CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de tecnologia em Segurança da Informação

Bruno Bertole Fragoso Nunes

Segurança da rede internet com a implantação do protocolo IPSEC

Americana, SP
2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de tecnologia em Segurança da Informação

Bruno Bertole Fragoso Nunes

Segurança da rede internet com a implantação do protocolo IPSEC

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof.(a) Esp. Rogério Nunes de Freitas

Área de concentração: Segurança de redes

Americana, SP.
2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Nunes, Bruno Bertole Fragoso
N923s Segurança da rede Internet com a implantação do protocolo IPSEC. / Bruno Bertole Fragoso Nunes. – Americana: 2014.
53f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Rogério Nunes de Freitas

1.Segurança em Sistemas de informação 2. Comunicação de dados I. Freitas, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Bruno Bertole Fragoso Nunes

Segurança da rede internet com a implantação do protocolo IPSEC

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança de redes

Americana, 26 de junho de 2014.

Banca Examinadora:

_____
Rogério Nunes de Freitas (Presidente)
Especialista
FATEC Americana

_____
Renato Kraide Soffner (Membro)
Doutor
FATEC AMERICANA

_____
Sisino Motta Neto (Membro)
Especialista
FATEC AMERICANA

AGRADECIMENTOS

Primeiramente eu agradeço aos professores que ao longo da jornada acadêmica, compartilharam os seus conhecimentos obtidos em suas vidas. Agradeço também especialmente o professor Rogério Nunes de Freitas, que me orientou nesse trabalho e não mediu esforços para me ajudar nas dificuldades encontradas. Aos amigos de classe que passaram três anos de suas vidas, compartilhando alegrias, conhecimentos e experiências vividas. E por fim, agradeço a minha família que esteve ao meu lado me ajudando nas dificuldades.

RESUMO

Desde a criação da Internet até os dias atuais, muitas pessoas tiveram e têm acesso para lazer ou trabalho. Muitos dos equipamentos conectados que vão desde computadores, celulares e tabletes até televisões, e geladeiras que auxiliam no uso doméstico. Essa facilidade e agilidade no cotidiano escondem alguns perigos que podem ocasionar prejuízos e até a falência de uma empresa caso algum arquivo sigiloso seja visualizado ou alterado. A área de segurança da informação foca a solução e prevenção desses perigos. Existem várias ferramentas e boas maneiras para reduzir bastante os riscos. Esse trabalho de conclusão de curso apresentará um protocolo voltado a segurança no tráfego de informações, esse protocolo utiliza vários métodos de segurança nas transferências, a fim de que pessoas desconhecidas ou mal intencionadas não tenham acesso a informação.

Palavras-chave: IPSEC, Internet, IPV6

ABSTRACT

Since the creation of the Internet to this day, many people had and have access to leisure or work. Many of connected devices ranging from computers, mobile phones, tablets until televisions, refrigerators that help household. This ease and agility in everyday life, hides some dangers that can cause damage and even business failure if some confidential file to be viewed or changed. The area of information security focuses on the prevention and solution of these dangers, there are several tools and good ways to greatly reduce the risks. This work of course completion will present a protocol oriented safety information traffic, this protocol uses various security methods in transfers, so that unknown or ill-intentioned people do not have access to information.

Keywords: IPSEC, Internet, IPV6

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

3DES – *Triple Data Encryption Standard*

ACL – *Access Control List*

AH – *Authentication Header*

ARPANET – *Advanced Research Projects Agency Network*

DES – *Data Encryption Standard*

DOD – *Department of Defense*

DOS – *Denial of Service*

ESP – *Encapsulating Security* Payload

HMAC – *Hash-based Message Authentication Code*

IANA – *Internet Assigned Numbers Authority*

IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos

IKE – *Internet Key Exchange*

IP – *Internet Protocol*

IPSEC – *Internet Protocol Security*

IPV4 – *Internet Protocol Version 4*

IPV6 – *Internet Protocol Version 6*

ISAKMP – *Internet Security Association and Key Management Protocol*

ISO – *International Organization for Standardization*

LAN – *Local Area Network*

LLC – *Logical Link Control*

MAC – *Media Access Control*

NAT – *Network Address Translation*

OSI – *Open Systems Interconnection*

RFC – *Request for Comments*

SA – *Security Association*

SPI – *Serial Peripheral Interface*

SSL – *Secure Sockets Layer*

TCP – *Transmission Control Protocol*

TI – Tecnologia da Informação

VPN – *Virtual Private Network*

WAN – *Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

A internet facilitou muitas tarefas que antes exigia tempo, esforço entre outras coisas. Atualmente, a internet proporciona várias ferramentas para ajudar no cotidiano das pessoas, nem se pensava que seria possível fazer compras pela internet e até assistir um filme pela televisão utilizado a internet.

Ao longo do tempo, foram criadas arquiteturas que suportam vários aparelhos conectados a essa rede mundial. Desde quando houve o surgimento da internet, foram aparecendo vários problemas, como a arquitetura da internet, ferramentas que utilizam a internet, assim obrigaram a ser feita analises para obter melhorias nos equipamentos que beneficiassem o usuário.

Com tanta diversidade de ferramentas e informações que a internet oferece, também existem riscos que podem prejudicar uma empresa ou pessoas. Vários pacotes trafegam diariamente pela rede, alguns pacotes com informações que não possuem grande valor, já outros com informações que em poder de pessoas mal intencionadas podem acarretar grandes prejuízos.

Existem soluções para vários tipos de ameaças existentes, cada uma com pontos fortes e fracos, mas com o objetivo de proporcionar uma maior segurança para a rede. Nesse trabalho de conclusão de curso, foi escolhido como ferramenta de segurança o protocolo IPSec. Esse protocolo oferece uma arquitetura que une a autenticação, a criptografia e até um modo para que as mensagens sejam transferidas de maneira segura, evitando assim a visualização ou alteração de um pacote. Esse protocolo surgiu especificamente para as redes IPv6, mas depois foi feita uma adaptação para redes IPv4. No estudo de caso será abordado o funcionamento com as duas redes e cada capítulo mostrará a importância desse protocolo.

O objetivo geral desse trabalho foi fazer um levantamento sobre o protocolo IPSec, a fim de avaliar as vantagens de usá-lo como uma ferramenta de segurança para pequenas e grandes empresas. Como objetivo específico é proposto um teste para implantar o protocolo IPSec em duas filiais, e configurar da melhor maneira para se obter uma grande segurança nas transferências de arquivos

A metodologia utilizada foi a pesquisa bibliográfica, utilizando livros de autores especializados na área, ferramentas específicas de grandes empresas para redes de

computadores, e consulta em documentos de órgãos importantes da arquitetura da rede.

No segundo capítulo desse trabalho, é descrito o surgimento da internet e sua evolução. Em sequência é abordado o papel da segurança da informação na área de TI, bem como as características, requisitos e os perigos existentes que estão na internet.

O terceiro capítulo aborda o modelo OSI e as suas camadas, apresentando a importância de cada uma para a rede. É também abordado o modelo TCP/IP que foi um modelo base para o modelo OSI, e no fim desse capítulo é feito uma avaliação entre o protocolo IPv4 e IPv6.

O quarto capítulo expõe o tema principal, o IPSec, explicando o significado desse protocolo, suas características, o funcionamento e as ferramentas que o auxiliam para que a transferência seja segura.

No último capítulo o estudo de caso é feito com uma simulação em duas redes, um rede IPv4 e outra IPv6. Mostrando como o IPSec funciona e a vantagem de utilizar esse protocolo.

E por fim, as conclusões sobre a pesquisa do protocolo IPSec e o estudo de caso.

2 SEGURANÇA NA INTERNET

Atualmente, as empresas e usuários comuns usam os computadores, e outros aparelhos para armazenar diversas informações importantes, variando de dados financeiros de uma empresa até números de cartões de crédito de um usuário que utiliza a internet para fazer compras *online*. Isso acabou gerando uma grande necessidade de ter proteção, assim evitando possíveis vazamentos de informações, ou problemas que possam levar a enormes prejuízos e frustrações (STALLINGS, 2005).

Conforme Kurose (2010), uma parte da segurança da informação foca em como pessoas mal intencionadas podem danificar uma rede de computadores, e o que especialistas podem fazer para defender a rede, e como criar novas arquiteturas imunes contra possíveis ataques. O surgimento de novas ameaças todos os dias e a frequência que ocorrem, alavancou ainda mais a segurança de rede, se tornando uma aliada em uma rede de computadores.

2.1 Evolução

Conforme Stallings (2005), antigamente a segurança das informações valiosas era feita através de meios físicos e administrativos, como o uso de armários com trancas de segredo, até pesquisas nos dados pessoais das contratações de funcionários para a empresa.

Com o passar dos anos e o avanço da tecnologia, a necessidade de proteger os dados aumentou, assim ocasionando duas mudanças no setor de tecnologia da informação. A primeira mudança contribuiu para o surgimento de ferramentas automatizadas que protegessem a informação de maneira constante, e também o uso de sistemas compartilhados que possibilitassem o acesso a máquina de outros lugares. A segunda mudança focava a segurança no canal em que ocorria o tráfego de pacotes, analisando e validando o envio de um terminal de usuário para um servidor. Para os sistemas automatizados, o dois métodos mais utilizados para a segurança é a criptografia assimétrica e simétrica.

"A tecnologia básica em que se fundamentam praticamente todas as aplicações automatizadas de segurança de rede e de computador é a criptografia" (STALLINGS, 2005, p.380)

2.2 Requisitos básicos de segurança

Conforme Kurose (2010), existem quatro requisitos para se obter uma maior segurança no ambiente computacional. Sendo eles a confidencialidade, a autenticação, a integridade e a segurança computacional.

A confidencialidade determina que o remetente e o destinatário serão os únicos a entender a mensagem enviada ou recebida. Existem pessoas mal intencionadas que buscam interceptar as mensagens para visualizar o conteúdo, e para evitar que essas pessoas consigam capturar a mensagem e entende-la, é preciso usar a criptografia que possibilite somente que o remente e destinatário consigam entender.

A autenticação do ponto final determina que o remetente e destinatário confirme a identidade na comunicação entre eles, comprovando realmente que são os mesmos nessa comunicação.

Integridade de mensagem, o remetente e o destinatário enviam e recebem uma mensagem, e essa mensagem não deve estar alterada por alguma falha. Deve ser assegurado que a mensagem não sofra nenhuma alteração, exclusão ou adição. Os protocolos de transporte e enlace podem ajudar nesse processo para que a mensagem recebida esteja da mesma forma que foi enviada.

E por último a segurança operacional, as empresas, universidades e usuários usam uma rede conectada à internet. Essa rede pode ser atacada e danificada por pessoas mal intencionadas, elas geralmente obtêm acesso por via da internet pública. Entre esses ataques, podem ser adicionados *worms* para obtenção de arquivos confidenciais, entre outros. Existem alguns mecanismos para evitar esse tipo de invasão, o uso de *firewalls* e sistemas que detectam invasores auxiliando a deter esses ataques contra a rede.

2.3 Ataques

> Um modo útil de classificar os ataques de segurança (RFC2828) é em termos de ataques passivos e ataques ativos. Um ataque passivo tenta aprender ou utilizar informações do sistema sem afetar os recursos do mesmo. Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação. (STALLINGS, 2005, p.380)

2.3.1 Ataques passivos

Os ataques passivos geralmente envolvem o monitoramento e a espionagem das transmissões de informações, podendo resultar no vazamento do conteúdo da mensagem e a análise de tráfego.

Como o próprio nome já diz, o vazamento do conteúdo das mensagens, tem como objetivo capturar mensagens de *e-mail*, conversas telefônicas ou arquivos transferidos que possam conter alguma informação de valor, é importante dificultar o vazamento dessas informações. Outro tipo de ataque passivo é a análise de tráfego, isso ocorre com o objetivo de identificar os *hosts* que estão se comunicando, o tamanho da mensagem e a frequência que são enviadas.

Geralmente é difícil identificar os ataques passivos, porque eles não visam a alteração dos dados, e sim a visualização do conteúdo da mensagem capturada. Quando ocorre a visualização por um terceiro, tanto a parte que enviou a mensagem, e a parte que recebeu, não percebe que a mensagem foi visualizada. Uma possível prevenção para esse problema é o uso de criptografia, isso acaba dificultando o acesso a essas informações (STALLINGS, 2005).

2.3.2 Ataques ativos

"Os ataques ativos envolvem alguma modificação de dados ou a criação de um fluxo falso e podem ser subdivididos em quatro categorias: de falsidade, de repetição, de modificação de mensagens e de negação de serviço." (STALLINGS, 2005, p.381)

O ataque de falsidade é identificado quando um indivíduo finge ser uma outra pessoa para conseguir privilégios no alvo escolhido, geralmente esse ataque acontece com o uso de captura das sequências de autenticação. Um ataque de repetição é caracterizado pela captura de dados e a retransmissão que gera algum dano. O ataque de modificação de mensagens é simplesmente a alteração da mensagem para produzir algum dano, e por último o ataque de negação de serviço, geralmente é escolhido um alvo para causar algum distúrbio no serviços e no servidor, podendo até causar o impedimento do gerenciamento dos recursos, comprometendo o desempenho.

Os ataques ativos são difíceis de prevenir, para evitar isso, seria necessário, a proteção de todas as linhas de comunicação e equipamentos, mas o objetivo é detectar esses ataques e recuperar os dados que foram comprometidos (STALLINGS, 2005).

2.4 Riscos

Conforme Kurose (2010), os vilões são os perigos de uma rede, eles ameaçam as redes de computadores, e os especialistas nessa área procuram defender a rede e até criar arquiteturas imunes a novos ataques. Cada vez mais surgem variedades de ameaças e ataques ainda mais destrutivos, assim a área de segurança de rede ficou em evidência na área de redes de computadores.

Os chamados vilões podem fazer diversos estragos na rede, resultando em prejuízos para uma empresa ou pessoa. Serão abordados dois itens comuns que trazem riscos gerados por um indivíduo.

Muitos aparelhos são conectados à internet, tanto para receber e enviar dados como músicas, *e-mail*, vídeos e etc. Nesse processo pode ocorrer de um *malware*

ser recebido, sendo executado e infectando a máquina, isso possibilita a exclusão de arquivos. A instalação de um *spyware* tem como objetivo coletar dados de número de cartão de crédito, senhas e as mais variadas informações para o criador do *spyware*. Mas para ser infectado é necessário de uma interação com o usuário, como um anexo de *e-mail* que contém esse código malicioso, e sendo executado o anexo o processo do *malware* é iniciado.

Outro tipo de ataque que coloca a infraestrutura e os servidores em perigo é o ataque de recusa de serviços (DOS), esse tipo de ataque deixa os serviços indisponíveis. Esse ataque é divido em três categorias, ataque de vulnerabilidade, de inundação na largura de banda e de inundação na conexão.

O ataque de vulnerabilidade é determinado pelo envio de mensagem a uma aplicação para ser executado em um hospedeiro, sendo executado, o serviço escolhido pode parar de funcionar. A inundação na largura de banda é o ato de enviar vários pacotes ao hospedeiro até lotar, assim ocasionando o impedimento para aceitar mais pacotes. E por último a inundação na conexão, a pessoa que está atacando estabelece várias conexões TCP, e isso resulta em um grande atolamento de conexões ao mesmo tempo, e o servidor acaba parando de aceitar conexões.

3 MODELO OSI

Conforme Kurose (2010), o modelo OSI foi criado pela Organização Internacional para Padronização (ISO) no final dos anos 1970, e o principal objetivo era que a redes de computadores fossem organizadas em sete camadas. Esse modelo surgiu quando os protocolos de internet estavam se amadurecendo e alguns até em desenvolvimento, o criador do modelo OSI não estava com o foco na internet quando o criou. Nessa mesma época os cursos universitários e de treinamento atualizaram os cursos para cumprir a exigência da ISO.

O modelo OSI possui sete camadas, sendo elas a camada de apresentação, de sessão, de transporte, de rede, de enlace e a camada física, sendo que a camada de apresentação e sessão, foram incluídas nesse modelo. A Figura 1 mostra o modelo OSI e o TCP/IP, e as camadas que cada um possui.

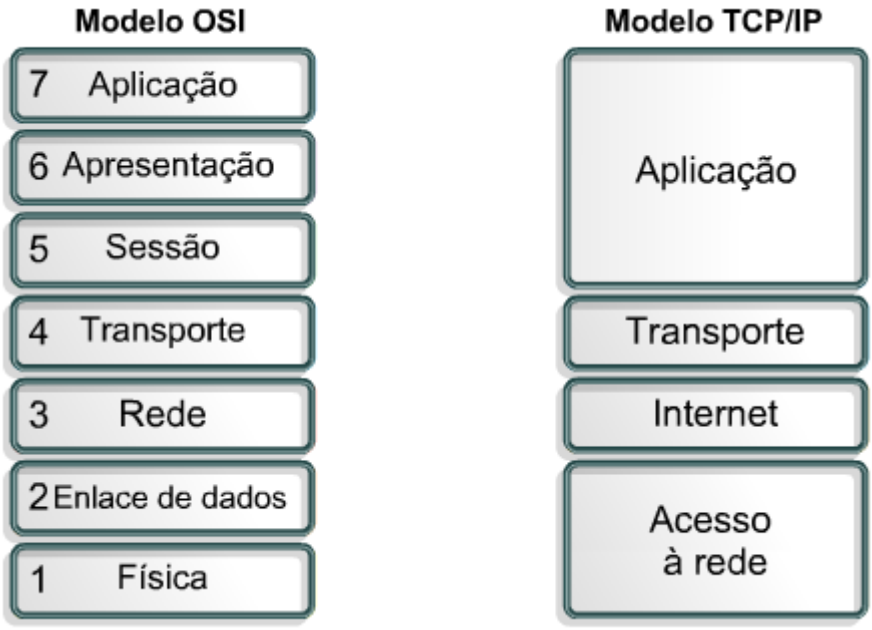

Figura Error! Bookmark not defined. **- Comparação entre o modelo OSI e TCP/IP**
Fonte: Jbgsm. Disponível em: (http://jbgsm.files.wordpress.com/2010/05/377.png). Acesso em 15 de abr. 2014.

A internet propriamente dita utiliza o modelo TCP/IP, e então surge duas dúvidas referente as camadas adicionadas no novo modelo.

> [...] os serviços fornecidos por essas camadas são irrelevantes? E se uma aplicação precisar de um desses serviços? A resposta da Internet para essas perguntas é a mesma — depende do criador da aplicação. Cabe ao criador da aplicação decidir se um serviço é importante, e se o serviço for importante, cabe ao criador da aplicação desenvolver essa função para ela. (KUROSE; ROSS, 2010, p.39-40)

3.1 Camadas do Modelo OSI

Como já explicado, o modelo OSI possui sete camadas que agora serão abordadas para explicar a sua função e importância nesse modelo.

A primeira é a camada de aplicação, ela é a camada que mais interage com o usuário final, essa camada e o usuário interagem com o software de aplicação, por exemplo, um *browser*. Essa camada trata mais de gerenciamento, transferência de arquivos, consulta de banco de dados entre outros, com o foco principal em oferecer serviços para aplicação que o usuário utilizará.

Logo em seguida vem a camada de apresentação, a função dela é converte os dados para ocorrer a troca da camada de aplicação para a camada de sessão, ou vice-versa. Nessa camada ocorre a criptografia e compactação dos arquivos que são enviados, esses arquivos podem ser imagens, vídeos, músicas, documentos entre outros.

A seguir está a camada de sessão, ela é responsável pelo estabelecimento das conexões e o gerenciamento do envio e recebimento das informações, e pelo encerramento da conexão. Essas conexões utilizam protocolos que já estão implementados, além disso, há um gerenciamento de quem está na sessão, isso garante que somente as pessoas autorizadas tenham acesso nessa sessão.

A próxima é a camada de transporte, ela faz o gerenciamento da conexão desde a origem até o destino, assim garantindo que os pacotes sejam entregues para no

destino certo, sem erros e na sequência que foi enviada. Essa camada também faz um controle de fluxo, gerenciando o fluxo de pacotes e garantindo que o remetente não envie mais pacotes de dados do que a capacidade do destinatário em processar.

Na camada de rede, ocorre a gerência do roteamento dos pacotes, assim encaminhando-os para as redes que foram citadas como destinatários. Para acontecer a entrega dos pacotes, são usados protocolos roteáveis, e nessa camada é definido o endereço de rede, que é um endereço lógico. (BARRETT, 2010)

Já a camada de enlace de dados faz o controle de fluxo, do erro e o sincronismo com a camada física, essa camada tem especificações definidas que são características, protocolo e rede.

"A especificação IEEE 802.2 dividiu a camada de enlace de dados em duas subcamadas: a camada controle lógico do enlace (Logical Link Control - LLC) e a camada controle de acesso ao meio (Media Access Control - MAC)." (BARRETT; KING, 2010, p.37)

A subcamada LLC gerencia as comunicações com o dispositivo somente com um enlace, ocorrendo o controle de fluxo e a verificação de algum erro. Já a subcamada MAC faz o gerenciamento de acesso dos protocolos ao meio físico, na prática ela controla o acesso e os controladores das placas de rede.

E por fim a camada física, que é voltada a parte mecânica e elétrica dos equipamentos de rede, fazendo a conversão de bits para dados que serão transmitidos para outra rede (BARRETT, 2010).

3.2 Funcionamento

Conforme Barrett (2010), o modelo OSI tem como objetivo que a troca de dados realizada por dispositivos, seja dividida em camadas, sendo assim, cada camada aplicará as funções especiais nos pacotes de dados. Em cada troca, o fluxo de dados descerá pelas camadas e chegará ao destino, fazendo o caminho pelas camadas, subindo cada camada do destinatário e chegando na camada de aplicação.

> A programação e o hardware que fornecem essas camadas, na realidade, são uma combinação de aplicações, sistema operacional do computador, protocolos de transporte e rede, e o software que permitem que você coloque um sinal em uma das linhas ligadas ao seu computador. (BARRETT; KING, 2010, p.35-36)

Cada camada usa formas de informação de controle para se comunicar com as outras camadas no sistema operacional, as informações contêm solicitações e instruções que são trocadas entre as camadas do modelo OSI. Esses dados são separados e formam um conjunto de pacotes, e nesses pacotes estão o cabeçalho, os dados e o *trailer*.

O cabeçalho armazena as informações do endereço do remetente e do destinatário, *clock* e sinal de alerta, logo em seguida estão os dados que foram enviados e por fim o *trailer*, que verifica se as informações que estão no pacote estão válidas.

Essas verificações analisam se os pacotes estão corrompidos ou danificados no momento da transferência, essa verificação consta em várias camadas do modelo OSI. Existe também o controle de fluxo, ele é responsável sobre as transmissões, para não ocorrer um congestionamento na rede, e caso ocorra serão usados janelas, *buffers* e mensagens de supressão do remetente.

O janelamento tem um esquema sobre o controle do fluxo, sempre que houver transmissão, o remetente receberá uma confirmação do destino depois de uma certa quantidade de pacotes enviados. O *buffer* armazena as informações que estão em excesso, na memória e nos equipamentos de rede. Os equipamentos de recepção utilizam as mensagens de supressão da fonte para evitar que os *buffers* não consigam armazenar os pacotes recebidos.

"As setes camadas do modelo de referência OSI podem ser divididas em duas categorias: camadas superiores e camadas inferiores." (BARRETT; KING, 2010, p.37).

Podemos considerar que as camadas superiores tratam da aplicação, e as inferiores tratam do transporte dos dados. A Figura 2 ilustra como ocorre a transição dos pacotes enviados até chegar ao destinatário.

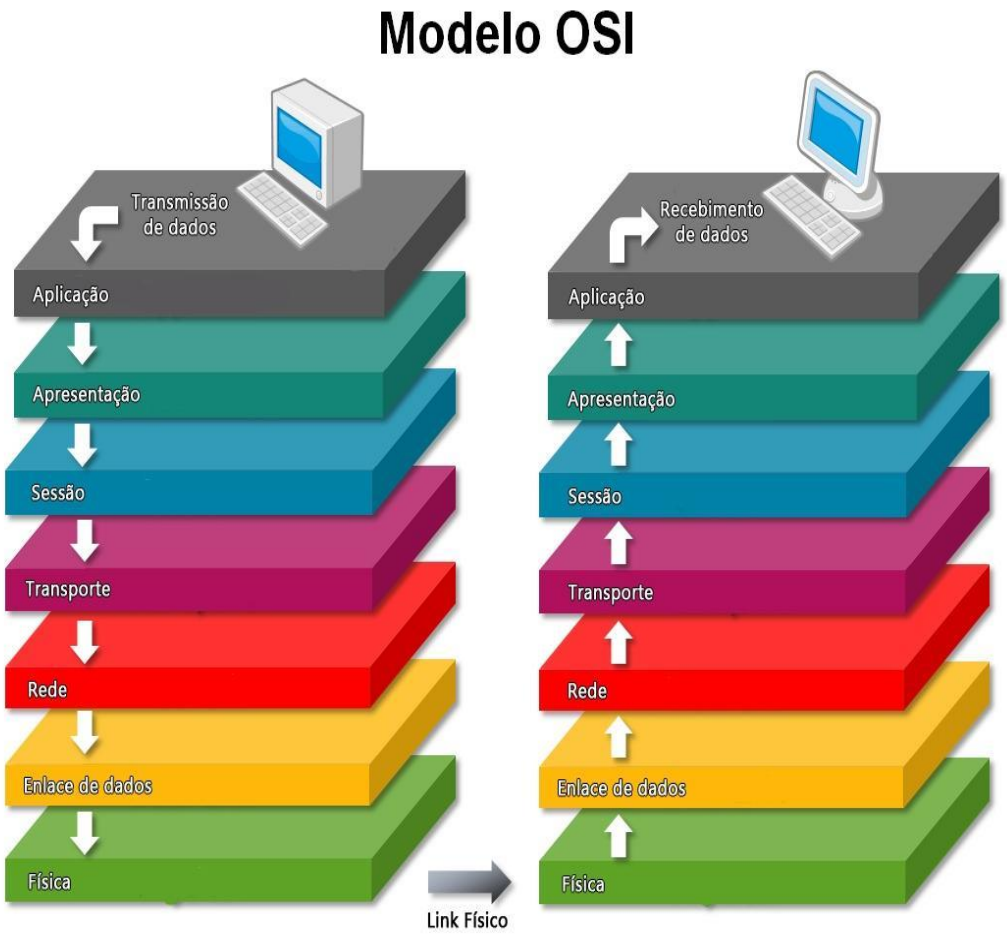

Figura Error! Bookmark not defined. **- Arquitetura do modelo de referência OSI**
Fonte: Mitos da rede. Disponível em: (http://mitodasredes.blogspot.com.br/2013/08/modelo-osi.html). Acesso em 10 de abr. 2014.

3.3 Camada de rede

Mais adiante será abordado o assunto principal, o protocolo IPSec, esse protocolo está localizado na camada de rede que agora será mais detalhada, afim de entender seu objetivo e funcionamento. O objetivo da camada de rede é simplesmente transportar pacotes de um remetente para um destinatário, mas para isso ocorrer, existem duas funções dessa camada, o repasse e roteamento.

O repasse encaminha o pacote que chegou pelo enlace de entrada do roteador até o enlace de saída apropriado. Já o roteamento escolhe a melhor rota ou caminho para que os dados enviados pelo remetente cheguem ao destinatário, essas rotas usam um algoritmo que determina os caminhos, chamados de algoritmos de roteamento.

"Cada roteador tem uma tabela de repasse. Um roteador repassa um pacote examinando o valor de um campo no cabeçalho do pacote que está chegando e então utiliza esse valor para indexar sua tabela de repasse." (KUROSE; ROSS, 2010, p.230)

Com esse resultado, será indicado em quais enlaces dos roteadores serão passados os pacotes enviados, e o cabeçalho que é examinado pode conter o endereço de destino ou a indicação da conexão ao qual o pacote pertence. A figura 3 contém várias redes conectadas, que permitem observar possíveis caminhos que serão traçados pelos pacotes. (KUROSE, 2010)

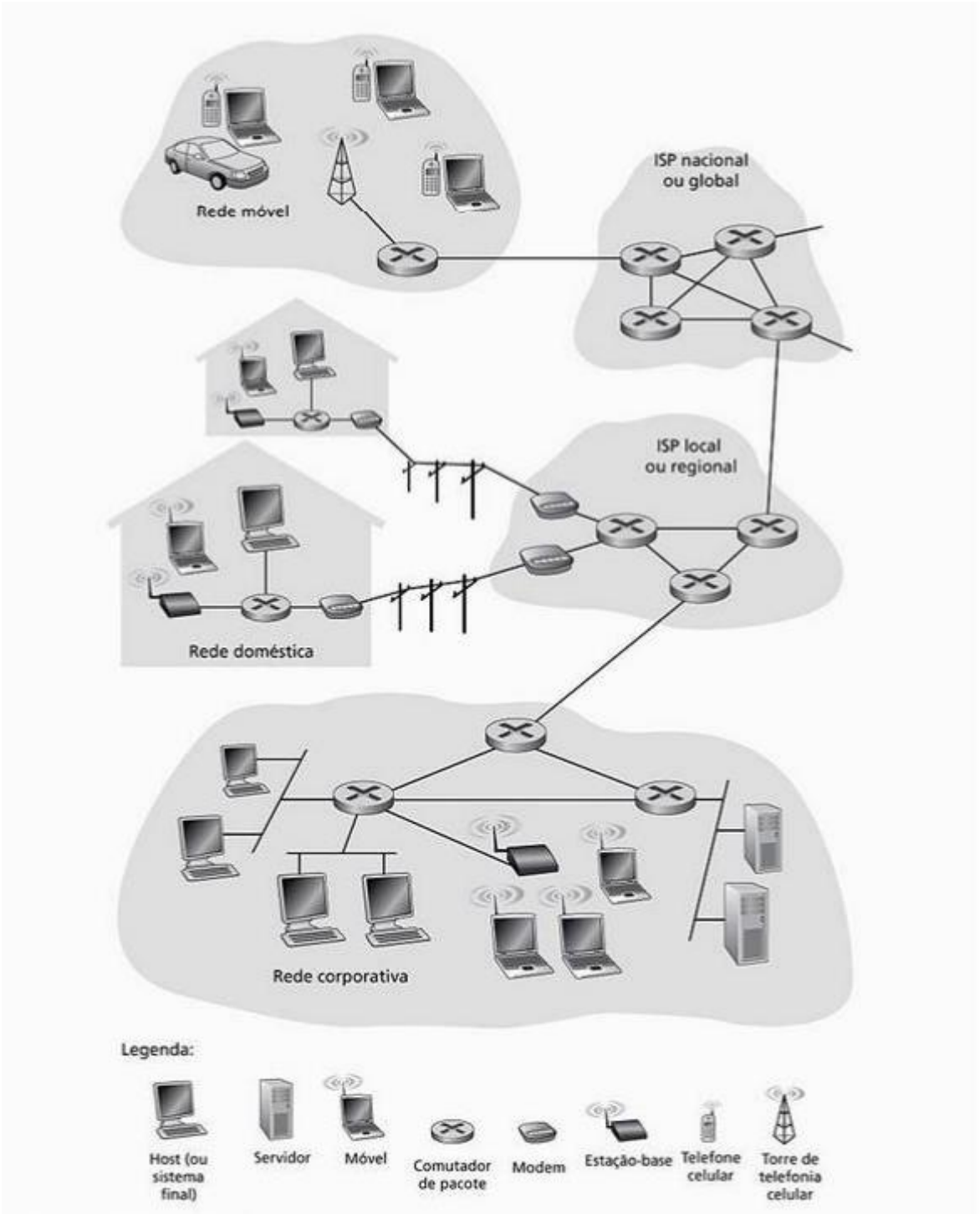

Figura Error! Bookmark not defined. **- Redes de computadores**
Fonte: (KUROSE; ROSS, 2010, p.230).

3.4 Modelo Base: TCP/IP

Conforme o autor Tanenbaum (2003), a ARPANET era uma rede usada para pesquisas e foi patrocinada pelo DOD (Departamento de Defesa dos Estados Unidos), em um ritmo devagar, muitas universidades e órgãos públicos foram conectados na rede usando linha telefônica dedicada. Mais adiante foram criadas redes para rádios e satélites, isso ocasionou problemas nos protocolos que já existiam, e solução para isso foi a criação de uma nova arquitetura.

"Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos de projeto, desde o início." (TANENBAUM, 2003, p.48)

Com isso foi criado o modelo TCP/IP, e foi dado esse nome por causa dos principais protocolos que estão nesse modelo. Uma das preocupações do DOD era se algum equipamento ou linha da sub rede fosse destruído, as transferências deveriam ocorrer normalmente, enquanto a máquina do destino e remetente estivessem funcionando. E outro objetivo era uma arquitetura que se adaptasse a aplicações que exigiam os serviços em tempo real. A figura 4 mostra a arquitetura do modelo TCP/IP.

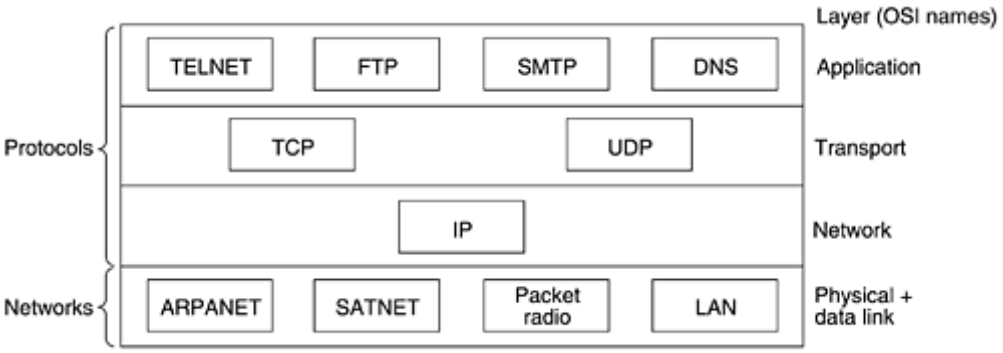

Figura Error! Bookmark not defined. **- Modelo TPC/IP e protocolos**
Fonte: (TANENBAUM, 2003, p.47).

3.5 Protocolo IPv4 x Protocolo IPv6

De acordo com Brito (2013), em 1983 existiam mais de quinhentos computadores conectados na rede, a partir disso, surgiu a internet baseada no protocolo IPv4 na época de 1970-1980, e hoje se tornou alvo de críticas pelo problemas que existem nesse modelo.

> [...] em 1970-80, o objetivo era projetar uma rede distribuída, com o intuito de conectar algumas poucas instituições de pesquisa. Naquela época, não havia requisitos de escalabilidade, segurança e mobilidade. Aliás, era um momento em que ainda existiam dúvidas acerca do interesse de pessoas comuns em computadores pessoais. (BRITO, 2013, p.22)

O endereço IPv4 contém 32 *bits* e são separados em quatro blocos de 8 *bits*, para uma melhor facilidade, ele foi escrito no sistema decimal e separou-se por ponto a cada oitos bits. Na época que o IPv4 foi criado, não se esperava esgotar todos os endereços, porque ele disponibilizava ao total 4.294.967.296 endereços, mas em 2011 a IANA anunciou o esgotamento de endereços IPv4.

Em junho de 2012, o IPv6 se tornou o novo padrão da internet, obrigando a novos dispositivos a terem suporte ao IPv6. O IPv4 não será inutilizado em pouco tempo, as transições de endereços IPv4 para IPv6 irão demorar alguns anos. E além do mais, o IPv6 tem várias vantagens, como a grande gama de endereços, cabeçalho simplificado, processamento simplificado, assim evitando uma sobrecarga nos roteadores resultando em um melhor desempenho, maior segurança com o uso do IPSec, entre outros.

De acordo com o site IPv6.br (2014), em fevereiro de 2014, o sistema de busca google, analisou que 3% das máquinas que acessaram o próprio site estavam usando IPv6, sendo que em setembro do ano anterior existiam somente 2% de acessos com o uso do IPv6. A figura 5 mostra o aumento de acessos ao site google usando o Ipv6.

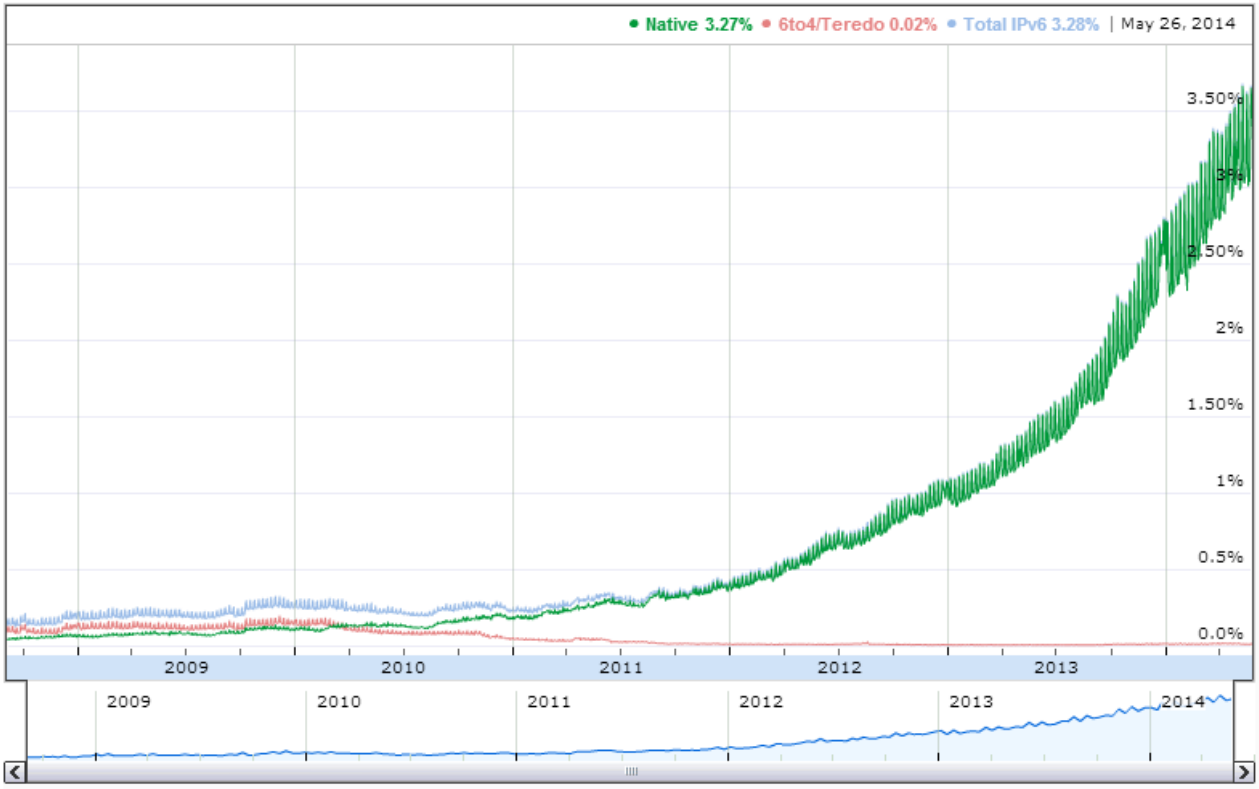

Figura Error! Bookmark not defined. **- Aumento no acesso com o uso do protocolo IPv6**
Fonte: Google. Disponível em: (http://www.google.com/intl/en/ipv6/statistics.html). Acesso em 02 de abr. 2014.

4 PROTOCOLO IPSEC

> O IPSec (RFC 4301) é uma solução de segurança em nível da camada de rede, criada para proteger o tráfego na Internet e bastante disseminada no mercado atualmente. O IPSec pode ser utilizado diretamente nos *hosts* ou mesmo em dispositivos como roteadores e *firewalls*. (BRITO, 2013, p.161)

4.1 Características

Conforme Silva (2010), o protocolo IPSec tem como objetivo principal permitir que envios e recebimentos de dados na camada de rede ocorram com segurança. Na época que foi criado, o intuito era preencher a lacuna que afetava as transferências, como a autenticação, confidencialidade e a integridade dos pacotes.

> O IPSec de acordo com Kent e Atkinson (1998) apud Falconi (2004, p. 36-37) é classificado como um conjunto de protocolos que proveem serviços de autenticidade e confidencialidade para comunicações na Internet. Protege o datagrama IP inteiro no modo fim a fim, sendo que nenhuma máquina intermediária na Internet pode ter acesso ou pode modificar qualquer informação sobre a camada IP.

Conforme Stallings (2005), o IPSec auxilia as redes LAN, WANs públicas e privadas e a internet, e existem várias aplicações e vantagens que são oferecidas por esse protocolo. Uma delas é a proteção em redes WAN ou até mesmo na internet, as empresas geralmente usam *links* dedicados para se comunicarem de maneira mais segura entre as filiais. Com o uso do IPSEC existe a possibilidade de criar uma rede privada utilizando a Internet, isso traz benefícios como a diminuição de custos de redes privadas que usam *links* dedicados, ainda existem outras aplicações como a segurança em acesso remoto, proteção em comunicação, entre

outras. Essas aplicações variadas que o IPSec disponibiliza para a rede, é justo pela capacidade de criptografar e autenticar todo tráfego independente da rede no nível do IP.

Além dessas aplicações, existem várias vantagens de usar esse protocolo pensando em segurança na rede, por exemplo, tornar o fluxo de transferências de pacotes melhor, mais rápido e confiável. Isso se deve pelo motivo do IPSec poder ser implementado em um roteador ou *firewall*, resultando em forte segurança em todo tráfego enviado e recebido, um item positivo é a vantagem de ser transparente, assim não aparecendo para os usuários finais e aplicações.

> O IPSec fornece três recursos principais: uma função apenas de autenticação, chamada *Authentication Header* (AH), Uma função combinada de autenticação/criptografia, chamada *Encapsulating Security Payload* (ESP), e uma função de troca de chave. (STALLINGS, 2005, p.398)

4.2 Funcionamento

Conforme o autor Kurose (2010), uma empresa pode expandir para várias regiões, e alguns serviços podem ficar separados em outros estabelecimentos, isso resulta em a empresa ter uma própria IP para acessar ou enviar dados de maneira totalmente segura e sigilosa.

Pelo alto custo de criar e manter uma rede independente, a solução acaba sendo a criação de VPNs em uma rede de Internet pública. Com uma VPN, o trafego interno é criptografado antes de ir para a internet, garantindo o sigilo dos pacotes enviados. Um exemplo para explicar melhor, é o caso de uma matriz que possui uma filial e funcionários que trabalham em várias regiões em um dia, se um funcionário da matriz envia alguma informação para alguém dentro da matriz, o pacote não precisa ser criptografado, ele fica da forma original sem o uso do IPSec, mas caso o funcionário da filial queira se comunicar com um funcionário de uma filial, o tráfego das informações é criptografado antes de entrar na rede Internet. A seguir, a figura 6 mostra um exemplo de uma rede VPN com o uso do IPSec.

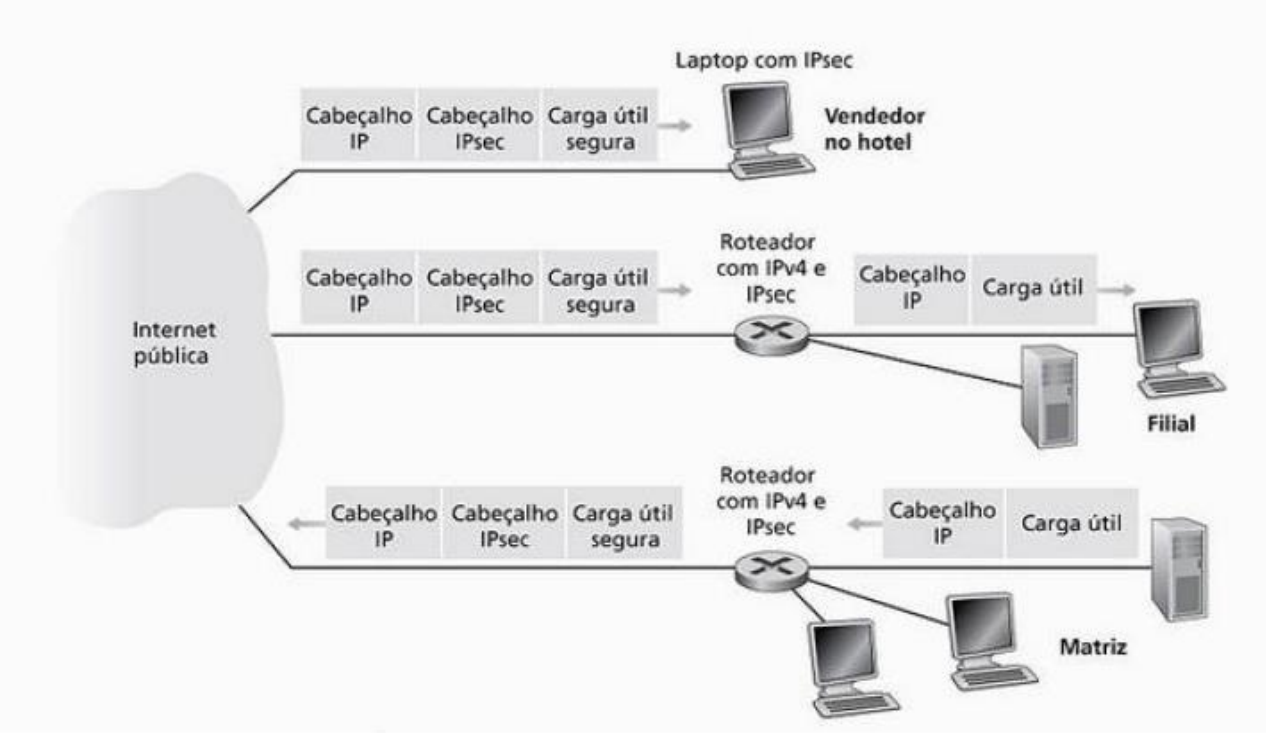

Figura Error! Bookmark not defined. **- Uma VPN utilizando o protocolo IPSec**
Fonte: (KUROSE; ROSS, 2010, p.527).

No exemplo mostrado, quando algum funcionário da matriz quer enviar uma mensagem para o vendedor que está localizado no hotel, o roteador que está na matriz faz a conversão do datagrama original para o datagrama IPSec e o encaminha para a internet, e depois para o vendedor. Dentro do cabeçalho IPSec, contém um datagrama tradicional, resultando na forma de que os roteadores processem o datagrama como fosse tradicional.

"[...] a carga útil do datagrama IPsec inclui um cabeçalho IPsec, que é utilizado para o processamento do IPsec; além disso, a carga útil do datagrama IPsec está codificada." (KUROSE; ROSS, 2010, p.526)

Quando o laptop do vendedor receber o datagrama IPSec, a carga útil é decodificada e pode oferecer serviços de segurança, por exemplo verificar a integridade dos dados, e a parte da carga útil que não for descodificada, passará para a camada superior. Nos próximos tópicos, será apresentado de forma mais detalhada cada processo.

4.2.1 Protocolos AH e ESP

Conforme Brito (2013), a estrutura do IPSec possui dois sub protocolos que oferecem maior flexibilidade, sendo eles o AH e o ESP, esses sub protocolos estão nos cabeçalhos do IPV6 também, e sendo assim eles fazem parte do suporte do IPSEC.

Conforme Stallings (2005), os protocolos principais no IPSec são o AH (Cabeçalho de autenticação) e o ESP (Carga de segurança de encapsulamento), o uso de algum deles ocorrem quando um remetente usa o IPSec para envios de datagramas seguros para um destinatário, esse podendo ser um hospedeiro ou roteador. Esses protocolos tem uma pequena diferença, no caso do AH ele oferece a autenticação do remente e integridade dos pacotes, mas não tem a opção de sigilo, já no caso do ESP, ele oferece integridade, sigilo e autenticação. Geralmente o sigilo é o foco principal nas VPNs e aplicações IPSec, e por esse motivo o ESP é o mais utilizado.

4.2.2 Modo de Transporte e Modo Túnel

O protocolo ESP tem duas opções de modo de operação, o modo túnel e o modo de transporte. O modo de transporte oferece segurança nos protocolos da camada superior, sendo assim essa segurança é para os dados (*payload*) do pacote IP, esse modo é especificamente para comunicação fim a fim entre *hosts*, como um cliente e o servidor. O modo de transporte criptografa somente os dados e existe a opção de autenticar o *payload* IP, mas o cabeçalho IP não é criptografado. O intuito desse modo é para empresas que tenham uma rede pequena e que possuam máquinas equipadas com o IPSec (STALLINGS, 2005).

"[...] somente os dados são criptografados, não havendo nenhuma alteração no cabeçalho da camada de rede, o que permite o roteamento normal dos pacotes pela Internet. Por isso, esse modo de operação é comum em comunicações *host-to-host*." (BRITO, 2013, p.162)

Conforme Stallings (2005), o modo túnel oferece a segurança tanto para o pacote IP completo, tanto para o cabeçalho e para os dados. Esse processo ocorre da seguinte maneira, depois dos campos ESP já estarem incluídos no pacote IP, todo o conteúdo, incluído os campos de segurança é processado como *payload* de pacote IP externo, e isso acaba gerando um novo cabeçalho IP externo. O pacote de origem é transportado por um túnel de uma rede IP para outra, os roteadores não conseguem visualizar o cabeçalho original. Com isso o pacote original passa por esse processo, e resulta em maior tamanho com endereços de origem e destino diferentes, assim reforçando a segurança, e por fim, esse modo é usado quando se deseja criar uma VPN mais avançada.

> [...] todo o pacote é criptografado, o que inclui o *payload* de dados e também os cabeçalhos da camada de rede. Para tanto, é necessário que o pacote seja reencapsulado e receba um novo cabeçalho (túnel) ou, caso contrário, seria impossível roteá-lo pela Internet. Por isso, esse modo de operação é comum em comunicação *site-to-site* onde é estabelecida uma VPN entre roteadores seguros nas bordas. (BRITO, 2013, p.162)

Abaixo a figura 7, mostra como o pacote IP fica no modo de transporte e modo de túnel.

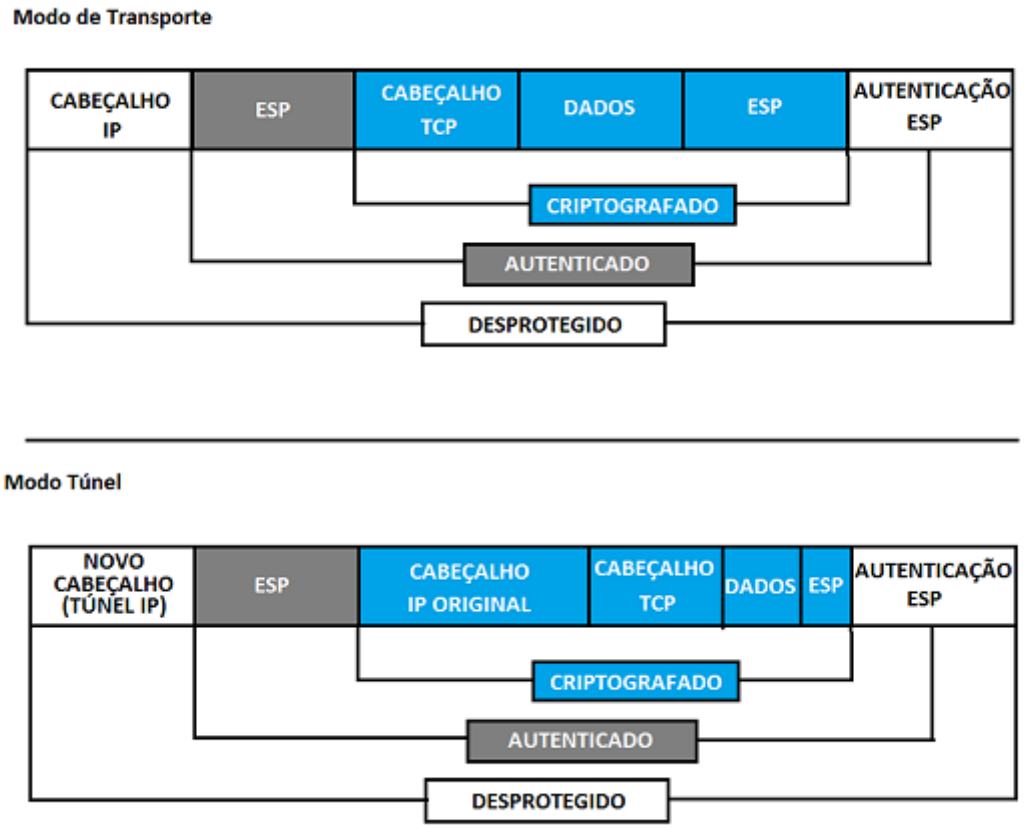

Figura Error! Bookmark not defined. **- Modo de transporte e túnel**
Fonte: Figura baseada em (BRITO, 2013, p161).

4.2.3 Associação de Segurança (SA)

De acordo com Stallings (2005), quando um remetente pretende enviar datagramas IPSec utilizando um protocolo AH ou ESP, antes desse envio é necessário criar uma conexão lógica na camada de rede, essa é chamada de associação de segurança (SA).

A SA nada mais é que uma conexão lógica simplex, sendo unidirecional do remente para o destinatário, se caso duas filiais querem enviar datagramas seguros uma para a outra, então é criado duas SA. Dentro de uma SA existem informações,

essas informações são acessadas pelo roteador para saber como deverá autenticar e criptografar o datagrama que será encaminhado através de uma SA para outro roteador que usara-as mesmas informações.

São seis informações que estão contidas dentro de uma SA, existe um identificador de 32 *bits*, chamado de SPI (Índice de Parâmetro de Segurança), a interface do remetente e do destinatário, qual criptografia será usada, a chave dessa criptografia, uma chave de autenticação e por último, qual o tipo de verificação de integridade. Um roteador ou hospedeiro que utiliza o protocolo IPSec, guardas essas informações para muitas SAs.

4.2.4 Datagrama IPSec

Como o modo túnel é o mais utilizado para VPNs, então será explicado o datagrama IPSec sendo executado no modo túnel. Começando por um exemplo de um computador de uma rede interna de uma matriz, que quer enviar uma mensagem para um computador de uma filial, o roteador da matriz executa etapas para converter o datagrama original em um datagrama IPSEC.

A primeira etapa é a anexação do campo trailer ESP atrás do datagrama original, depois é codificado o resultado utilizando a chave e algoritmo escolhido pela SA, e será adicionado mais um campo chamado cabeçalho ESP, o resultado desse pacote se chama "enchilada", então é criado uma autenticação MAC em toda enchilada usando a chave e algoritmo definidos na SA, é anexado um campo MAC em toda a enchilada formando uma carga útil e a última etapa é criar um novo cabeçalho IP que irá conter todas as informações que foram adicionadas antes da carga útil. Podemos observar a imagem 8 como ficou o datagrama IPSec.

Figura Error! Bookmark not defined. **- Datagrama IPSec**
Fonte: (KUROSE; ROSS, 2010, p.529).

Esse datagrama IPSEC contém o datagrama original mais uma carga útil que foi incluída com alguns campos, sendo eles o cabeçalho ESP, *trailer* ESP e o campo de autenticação ESP. Uma observação interessante é que o datagrama IP original contém o endereço de uma máquina que por exemplo estava em uma matriz, como visto o campo novo cabeçalho IP foi adicionado, nele contém o endereço IP da interface do roteador que é utilizado no túnel, e mais uma observação, o número de protocolo será 50, identificando que esse datagrama IPSec utiliza um protocolo ESP.

No campo *trailer* ESP existem mais três campos abaixo, enchimento, tamanho do enchimento e próximo cabeçalho. O campo enchimento é usado junto com os outros dois campos do lado, quando adicionado ao datagrama original, a mensagem que será encaminhada se transforma em um número inteiro de blocos (KUROSE, 2010).

"O enchimento de dados confunde os *sniffers*, que tentarem acessar as informações sobre a criptografia dos dados em trânsito, nesse caso tentando estimar o número de dados que está sendo transmitido." (BURNETT; PAINE, 2002, p.184)

O campo tamanho do enchimento indica ao destinatário a quantidade de enchimento que foi inserido. E o último campo do *trailer* ESP é o próximo cabeçalho, esse fornece qual tipo de dados está contido no campo de dados da carga útil, esses dados e o *trailer* ESP são concatenados e cifrados.

O cabeçalho ESP também contém campos adicionais, o SPI e o número de sequências. O SPI fica responsável por indicar ao destinatário a SA à qual o datagrama enviado pertence, e o número de sequências é usado para evitar que ataques de repetição aconteçam (KUROSE, 2010).

4.2.5 Gerenciamento de chave

Conforme Stallings (2005), o gerenciamento de chave do protocolo IPSec determina e distribui as chaves secretas, existe suporte para dois tipos de gerenciamento, o manual e o automatizado.

No gerenciamento manual, o administrador do sistema fica responsável pela configuração de cada sistema com as próprias chaves e com outras chaves de sistemas de comunicação, isso é relevante em pequenos ambientes estáticos. O gerenciamento automatizado é feito por um sistema, que gera novas chaves pela demanda, e em ambientes grandes esse procedimento facilita e agiliza esse processo.

Conforme Kurose (2010), o IPSec faz o gerenciamento de chaves com o uso do protocolo de troca de chave (IKE). Cada entidade que utiliza o IPSec, possui um certificado o qual possui uma chave pública.

"Da mesma forma que o SSL, o protocolo IKE tem os dois certificados de troca de entidades, autenticação de negociação e algoritmos de criptografia, e seguramente troca de materiais de chave para criar chaves de sessão nas SAs IPsec." (KUROSE; ROSS, 2010, p.531)

Para realizar esse processo o IKE tem duas fases. A primeira fase ocorre durante a primeira troca de mensagens, tanto o remetente quanto o destinatário usam Diffie-Hellman para a criação de um IKE SA bidirecional entre os roteadores que serão utilizados para a comunicação. Esse IKE SA bidirecional é diferente do SA IPSec, o IKE SA cria um canal autenticado e cifrado entre os roteadores que serão usados. Na primeira troca, ocorre o estabelecimento das chaves para a criptografia e autenticação do IKE SA, e também estabelece um segredo mestre que será usado nas chaves SA IPSec na segunda fase.

Na segunda fase, ocorre a segunda troca de mensagens e os lados que querem estabelecer a comunicação revelam a sua identidade um ao outro, por fim são assinadas as mensagens que serão enviadas através do canal IKE SA, e nessa fase os dois lados troca algoritmos de autenticação e criptografia entre si para ser empregado pelo SA IPSec.

4.3 VPN (Virtual Private Network)

Conforme Pinheiros (2004), uma VPN é uma boa alternativa para empresas que tenham filiais, fornecedores, clientes entre outros espalhados por uma grande região, e precisam se comunicar de maneira segura e sigilosa e evitar altos custos de conexões dedicadas. Por exemplo, uma empresa pode criar uma VPN a partir de uma Internet pública, sem que afete a segurança e outros itens importantes em uma conexão de dados.

> Os conceitos fundamentais de uma VPN são a criptografia e o tunelamento, onde a criptografia garante a autenticidade, a integridade e o sigilo das informações e o tunelamento permite a utilização da rede pública para o tráfego seguro dessas informações. (PINHEIROS, 2004)

O objetivo de uma VPN é estabelecer um túnel de criptografia entre os pontos onde será conectado para a comunicação, usando a internet para as transferências de dados e de informações em um ambiente seguro para os usuários, e também para usuários móveis ou remotos através de uma conexão *dial-up* criptografada.

O quesito mais importante para se ter uma VPN é a segurança, essa deve impedir que dados sejam capturados ou modificados. Um administrador de rede que esteja em uma empresa que possua uma VPN, pode definir os usuários que terão acesso a recursos da rede e também os usuários que não terão esse privilégio. Abaixo a figura 9 mostra uma ilustração de uma rede VPN.

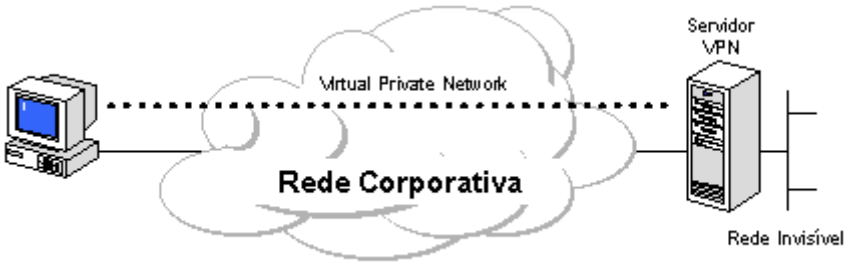

Figura Error! Bookmark not defined. **- Rede corporativa usando a VPN**
Fonte: Projeto de redes. Disponível em: (http://www.projetoderedes.com.br/artigos/artigo_seguranca_vpn.php). Acesso em 20 de abr. 2014.

> As Redes Privadas Virtuais constituem um componente importante dentro do ambiente corporativo das empresas, apresentando-se como uma alternativa segura para transmissão de informações através das redes públicas ou privadas, uma vez que oferecem diversas vantagens para implementação e níveis variados de segurança. (PINHEIROS, 2004)

Porém, um planejamento deve ser feito antes de implantar uma VPN, o tempo de transmissão nas aplicações são um ponto negativo, problemas de desempenho no qual os administradores e usuários não tem controle sobre isso, e pode acabar comprometendo a qualidade dos serviços.

4.4 Criptografia DES e 3DES

A especificação mais nova do IPSec exige que ele aceite o DES para a criptografia que é usada, mas existem diversos algoritmos que podem ser usados no IPSec. A maior preocupação referente ao DES é a força de criptografia dele, e isso acaba sendo um fator para que o 3DES seja o principal algoritmo usado (STALLINGS, 2005).

Conforme FARREL (2005) apud Basso (2011), o DES é um algoritmo usado para criptografar e descriptografar as informações que estão no formato binário, é usado uma chave de tamanho mínimo de 64 *bits*, sendo que 56 *bits* são especificamente para a definição da chave, e os 8 *bits* são para o uso de detecção de erros na chave.

"No início de 1979 de acordo com Tuchman (1979) apud Tanenbaum (2003, p. 557), a IBM percebeu que o tamanho da mensagem DES era muito pequeno e criou uma forma de aumentá-lo usando a criptografia tripla."

Conforme Tanenbaum (2003), o 3DES utiliza duas chaves e três estágios para criptografar as informações. No primeiro estágio ocorre a criptografia do texto simples utilizando a chave k1, depois disso é realizado o processo inverso, a descriptografia utilizando a chave k2, e na última etapa é feita uma nova criptografia utilizando a chave k1.

> O motivo para criptografar, descriptografar e criptografar mais uma vez é a compatibilidade retroativa com os sistemas DES de chave única existentes. Tanto as funções de criptografia quanto as de descriptografia são mapeamentos entre conjuntos de números de 64 bits. (TANENBAUM, 2003, p.788)

4.5 RFC 4301

Conforme Kent and Seo (2005), o documento mais atual sobre o IPSec é a RFC 4301, esse documento contém itens que foram adicionados desde da primeira RFC referente ao protocolo IPSec. Nessa RFC é abordado a segurança da arquitetura IP que fornece a segurança das transferências na camada IP.

Nesse documento está especificado a base da arquitetura IPSec, descrevendo também os serviços de segurança no tráfego IP, tanto em ambientes IPv4 quanto IPv6. Na RFC 4301 é indicado os requisitos de sistemas para a implementação do IPSec, elementos fundamentais do sistema, como os elementos trabalham em conjunto para se inserir no ambiente IP, e também aborda os serviços de segurança do IPSec e como são empregados nesse ambiente.

Algumas funções essenciais como a utilização do IPSec em NAT, protocolos de segurança AH e ESP, associações de segurança, gerenciamento de chaves, algoritmos de criptografia e autenticação, não são explicadas totalmente, na maioria delas são apontadas as RFC que tratam sobre o assunto.

4.6 IPv6: IPSEC como ferramenta de segurança

Conforme Brito (2013), a arquitetura do IPv6 é mais vantajosa comparado ao IPv4, tanto que a segurança na versão 4 era somente um projeto e agora com a nova versão, a segurança é o critério mais importante. O Protocolo IPSec foi especificamente criado para o IPv6, e depois foi aproveitado para ser usado no IPv4, atualmente existem várias soluções de segurança que oferecem suporte ao protocolo IPSec.

> Essa afirmação "folclórica" de que o IPv6 é um protocolo mais seguro vem do fato de ele possuir suporte nativo ao IPSEC. Por isso, muitas pessoas pensam que todo o tráfego v6 sempre é criptografado automaticamente sem nenhuma intervenção ou configuração do administrador - o que NÃO é verdade! (BRITO, 2013, p.134)

Pelo fato do IPv6 agora possuir a segurança nativa, é determinado que o IPSec esteja incluso nos protocolos da arquitetura TCP/IPv6. Assim, dispositivos que suportam o IPv6 já estão com o IPSec incluso, sendo uma segurança embutida no IPv6, ao contrário de dispositivos que tenham suporte somente para IPv4, nesse caso os profissionais de redes tem que analisar a existência do suporte ao IPSec.

Mesmo no caso de um equipamento ter o suporte ao IPSec, deve-se ficar atento, a segurança não é autoconfigurável, a criptografia e autenticação são itens que devem ser configurados manualmente pelo administrador.

5 DEMONSTRANDO O PROTOCOLO IPSEC

Nos capítulos anteriores foram abordados as características do IPSec e todo o processo de funcionamento, desde da camada que se localiza, trocas de chaves, criptografia entre outras itens importantes. Esse protocolo é nativo do IPv6, depois disso foi inserido também no IPv4.

Agora será apresentado dois exemplos práticos da utilização do protocolo IPSec em uma rede, para isso foi utilizado duas ferramentas da cisco para a simulação, o packet tracer e o gns3.

5.1 Rede IPv4

Para esse cenário de rede IPv4 foi utilizado o programa packet tracer para fazer a simulação, e o site **learning network** para a configuração. Na figura 10, existem duas redes IPv4 e precisam se comunicar com segurança para a transferência de arquivos sigilosos, e para isso utilizaram o IPSec e todas as ferramentas desse protocolo.

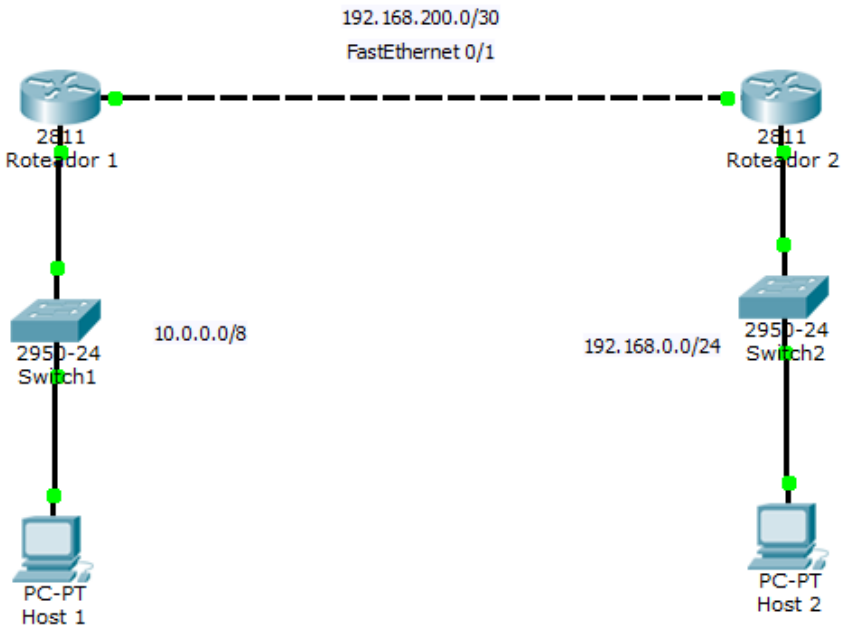

Figura Error! Bookmark not defined. **- Topologia da rede IPv4**
Fonte: Autoria própria.

Foram utilizados dois roteadores, dois *switchs* e dois *host* como é mostrado no exemplo, ambas as redes receberam o endereço IPv4 e de forma manual. Os *hosts* receberam os IPs das próprias rede mudando apenas o último valor para 2, já os roteadores possuem duas interfaces, as f0/1 para se comunicar com o outro roteador, e a interface f0/0 para se comunicar com a rede interna.

Após a configuração manual dos endereços, se iniciou a ativação e configuração do protocolo IPSec. Foram inseridos vários comandos nos consoles de ambos roteadores para a configuração, os primeiros comandos foram referentes ao tipo de autenticação, criptografia e verificação de integridade de dados que estarão na política, na figura 11 são mostrados esses comandos.

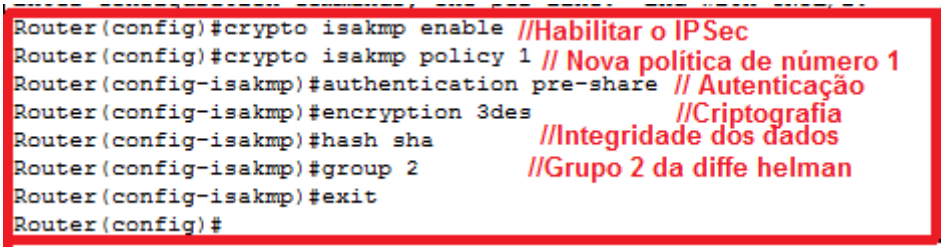

Figura Error! Bookmark not defined. **- Configuração de política**
Fonte: Autoria própria.

Esses comandos são inseridos da mesma forma em ambos os roteadores. Analisando a figura 10, o primeiro passo foi habilitar o protocolo IPSec, logo em seguida foi criada uma política e depois definidos os tipos de autenticação, criptografia, verificação de integridade dos dados e qual tipo de trocas de chaves serão usadas. Nesse exemplo foi usado a autenticação *pre-share*, a criptografia 3DES, a verificação de integridade *hash sha* e o grupo dois de trocas de chaves da *diffie helman*.

O próximo passo é sobre a configuração de qual sub protocolo será utilizado, número da chave, quais redes estarão incluídas na VPN, logo a seguir a figura 12 ilustra os comandos digitados.

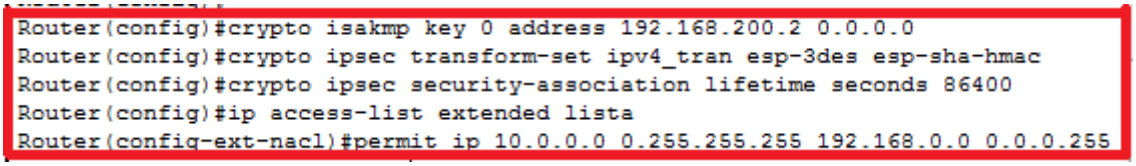

Figura Error! Bookmark not defined. **- Configuração de permissão, sub protocolo e número de chave.**

Fonte: Autoria própria.

Na primeira linha o código *key* 0 significa que a chave que será usada é a de número 0, e o endereço IP do outro roteador que será localizado para a transferência segura, e em vez da máscara de sub rede do roteador é colocado 0.0.0.0. Na segunda linha é definido um conjunto de transformação chamado ipv4_tran e também qual será o sub protocolo AH ou ESP, nesse caso o ESP. Na terceira linha é informada a duração da chave até expirar, na quarta linha é criada uma ACL com o nome lista que vai informar que o tráfego usará um túnel VPN, e na última linha é informado quais redes internas serão permitidas. Uma pequena observação, essa configuração foi feita no roteador 1, sendo assim, a configuração do roteador dois contém duas mudanças, na primeira linha que o IP será do roteador 1, e na última linha que o endereço IP da rede internet, sendo a primeira rede interna do roteador 2 e depois a rede interna do roteador 1.

Na próxima figura será mostrado a configuração referente ao mapa de criptografia e quais redes estão incluídas.

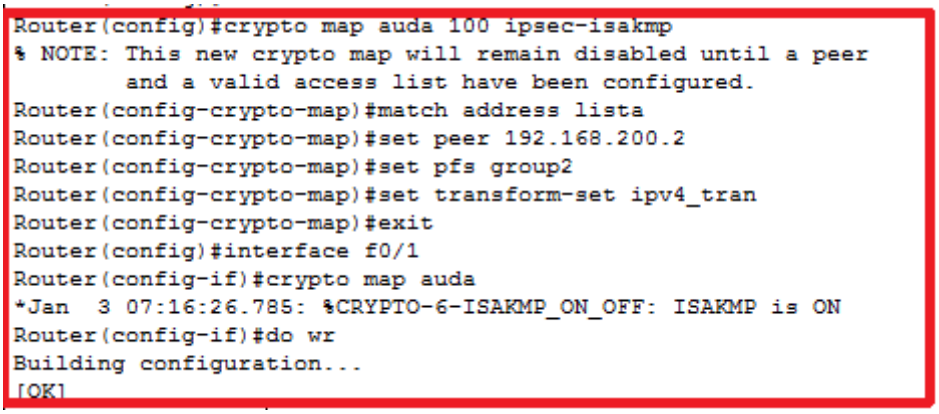

Figura Error! Bookmark not defined. **- Mapa de criptografia**
Fonte: Autoria própria.

Essa é a última etapa dessa configuração, na primeira linha foi criado um mapa de criptografia chamado de auda, com o número de sequência 100, no momento que é executada essa linha, o mapa é desativado até que seja feita a configuração de lista de acesso. Na segunda linha é indicado que os endereços estão na lista de acesso chamado lista, já na terceira linha é indicado o IP do roteador 2 para o mapa de criptografia. Na quarta linha e quinta linha é definido que o grupo 2 e o conjunto de transformação chamado ipv4 estarão no mapa de criptografia.

Depois disso é acessado a interface 0/1, responsável pelo contato com o

roteador 2, feito isso o comando contendo o mapa e o nome dele é executado, e assim é ativado o IPSec.

Agora serão exibidos alguns comandos que mostram como estão as configurações atuais. A figura 14 a seguir contém as políticas que foram ativadas e as opções e as opções definidas, bem como criptografia, autenticação entre outros.

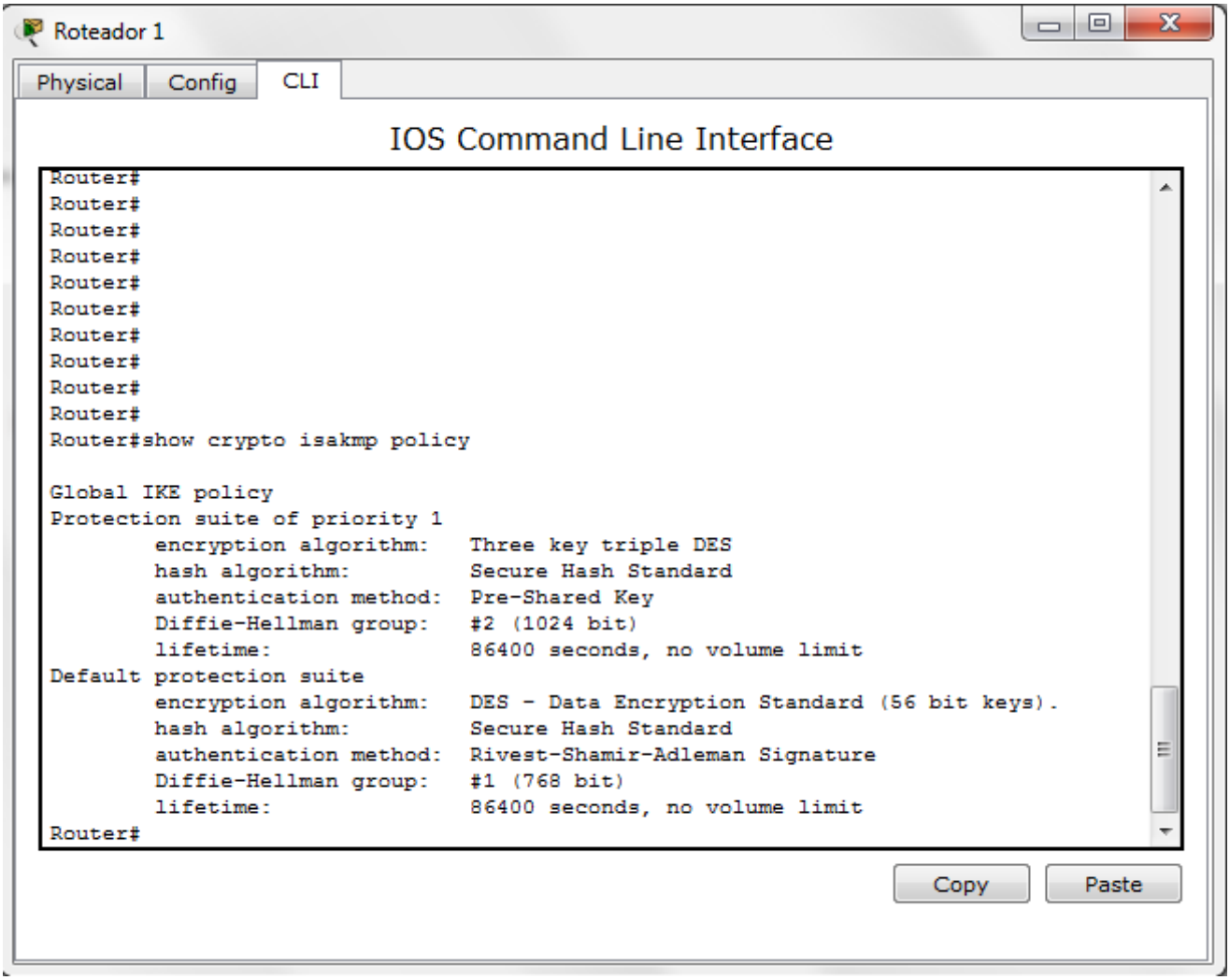

Figura Error! Bookmark not defined. **- Políticas Definidas**
Fonte: Autoria própria.

A figura 15 contém detalhes sobre o IP de origem e destino para a rota segura, IPs das redes internas autorizadas e em qual interface *fast ethernet* que foi aplicado o mapa de criptografia.

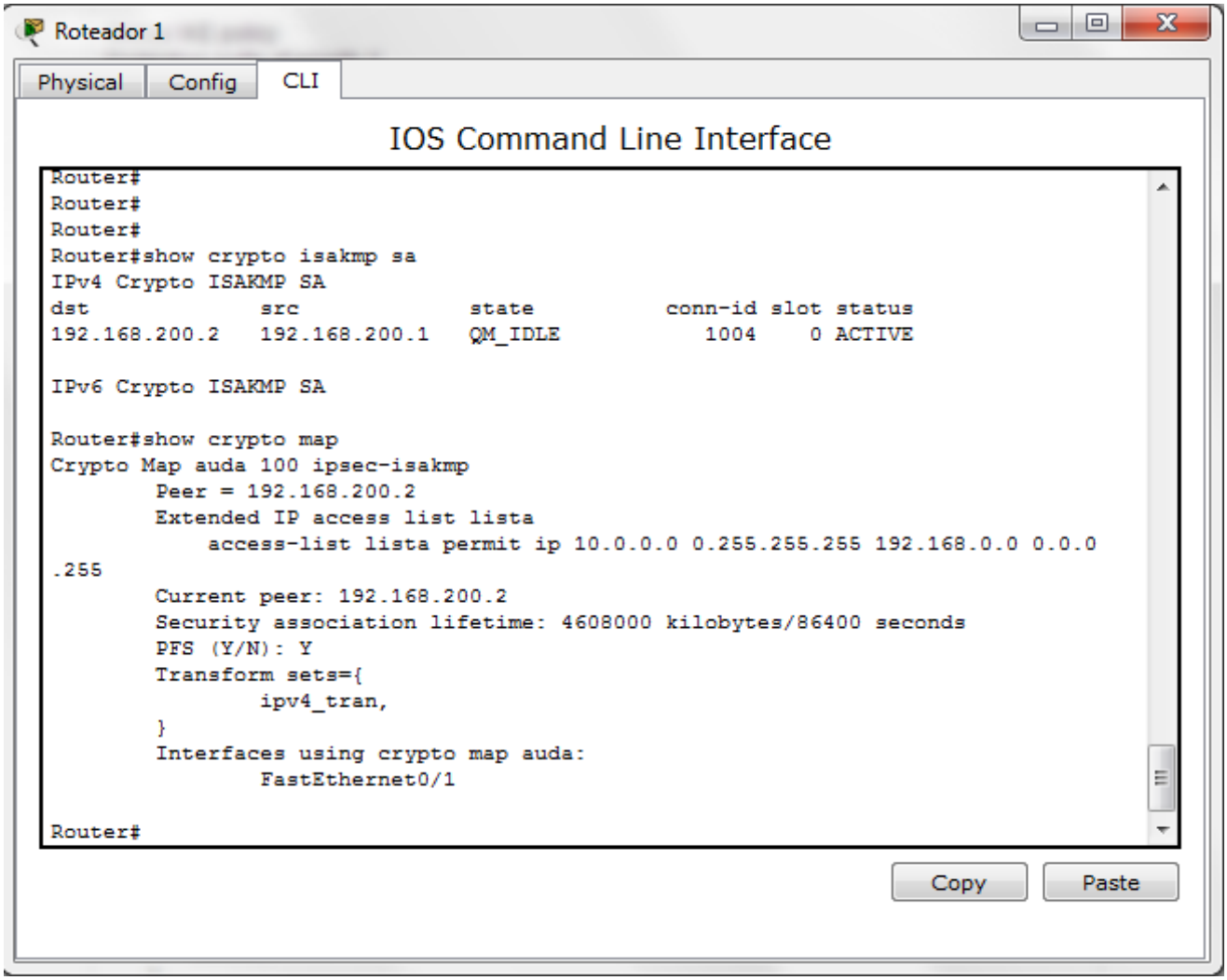

Figura Error! Bookmark not defined. **- Mapa de criptografia**
Fonte: Autoria própria.

E a figura 16 mostra informações sobre as redes autorizadas, tanto interna quanto a rede do outro roteador, antes desse comando, foi dado um *ping* do *host* do roteador 1 para o *host* do roteador 2. Depois disso, esse comando mostra quanto pacotes foram criptografados e descriptografados, e quantos foram encapsulados e descapsulados.

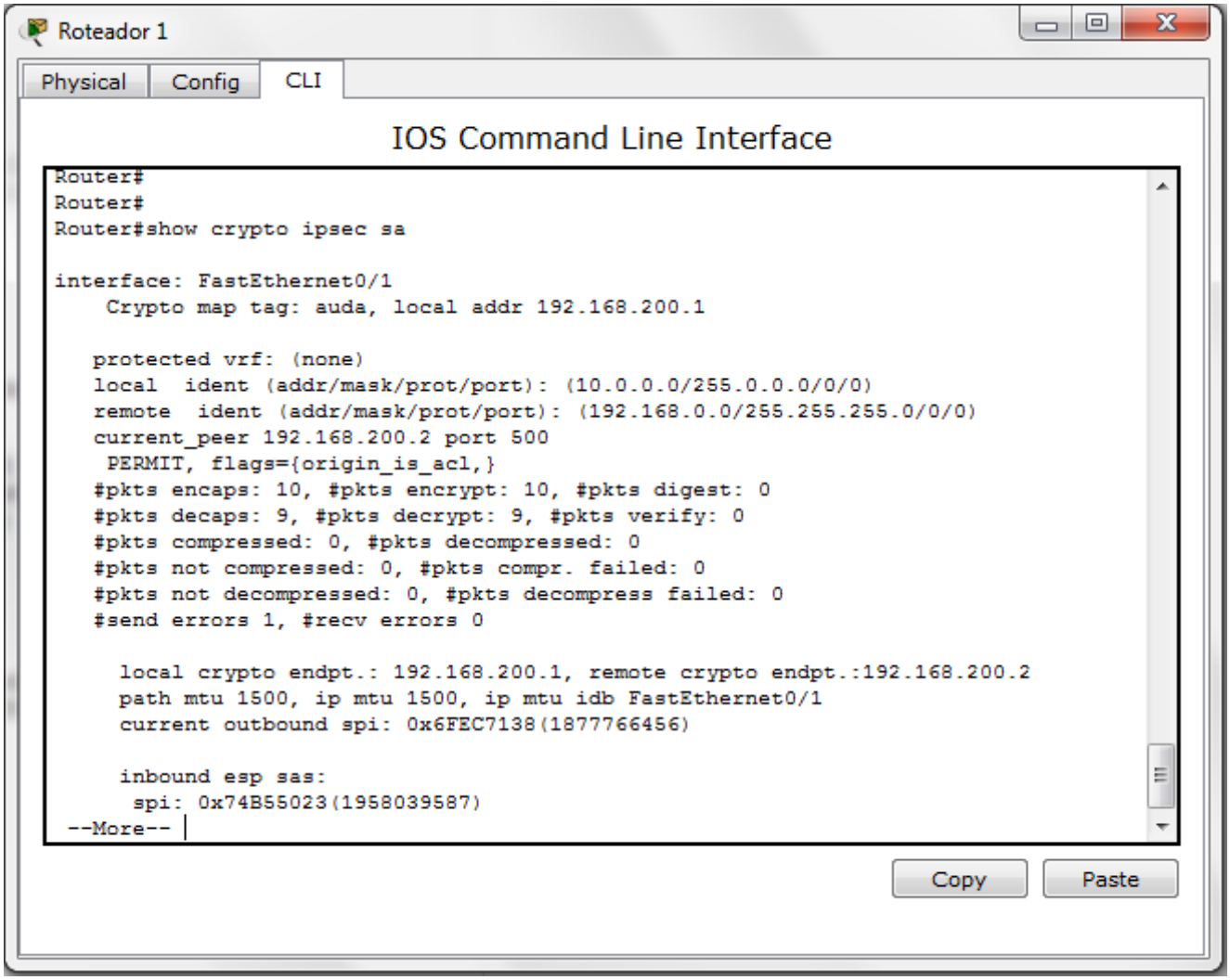

Figura Error! Bookmark not defined. **- Pacotes criptografados e encapsulados.**
Fonte: Autoria própria.

5.2 Rede IPv6

Nessa outra parte do estudo de caso será utilizado o programa gns3 da cisco para a construção de uma rede IPv6 e a configuração do IPSec, e um tutorial do fórum de suporte da cisco. Na figura 17, existe duas redes IPv6 se comunicando por dois roteadores, com a ativação e configuração IPSec, essas redes usarão um túnel para garantir mais segurança.

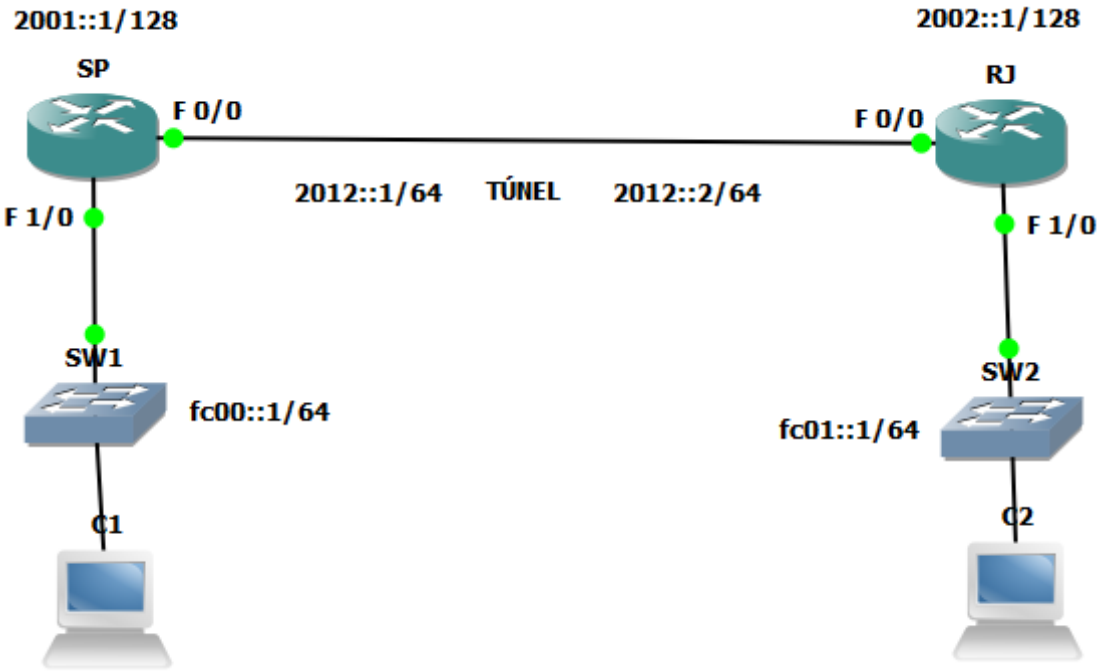

Figura Error! Bookmark not defined. **- Topologia da rede Ipv6**
Fonte: Autoria própria.

O Processo de configuração da rede IPv6 é bem semelhante à da rede IPv4, mudando pequenos detalhes. A figura 18 contém informações sobre as políticas definidas, sendo elas a criptografia, autenticação e o grupo de *diffie helman*.

```
R3(config)#
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#
```

Figura Error! Bookmark not defined. **- Configurações de políticas**
Fonte: Autoria própria.

As configurações das políticas foram configuradas da mesma maneira nos dois roteadores, sendo a criptografia 3DES e a autenticação *pre-share*. A figura 19 mostra a configuração do conjunto de transformação e o perfil do IPSec.

```
R3(config)#crypto isakmp key 0 ipsecvpn address ipv6 2002::1/128
R3(config)#crypto ipsec transform-set ipv6_tran esp-3des esp-sha-hmac
R3(cfg-crypto-trans)#mode tunnel
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec profile ipv6_ipsec_pro
R3(ipsec-profile)#set transform-set ipv6_tran
R3(ipsec-profile)#exit
R3(config)#
```

Figura Error! Bookmark not defined. **- Conjunto de transformação e o perfil do IPSec.**
Fonte: Autoria própria.

Na primeira linha é especificado o número da chave e o IP do próximo roteador, na segunda linha é criado um conjunto de transformação chamado ipv6_vpn que usará o sub protocolo ESP com a criptografia 3DES e a integridade dos dados será verificada pelo HMAC. Depois disso é criado um perfil IPSec com o nome ipv6_ipsec_pro e em seguida é definido que o conjunto de transformação será o ipv6_tran. A figura 20 mostra como é feita a configuração do perfil ISAKMP no IPv6.

```
R3(config)#crypto isakmp profile 3des
% A profile is deemed incomplete until it has match identity statements
R3(conf-isa-prof)#self-identity address ipv6
R3(conf-isa-prof)#match identity address ipv6 2002::1/128
R3(conf-isa-prof)#keyring default
R3(conf-isa-prof)#exit
```

Figura Error! Bookmark not defined. **- Configuração do ISAKMP**
Fonte: Autoria própria.

Nessa parte é especificado o endereço IP do próximo roteador, e se o endereço é IPv6 ou não, e a *keyring* ficou como padrão. Na próxima fase é configurado o túnel, onde será passado os pacotes, os comandos estão na figura 21.

```
R4(config)#interface tunnel 1
R4(config-if)#ipv6 enable
R4(config-if)#ipv6 address 2012::1/64
R4(config-if)#tunnel source 2001::1
R4(config-if)#tunnel destination 2002::1
R4(config-if)#tunnel mode ipsec ipv6
R4(config-if)#tunnel protection ipsec profile ipv6_ipsec_pro
R4(config-if)#
*Jun  6 13:09:02.715: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figura Error! Bookmark not defined. **- Configuração do Túnel**
Fonte: Autoria própria.

A interface escolhida foi a túnel 1 e foi atribuído um endereço IPv6, feito isso, foi definido o endereço de destino e origem, e por fim, a escolha do perfil da proteção do túnel IPSec, resultando na ativação do ISAKMP. A última parte é a configuração de rota, a figura 22 a rota sendo configurada.

```
R4(config)#ipv6 route fc01::/64 2012::2
R4(config)#
```

Figura Error! Bookmark not defined. **- Configuração das rotas**
Fonte: Autoria própria.

Essa configuração de rota é a parte final, primeiro é inserido o endereço IP da rede interna do outro roteador, e depois por onde será o próximo salto, que é pelo endereço IP do túnel configurado.

Feito todas essas configurações, é verificado se tudo ocorreu corretamente e da forma planejada. As próximas imagens serão sobre a execução do IPSec e verificação dele. A imagem 23 mostra que o destino e origem usarão o IPSec, as configurações da criptografia, e também quantos pacotes foram criptografados e descriptografados até agora.

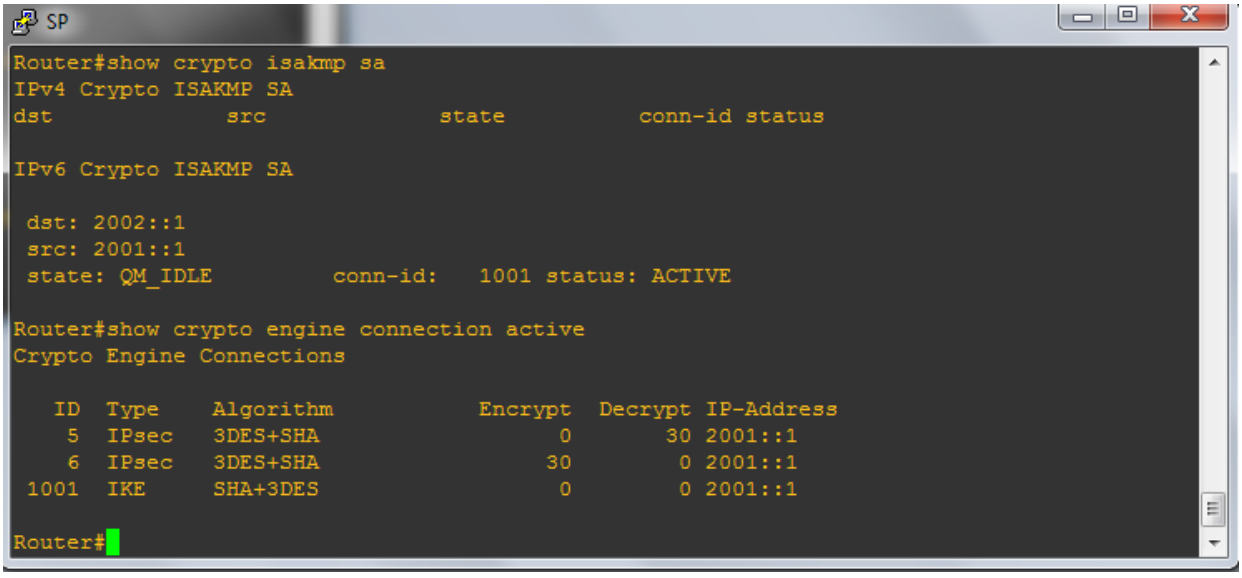

Figura Error! Bookmark not defined. **- Resultado final**
Fonte: Autoria própria.

6 CONCLUSÃO

Na internet existe um tráfego imenso de informações importantes, sem o uso de alguma ferramenta que possa reduzir o risco de algum problema, com certeza em algum momento os dados podem ser alterados ou visualizados sem consentimento do autor.

O IPSec é um protocolo que oferece uma grande segurança nas transferências de dados pela rede. São vários itens dentro do protocolo IPSec que juntos tornam-se um protocolo que auxilia em muito na questão da segurança.

Para o ativamento e configuração do IPSec é preciso ter conhecimento avançado em redes de computadores. Uma vez que a configuração demanda tempo e uma grande atenção. Antes de tudo, deve-se ser feita uma análise da rede, e conhecer a estrutura de funcionamento do IPSec e das redes que serão utilizadas, afim de fazer a melhor configuração possível.

O estudo de caso foi a parte mais importante desse trabalho, demostrou a prática de uma implantação em uma rede que continha uma filial e uma matriz, a configuração dessas redes foi organizada o mais próximo possível de uma rede organizacional. A configuração do IPSec exigi um alto nível de conhecimento em redes, principalmente em configurações de roteadores, pois exige uma planejamento de quais redes internas e externas serão utilizadas, e os tipos de criptografia e autenticação.

O protocolo IPSec pode ajudar muito os administradores de redes. Ele possui um conjunto que auxilia a segurança, primeiramente os sub protocolos tem um papel importante no IPSec, ele encapsula as informações de tal maneira que dificulta muito a ação de alguém que queira captura os pacotes e visualizar. Outro recurso é o modo de que são transferidos os pacotes, ele criptografa o cabeçalho original e gera um novo cabeçalho maior, o gerenciamento das chaves contém vários passos para obter sucesso, o esquema de duas chaves e três estágios acaba gerando uma segurança complexa para o IPSec. O IPSec tem uma vantagem em cima das criptografias e autenticações, ele não fica dependente de só alguns tipos, conforme novos tipos de criptografia são lançados, possibilita de ser usado no protocolo IPSec.

A questão de segurança acaba sendo indispensável quando existem dados importantes na rede, e outro motivo que acaba sendo interessante para as empresas, é o modo que pode se utilizar o IPSec junto com uma rede pública que é a Internet, assim reduzindo gasto com um *link* privado.

Esse trabalho foi importante para o aumento do meu conhecimento, pois visto que além do levantamento do estudo sobre o protocolo IPSec, houve a parte prática tanto quanto a criação de uma rede e a implantação e configuração do IPSec. Futuramente, posso utilizar esse conhecimento para ser aplicado em uma organização que farei parte, e assim ajudando a empresa com mais uma ferramenta de segurança de baixo custo.

REFERÊNCIAS BIBLIOGRÁFICAS

ASHIRKAR. **Configuration Example: Site-to-Site VPN for IPv6 IPsec**. 2012. Disponível em: < https://supportforums.cisco.com/document/112896/configuration-example-site-site-vpn-ipv6-ipsec>

AUDA, Y. R. **VPN site to site packet tracer 5.3 lab.** 2010. Disponível em: < https://learningnetwork.cisco.com/docs/DOC-10756> Acesso em: 15 mai. 2014

BARRETT, D.; KING, T. **Redes de computadores**. 1°. ed. Rio de Janeiro: LTC, 2010. 478p.

BASSO, C. **Implementação de IPSec integrado com o IPv6**. 2011. 66f. Monografia (Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade Tecnológica Federal do Paraná (UTFPR), Pato Branco, 2011. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/198/1/PB_COADS_2011_1_07.pdf> Acesso em: 2 jun. 2014

BRITO, S. H. B. **IPv6 O Novo Protocolo da Internet**. 1ª. ed. São Paulo: Novatec, 2013. 208p.

BURNETT, S.; PAINE, S. **Criptografia e Segurança: O Guia Oficial RSA**. 3ª. ed. Rio de Janeiro: Elsevier, 2002. 392p.

FALCONI, A. P. **Uso dinâmico do IPSEC com IPV6**. 2004. 81f. Dissertação (Mestrado em Computação Aplicada) - Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2004. Disponível em: <http://mtc-m18.sid.inpe.br/col/sid.inpe.br/jeferson/2005/01.07.10.46/doc/publicacao.pdf> Acesso em: 26 mai. 2014

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet : uma abordagem top-down**. 5ª. ed. São Paulo: Addison Wesley, 2010. 614p.

MOREIRAS, M. A. **Google já vê 3% dos usuários em IPv6**. 2014. Disponível em: < http://ipv6.br/google-ja-ve-3-dos-usuarios-em-ipv6/> **Acesso em: 15 abr. 2014**

PINHEIRO, J. M. S. **Segurança em Redes Privadas Virtuais.** 2004 Disponível em: < http://www.projetoderedes.com.br/artigos/artigo_seguranca_vpn.php> Acesso em: 20 mai. 2014

SEO, K; KENT, S. **RFC 4301** - **Security Architecture for Internet Protocol**. 2005. Disponível em: < http://tools.ietf.org/html/rfc4301> Acesso em: 02 mai. 2014

SILVA, S. H. V. C. et al. **API IPSEC - Viabilizando a segurança de redes**. In: Conferência de Estudos em Engenharia Elétrica, VIII, 2010, Uberlândia. Disponível em: < http://www.ceel.eletrica.ufu.br/artigos2010/ceel2010_04.pdf> Acesso em: 20 mai. 2014

STALLINGS, W. **Redes e sistemas de comunicação de dados : teoria e aplicações corporativas**. 5ª . ed. Rio de Janeiro: Elsevier, 2005. 449p.

TANENBAUM, A. S. **Redes de computadores**. 4ª. ed. Rio de Janeiro: Elsevier, 2003. 945p.