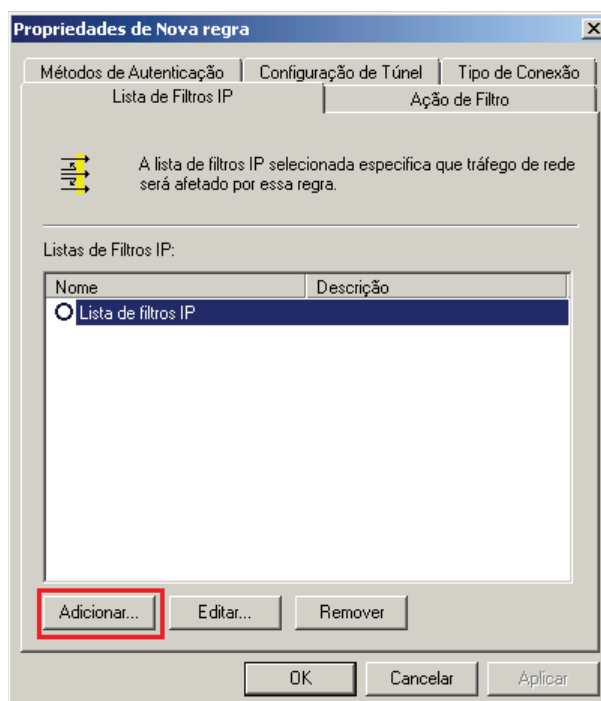


Figura 20 - Propriedades de Nova Regra

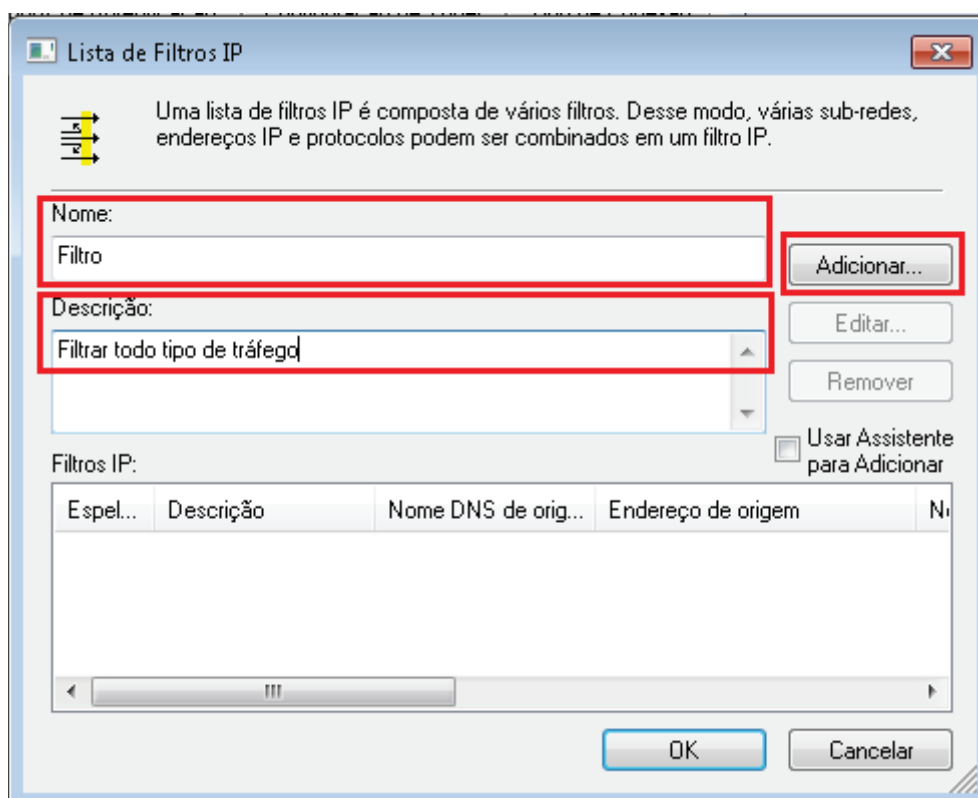


Figura 21 - Lista de Filtros IP

O próximo passo é configurar o endereço de origem e destino na aba “Endereços”, neste exemplo (figura 22) definimos os endereços como “Qualquer endereço IP”, isso significa que a regra será aplicada para qualquer endereço que esteja configurado nas interfaces de ambas as pontas, depois clicamos em “OK”.

Na aba “Protocolo” na opção “Selecione um tipo de protocolo:”, o protocolo foi definido como “Qualquer”, então todo o tráfego será submetido ao IPSec, ver figura 23.

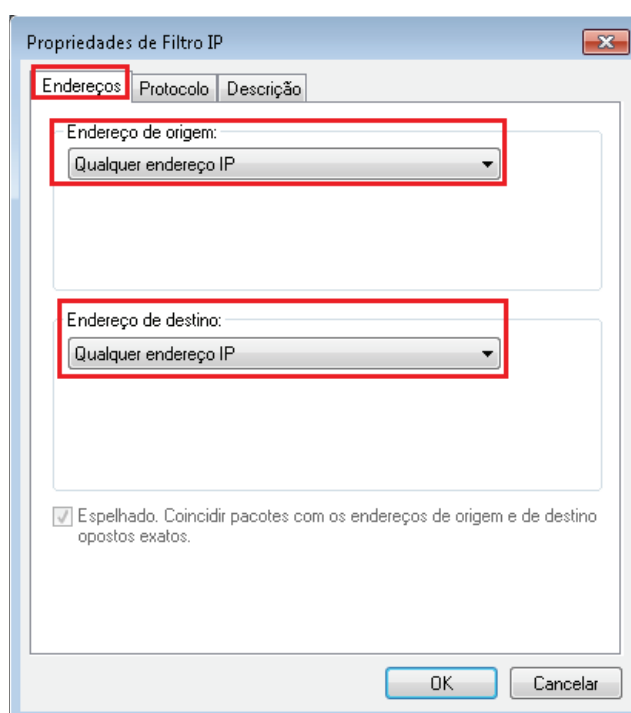


Figura 22 - Propriedades de Filtro IP

Na aba “Descrição” definimos uma descrição para o Filtro IP e depois clicamos em “OK”, ver figura 24.

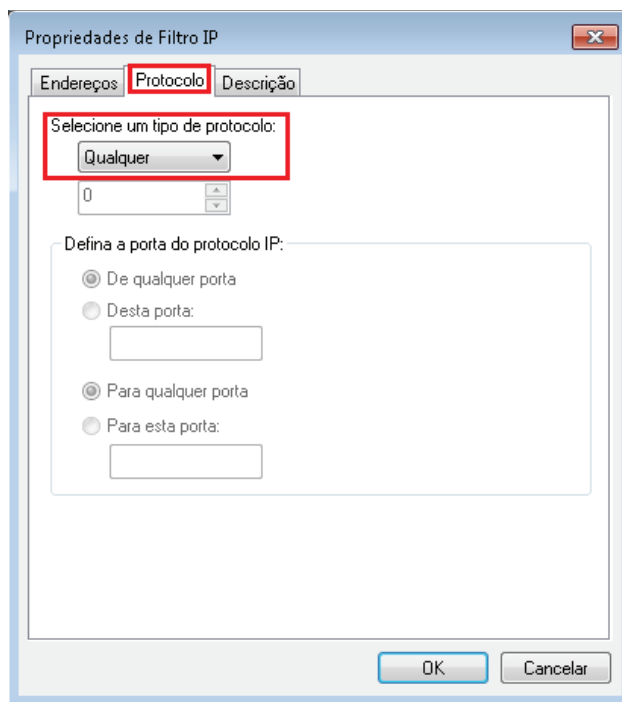


Figura 23 - Propriedades de Filtro IP – Protocolo

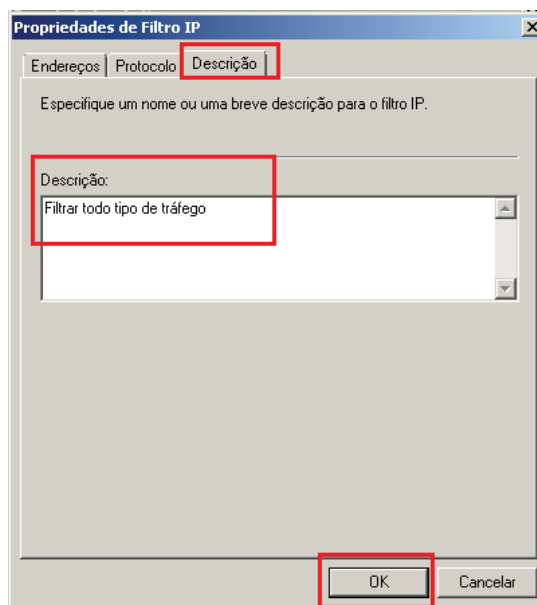


Figura 24 - Propriedades de Filtro IP – Descrição

Para finalizarmos clicamos novamente em ok, conforme a figura 25.

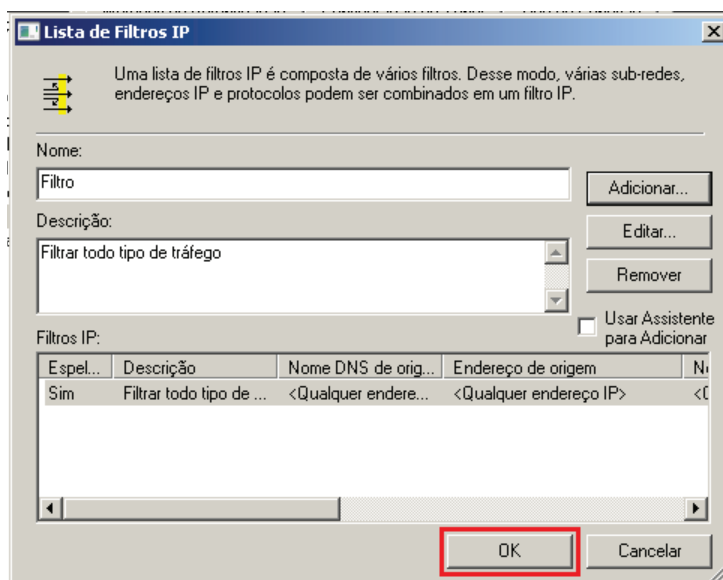


Figura 25 - Concluindo Lista de Filtro IP

Agora devemos selecionar o filtro criado e clicar em “Ação de Filtro” para configurarmos as ações que o filtro deverá executar, conforme a figura 26.

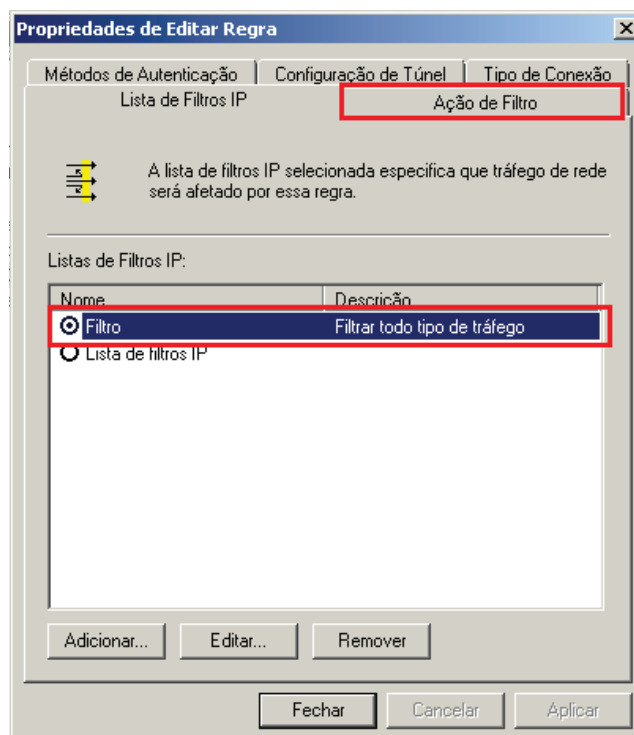


Figura 26 - Propriedades de Editar Regra

Na janela “Ação de Filtro” devemos desmarcar a opção “Usar Assistente para Adicionar” e clicar em “Adicionar...”, ver figura 27.

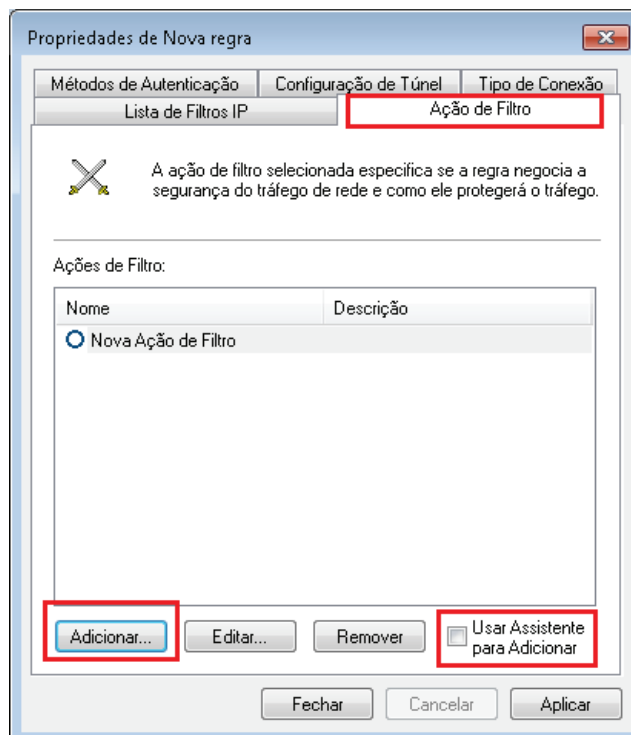


Figura 27 - Ação de Filtro

Na aba “Métodos de Segurança” selecionamos a opção “Negociar Segurança:” e clicamos em “Adicionar...”. Não devemos marcar nenhuma das demais opções conforme a figura 28.

Na aba “Método de Segurança”, após clicarmos em “Adicionar” devemos marcar a opção “Integridade e criptografia” e clicarmos na em “OK”, ver figura 29.

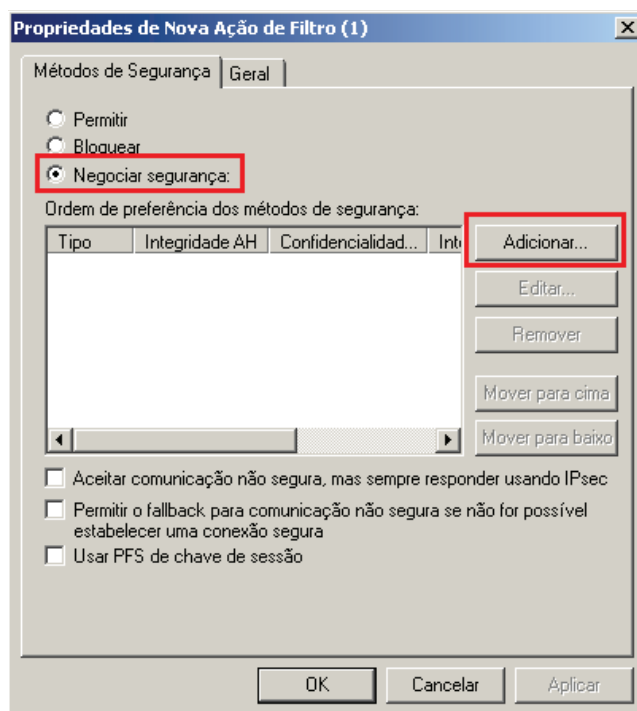


Figura 28 - Método de Ação de Filtro

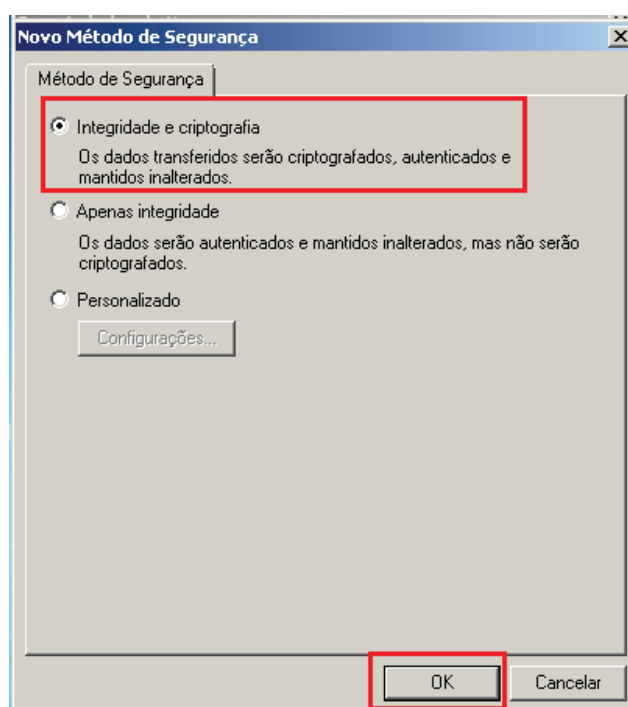


Figura 29 - Integridade e criptografia

Na aba “Geral” definimos o nome e a descrição para a ação de filtro, depois clicamos em “Aplicar” e em “OK”, ver figura 30.

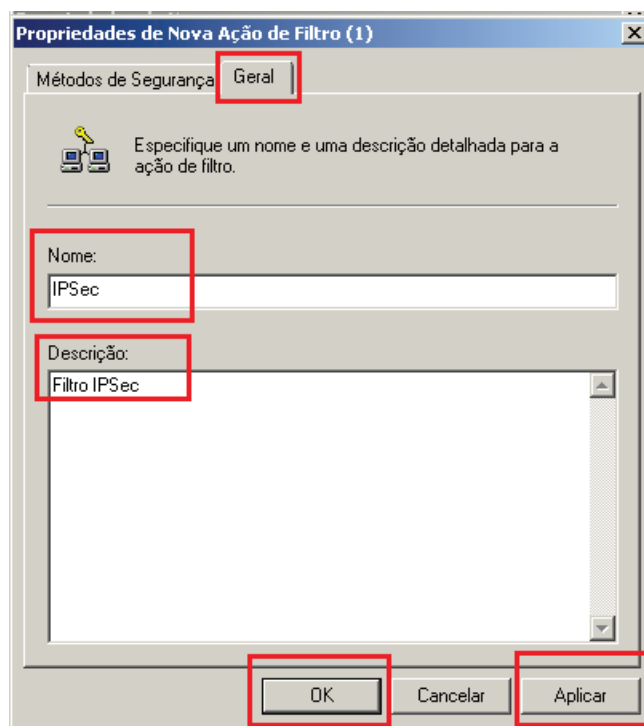


Figura 30 - Nome e Descrição para a Ação de Filtro

Na aba “Métodos de Autenticação” clicamos em “Adicionar” (figura 31), em seguida é aberta uma nova janela onde definiremos o método de autenticação que será utilizado na comunicação IPSec. Para ambiente de teste foi definido a troca de chave pré-compartilhada (figura 32) e definido a frase secreta “segurança_da_informação”, devemos clicar em “OK”.

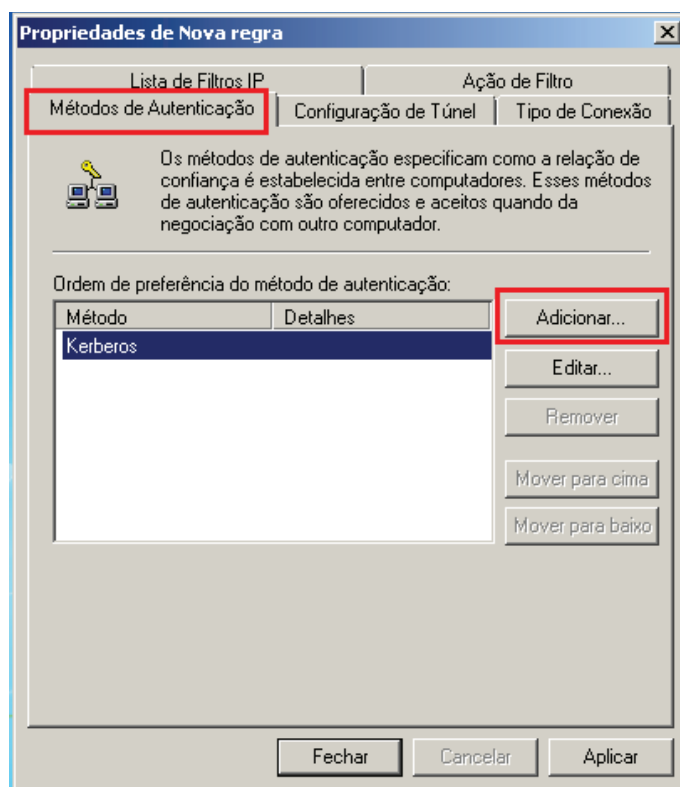


Figura 31 - Métodos de Autenticação

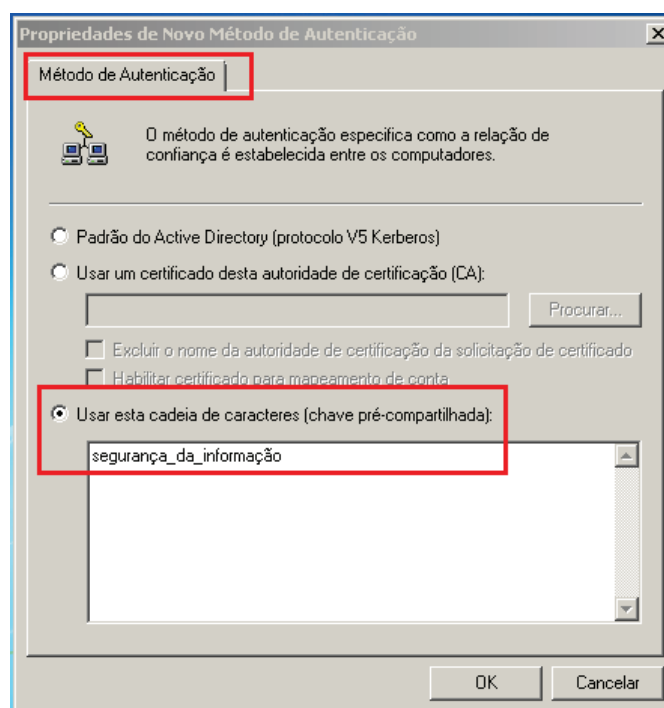


Figura 32 - Definindo um Método de Autenticação

Na aba “Configuração de Túnel” devemos manter marcada a opção “Esta regra não especifica um túnel IPsec.”, ver figura 33.

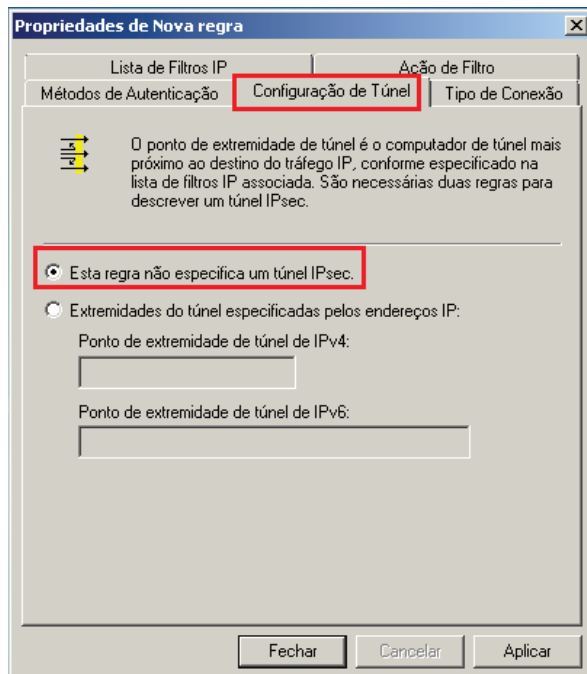


Figura 33 - Configuração de Túnel

Na aba “Tipo de Conexão” devemos marcar a opção “Todas as conexões de rede” e clicar em “Aplicar”, ver figura 34.

Retornamos a janela “Propriedades de IPsec” onde podemos visualizar o filtro que foi criado, devemos clicar em “Aplicar” e em “OK” para finalizarmos a configuração (figura 35). Então é apresentada novamente a janela “Diretiva de Segurança Local” com a diretiva IPsec que criamos, devemos selecionar a opção “Diretivas de segurança IP em Computador local” e clicar com o botão direito do *mouse* na diretiva IPsec criada e em “Atribuir” para podermos habilitar a diretiva, ver figura 36.

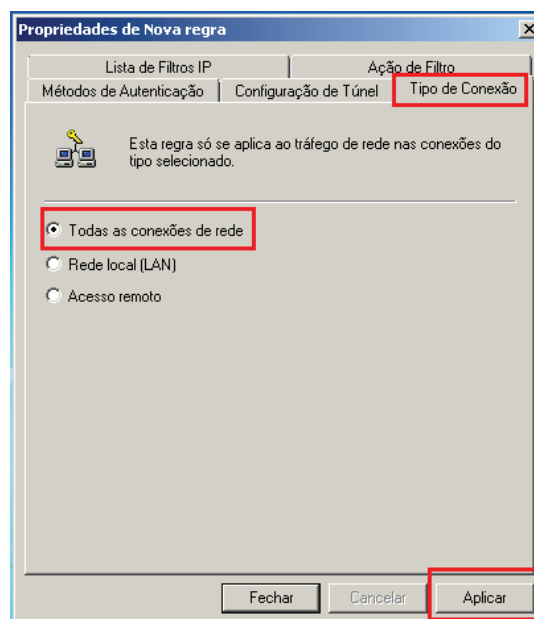


Figura 34 - Tipo de Conexão

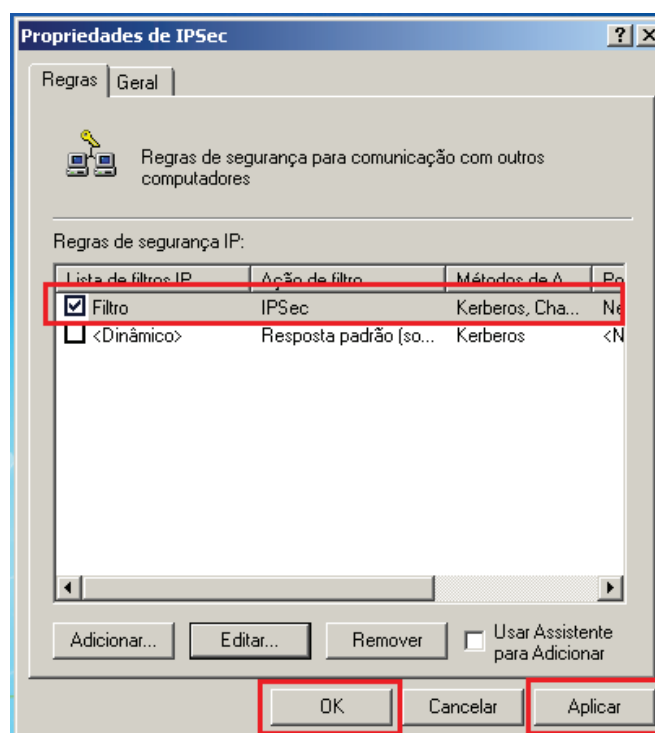


Figura 35 - Propriedades de IPSec após Configuração

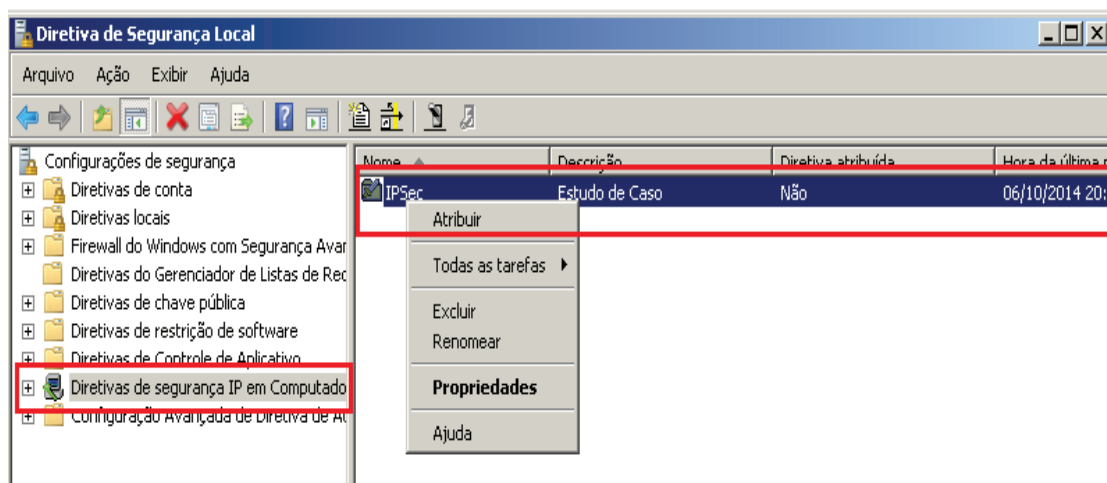


Figura 36 - Diretiva de Segurança Local após Configuração

3.3.2 – Testes

Após a configuração do ambiente vamos analisar o tráfego dos dados entre as duas VMs. O tráfego de dados será analisado utilizando os protocolos IPv4 e IPv6, sem e com IPSec configurado. Para a análise de tráfego será utilizado o software Wireshark (item 3.1). A figura 37 representa a topologia física do ambiente.

Na VM MAQ-1 foi ativado o recurso IIS com o serviço FTP configurado, a VM MAQ-2 será utilizada como *client*. O protocolo FTP será utilizado para que seja gerado tráfego entre as VMs, para posteriormente ser analisado.



Figura 37 - Topologia Física

3.3.2.1 – Análise Protocolo IPv4

Após geração de tráfego IPv4 sem o IPSec configurado e captura dos pacotes entre as VMs, podemos analisar o software Wireshark e verificar que os pacotes foram trafegados sem segurança. Aplicamos um filtro de pesquisa no Wireshark para visualizarmos apenas o protocolo FTP. Na figura 38, nos pacotes número 21 e 23 podemos visualizar o usuário e senha FTP em texto plano.

Verificamos que o protocolo IPv4 sem segurança é altamente vulnerável ao ataque de um *sniffer* de rede, onde toda a informação trafega de forma clara.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.001616000	10.1.1.1	10.1.1.2	FTP	81	Response: 220 Microsoft FTP Service
9	0.002257000	10.1.1.2	10.1.1.1	FTP	70	Request: USER anonymous
10	0.002358000	10.1.1.1	10.1.1.2	FTP	92	Response: 331 Password required for anonymous.
11	0.002710000	10.1.1.2	10.1.1.1	FTP	66	Request: PASS User@
12	0.002781000	10.1.1.1	10.1.1.2	FTP	79	Response: 530 User cannot log in.
20	6.079660000	10.1.1.1	10.1.1.2	FTP	81	Response: 220 Microsoft FTP Service
21	6.080119000	10.1.1.2	10.1.1.1	FTP	65	Request: USER maql
22	6.080200000	10.1.1.1	10.1.1.2	FTP	87	Response: 331 Password required for maql.
23	6.080441000	10.1.1.2	10.1.1.1	FTP	65	Request: PASS maql
24	6.081543000	10.1.1.1	10.1.1.2	FTP	75	Response: 230 User logged in.
25	6.081901000	10.1.1.2	10.1.1.1	FTP	61	Request: CWD /
26	6.082399000	10.1.1.1	10.1.1.2	FTP	83	Response: 250 CWD command successful.
27	6.083684000	10.1.1.2	10.1.1.1	FTP	62	Request: TYPE A
28	6.083771000	10.1.1.1	10.1.1.2	FTP	74	Response: 200 Type set to A.
29	6.084176000	10.1.1.2	10.1.1.1	FTP	60	Request: PASV
30	6.084365000	10.1.1.1	10.1.1.2	FTP	100	Response: 227 Entering Passive Mode (10,1,1,192,86).
34	6.085218000	10.1.1.2	10.1.1.1	FTP	60	Request: LIST
35	6.085453000	10.1.1.1	10.1.1.2	FTP	108	Response: 125 Data connection already open; Transfer starting.
38	6.085753000	10.1.1.1	10.1.1.2	FTP	78	Response: 226 Transfer complete.
46	10.264506000	10.1.1.1	10.1.1.2	FTP	81	Response: 220 Microsoft FTP Service

Figura 38 - Protocolo IPv4 sem IPSec

3.3.2.2 – Análise Protocolo IPv4 com IPSec

Após a configuração entre as VMs do protocolo IPv4 com IPSec (item 3.3.1), podemos analisar o tráfego IPv4 seguro. Primeiramente o IPSec faz a troca de chaves e estabelece a SA (item 2.6.3), conforme a figura 39.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000209000	10.1.1.2	10.1.1.1	ISAKMP	270	Identity Protection (Main Mode)
4	0.018734000	10.1.1.1	10.1.1.2	ISAKMP	250	Identity Protection (Main Mode)
5	0.038945000	10.1.1.2	10.1.1.1	ISAKMP	302	Identity Protection (Main Mode)
6	0.052588000	10.1.1.1	10.1.1.2	ISAKMP	302	Identity Protection (Main Mode)
7	0.056679000	10.1.1.2	10.1.1.1	ISAKMP	110	Identity Protection (Main Mode)
8	0.057808000	10.1.1.1	10.1.1.2	ISAKMP	110	Identity Protection (Main Mode)
9	0.060113000	10.1.1.2	10.1.1.1	ISAKMP	214	Quick Mode
10	0.061048000	10.1.1.1	10.1.1.2	ISAKMP	214	Quick Mode
11	0.071519000	10.1.1.2	10.1.1.1	ISAKMP	102	Quick Mode
12	0.090925000	10.1.1.1	10.1.1.2	ISAKMP	118	Quick Mode

Figura 39 - Protocolo ISAKMP IPv4

Após o estabelecimento do canal seguro, todo pacote trocado é autenticado e encriptado. A figura 40 mostra o tráfego IPv4 criptografado através do cabeçalho ESP.

No.	Time	Source	Destination	Protocol	Length	Info
13	0.091578000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
14	0.091783000	10.1.1.1	10.1.1.2	ESP	102	ESP (SPI=0xb064eefc)
15	0.092150000	10.1.1.2	10.1.1.1	ESP	86	ESP (SPI=0xd90f4118)
16	0.134775000	10.1.1.1	10.1.1.2	ESP	118	ESP (SPI=0xb064eefc)
17	0.135777000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
18	0.136189000	10.1.1.1	10.1.1.2	ESP	126	ESP (SPI=0xb064eefc)
19	0.137050000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
20	0.137518000	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0xb064eefc)
21	0.138558000	10.1.1.2	10.1.1.1	ESP	86	ESP (SPI=0xd90f4118)
22	0.138770000	10.1.1.1	10.1.1.2	ESP	86	ESP (SPI=0xb064eefc)
23	0.139016000	10.1.1.1	10.1.1.2	ESP	86	ESP (SPI=0xb064eefc)
24	0.139774000	10.1.1.2	10.1.1.1	ESP	86	ESP (SPI=0xd90f4118)
26	4.984280000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
27	4.984435000	10.1.1.1	10.1.1.2	ESP	102	ESP (SPI=0xb064eefc)
28	4.984711000	10.1.1.2	10.1.1.1	ESP	86	ESP (SPI=0xd90f4118)
29	4.985021000	10.1.1.1	10.1.1.2	ESP	118	ESP (SPI=0xb064eefc)
30	4.985460000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
31	4.985628000	10.1.1.1	10.1.1.2	ESP	118	ESP (SPI=0xb064eefc)
32	4.986174000	10.1.1.2	10.1.1.1	ESP	102	ESP (SPI=0xd90f4118)
33	5.007625000	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0xb064eefc)
34	5.007999000	10.1.1.2	10.1.1.1	ESP	94	ESP (SPI=0xd90f4118)
35	5.008192000	10.1.1.1	10.1.1.2	ESP	118	ESP (SPI=0xb064eefc)
36	5.008575000	10.1.1.2	10.1.1.1	ESP	94	ESP (SPI=0xd90f4118)
37	5.008700000	10.1.1.1	10.1.1.2	ESP	110	ESP (SPI=0xb064eefc)

Figura 40 - Protocolo IPv4 com IPSec

3.3.2.3 – Análise Protocolo IPv6

Na análise do protocolo IPv6 sem IPsec, aplicamos o mesmo método de captura de pacotes utilizado no IPv4. Podemos constatar que os dados trafegados entre as VMs também estão em texto plano. Nos pacotes número 19 e 21 (figura 41) podemos verificar o usuário e senha FTP.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.001673000	2001:db8::	2001:db8::	FTP	101	Response: 220 Microsoft FTP Service
7	0.003688000	2001:db8::	2001:db8::	FTP	90	Request: USER anonymous
8	0.003836000	2001:db8::	2001:db8::	FTP	112	Response: 331 Password required for anonymous.
9	0.007758000	2001:db8::	2001:db8::	FTP	86	Request: PASS User@
10	0.007950000	2001:db8::	2001:db8::	FTP	99	Response: 530 User cannot log in.
18	5.650299000	2001:db8::	2001:db8::	FTP	101	Response: 220 Microsoft FTP Service
19	5.650540000	2001:db8::	2001:db8::	FTP	85	Request: USER maql
20	5.650613000	2001:db8::	2001:db8::	FTP	107	Response: 331 Password required for maql.
21	5.650845000	2001:db8::	2001:db8::	FTP	85	Request: PASS maql
22	5.651178000	2001:db8::	2001:db8::	FTP	95	Response: 230 User logged in.
23	5.651463000	2001:db8::	2001:db8::	FTP	81	Request: CWD /
24	5.651669000	2001:db8::	2001:db8::	FTP	103	Response: 250 CWD command successful.
25	5.651973000	2001:db8::	2001:db8::	FTP	82	Request: TYPE A
26	5.652042000	2001:db8::	2001:db8::	FTP	94	Response: 200 Type set to A.
27	5.652435000	2001:db8::	2001:db8::	FTP	80	Request: EPSV
28	5.652622000	2001:db8::	2001:db8::	FTP	122	Response: 229 Entering Extended Passive Mode (49242)
32	5.653573000	2001:db8::	2001:db8::	FTP	80	Request: LIST
33	5.677486000	2001:db8::	2001:db8::	FTP	128	Response: 125 Data connection already open; Transfer starting.
36	5.678005000	2001:db8::	2001:db8::	FTP	98	Response: 226 Transfer complete.
44	8.537397000	2001:db8::	2001:db8::	FTP	101	Response: 220 Microsoft FTP Service

Figura 41 - Protocolo IPv6 sem IPsec

3.3.2.4 – Análise Protocolo IPv6 com IPsec

O estabelecimento do canal seguro através do protocolo ISAKMP no IPv6 (figura 42), ocorreu da mesma forma que no IPv4. Observamos ainda que o número dos pacotes correspondem aos mesmos do IPv4.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000380000	2001:db8::	2001:db8::	ISAKMP	250	Identity Protection (Main Mode)
4	0.001011000	2001:db8::	2001:db8::	ISAKMP	230	Identity Protection (Main Mode)
5	0.011940000	2001:db8::	2001:db8::	ISAKMP	274	Identity Protection (Main Mode)
6	0.025546000	2001:db8::	2001:db8::	ISAKMP	274	Identity Protection (Main Mode)
7	0.029348000	2001:db8::	2001:db8::	ISAKMP	146	Identity Protection (Main Mode)
8	0.029512000	2001:db8::	2001:db8::	ISAKMP	146	Identity Protection (Main Mode)
9	0.036853000	2001:db8::	2001:db8::	ISAKMP	258	Quick Mode
10	0.038123000	2001:db8::	2001:db8::	ISAKMP	258	Quick Mode
11	0.040242000	2001:db8::	2001:db8::	ISAKMP	122	Quick Mode
12	0.040816000	2001:db8::	2001:db8::	ISAKMP	138	Quick Mode

Figura 42 - Protocolo ISAKMP IPv6

Após o estabelecimento do canal seguro, todo pacote trocado é autenticado e criptografado (figura 43) da mesma forma que verificamos no protocolo IPv4.

No.	Time	Source	Destination	Protocol	Length	Info
13	0.041675000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
14	0.041869000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0x6fa9069e)
15	0.042213000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0xe5438bcb)
16	0.042642000	2001:db8::	2001:db8::	ESP	138	ESP (SPI=0x6fa9069e)
17	0.043006000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
18	0.043191000	2001:db8::	2001:db8::	ESP	146	ESP (SPI=0x6fa9069e)
19	0.043527000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
20	0.043660000	2001:db8::	2001:db8::	ESP	130	ESP (SPI=0x6fa9069e)
21	0.043950000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0xe5438bcb)
22	0.044031000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0x6fa9069e)
23	0.044123000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0x6fa9069e)
24	0.045469000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0xe5438bcb)
25	4.511630000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
26	4.511833000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0x6fa9069e)
27	4.512100000	2001:db8::	2001:db8::	ESP	106	ESP (SPI=0xe5438bcb)
28	4.512355000	2001:db8::	2001:db8::	ESP	138	ESP (SPI=0x6fa9069e)
29	4.512678000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
30	4.512830000	2001:db8::	2001:db8::	ESP	138	ESP (SPI=0x6fa9069e)
31	4.513135000	2001:db8::	2001:db8::	ESP	122	ESP (SPI=0xe5438bcb)
32	4.513573000	2001:db8::	2001:db8::	ESP	130	ESP (SPI=0x6fa9069e)
33	4.513916000	2001:db8::	2001:db8::	ESP	114	ESP (SPI=0xe5438bcb)
34	4.514111000	2001:db8::	2001:db8::	ESP	138	ESP (SPI=0x6fa9069e)
35	4.515200000	2001:db8::	2001:db8::	ESP	114	ESP (SPI=0xe5438bcb)
36	4.515343000	2001:db8::	2001:db8::	ESP	130	ESP (SPI=0x6fa9069e)

Figura 43 - Protocolo IPv6 com IPSec

Após os testes constatamos que a configuração do IPSec foi realizada apenas uma única vez nas VMs para ambos os protocolos IPv4 e IPv6. Na captura dos pacotes visualizamos que os mesmos pacotes trafegados em IPv4 correspondem aos mesmos trafegados em IPv6. Não foi constatado nenhuma diferença nos dados criptografados.

4 – Conclusão

O novo protocolo de Internet o IPv6 oferece novas funcionalidades que não existiam no IPv4, com essas novas funcionalidades o IPv6 está preparado para fornecer suporte a novas tecnologias. O espaço para endereçamento no IPv6 é gigantesco, essa é uma característica marcante no novo protocolo.

A segurança é altamente abordada pelos autores no IPv6, é dito que a segurança é nativa no novo protocolo, onde o IPsec faz parte da pilha de protocolos TCP/IPv6. Essa afirmação transmite a ideia que o IPv6 é mais seguro que o IPv4 e que os problemas com segurança serão todos resolvidos num passe de mágica. Com o IPsec sendo nativo no IPv6, significa que os equipamentos com suporte ao IPv6 também suportam o protocolo IPsec, porém o IPsec não é ativado automaticamente no IPv6 a configuração continua sendo manual como ocorre atualmente no IPv4 e que verificamos no estudo de caso.

Brito (2013) disse que: Muitas pessoas entendem que o IPv6 por si só criptografa os dados automaticamente durante sua transmissão, porém isso não é verdade. Através dos cabeçalhos de extensão AH e ESP o IPsec passa a ser embutido em equipamentos que suportam a pilha TCP/IPv6, isso é um grande potencial para que o IPv6 seja mais seguro, desde que o IPsec seja devidamente configurado no ambiente.

No estudo de caso podemos concluir que da mesma forma que no IPv4, no IPv6 o IPsec deve ser devidamente configurado, o IPv6 por si só não oferece mecanismo de segurança, porém com a eliminação do NAT, novas funcionalidades e endereços IPv6 globalmente roteáveis na Internet oferecidos em abundância aos usuários, será possível a utilização do IPsec para comunicação segura entre os *hosts* na Internet. Ainda Brito (2013): “[...] com IPv6 existe a possibilidade de proteger nativamente as comunicações fim-a-fim diretamente nos hosts das pontas, outra grande vantagem da eliminação do NAT”.

Os usuário preocupados com a segurança poderão trocar informações de modo seguro (criptografado) na Internet sem complicação, o que não ocorre com o IPv4. Ainda com a eliminação do NAT o modelo fim-a-fim, que foi proposto no projeto inicial do IPv4, volta a funcionar, também a rastreabilidade dos hosts torna-se possível.

O IPv6 é um protocolo com potencial enorme para que a segurança seja aplicada e melhorada continuamente na camada de rede, porém devido ainda ser pouco utilizado novas vulnerabilidades surgiram, o que é normal para todas as novas tecnologias.

Como proposta para estudos futuros, avaliar o desempenho do protocolo IPSec em redes IPv4 e IPv6 em ambiente com máquinas reais. Realizar um estudo da implementação do IPSec em modo túnel em redes IPv4 e IPv6. Implementar o IPSec em ambiente com a utilização do NAT, demonstrando as restrições existentes. Pesquisar como está a adoção do IPSec/IPv6 nas empresas.

BIBLIOGRAFIA

Assim se Faz. **Como fazer fundamentação teórica.** Disponível em <<http://www.assimsefaz.com.br/sabercomo/como-fazer-fundamentacao-teorica>>. Acesso em 23/10/2014.

Bucke Brito, Samuel Henrique. **IPv6: o novo protocolo da internet.** 1. ed. São Paulo: Novatec, 2013.

Equipe IPv6.br. **Apostila IPv6 Básico.** Disponível em: <<http://ipv6.br/download>>. Acesso em 04/09/2014.

Equipe IPv6.br. **O IPv6: cabeçalho.** Disponível em: <<http://ipv6.br/entenda/cabecalho>>. Acesso em: 17/04/2014.

Equipe IPv6.br. **O IPv6: funcionalidades básicas.** Disponível em: <<http://ipv6.br/entenda/funcionalidades>>. Acesso em: 28/05/2014.

Florentino, Adilson Aparecido. **IPv6 na prática.** 1. ed. São Paulo: Linux New Media do Brasil Editora Ltda, 2012.

Kurose, James F. **Redes de computadores e a Internet: uma abordagem top-down.** 3. ed. São Paulo: Pearson Addison Wesley, 2006.

Mendes, Roberto. **Redes MPLS: vpn em camada 3.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialmplscam/pagina_2.asp>. Acesso em: 28/08/14.

Miranda, Ivana. **VPN – Virtual Private Network**: rede privada virtual. Disponível em: <http://gta.ufrj.br/seminarios/semin2002_1/Ivana>. Acesso em: 28/08/2014.

Silva, Adailton; Teixeira Renata. **Arquitetura IP Security – Parte 1**. Disponível em: <<http://www.rnp.br/newsgen/9907/ipsec3.html>>. Acesso em: 23/06/2014.

Tanenbaum, Andrew S. **Sistemas Operacionais Modernos**. Tradução. 3. ed. São Paulo: Pearson Prentice Hall, 2009.

Tanenbaum, Andrew S.; Wetherall, David. **Redes de Computadores**. Tradução. 5. ed. São Paulo: Pearson, 2011.