UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

EDUARDO WOJCIK

ANÁLISE E SIMULAÇÃO DE VPN COM IPSEC EM ROTEADORES CISCO

MONOGRAFIA

CURITIBA
2011

EDUARDO WOJCIK

ANÁLISE E SIMULAÇÃO DE VPN COM IPSEC EM ROTEADORES CISCO

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Juliano de Mello Pedroso

CURITIBA
2014

AGRADECIMENTOS

Agradeço a oportunidade de ter conseguido estudar na Universidade Tecnológica Federal do Paraná, e a todos os colaborados que fazem parte desta instituição.

Ao Prof. Juliano de Mello Pedroso, pela orientação, e dedicação durante esse ano, obrigado pela confiança depositada em mim.

À Maria, minha mãe. É impossível expressar o amor e a admiração que tenho por ti.

À Lidia Wojcik. Você tornou possível a realização de um sonho.

Às minhas irmãs, Adriana e Fabiana pelo incentivo e apoio incondicional.

Aos meus amigos, Guilherme Clemente e Fabiano Ravaglio Heidemann que torceram por mim e me apoiaram sempre!

A todos que fazem parte da minha vida e contribuíram de alguma forma.

RESUMO

WOJCIK, Eduardo. **Análise e simulação de VPN com IPSEC em roteadores Cisco.** 2014. 56f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

O propósito desta monografia é apresentar e explicar as medidas necessárias para configurar o modo de túnel IPSEC utilizando roteadores Cisco para compartilhar de forma segura o acesso a uma rede privada, através da internet. Para as empresas, hoje, a necessidade de compartilhar dados entre diferentes filiais é maior do que nunca. A internet oferece um modo econômico e com uma infraestrutura pré-existente para realizar isso, mas possui muitas ameaças de segurança. A pesquisa apresenta conceitos teóricos juntamente com uma aplicação prática simulada em um ambiente real, demonstrando a viabilidade, as funcionalidades e as técnicas utilizadas para a aplicabilidade do IPSEC em redes de pequeno porte na internet atual utilizando roteadores Cisco.

Palavras-chave: IPSEC, VPN, análise, simulação.

ABSTRACT

WOJCIK, Eduardo. **Análise e simulação de VPN com IPSEC em roteadores Cisco.** 2014. 56f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

The purpose of this monograph is to present and explain the necessary steps to configure the IPSec tunnel mode using Cisco routers to securely share access to a private network through the Internet. For businesses today, the need to share data between different branches is greater than ever. The internet provides an economical way and with a pre-existing infrastructure to accomplish this, but it has many security threats. The research presents theoretical concepts along with a simulated practical application in a real environment, demonstrating the practicality, functionality and the techniques used for the applicability of IPSEC in small networks in the current Internet using Cisco routers.

Keywords: IPSEC, VPN, analysis, simulation.

LISTA DE SIGLAS

VPN - *Virtual Private Networks;*
IPSec - *Internet Protocol Security*;
IP - *Internet Protocol;*
OSI - *Open Systems Interconnection*;
RFC - *Request for Comments*;
IETF - *Internet Engineering Task Force*;
ISO - *International Standards Organization*;
IPv4 - *Internet Protocol version 4;*
IPv6 - *Internet Protocol version 6*;
NIC.br - Núcleo de Informação e Coordenação do Ponto BR;
QoS - *Class of Services*;
ARP - *Address Resolution Protocol;*
MAC - *Media Access Control*;
NTP - *Network Time Protocol*
IGMP - *Internet Group Management Protocol*;
MLD - *Multicast Listner Discovery;*
DHCP - *Dynamic Host Configuration Protoc*ol;
CIDR - *Classless Inter Domain Routing;*
PPP - *Point-to-Point Protocol;*
DNS - *Domain Name System*;
TTL - *Time to live;*
DH - *Diffie-Hellman*;
AH - *Authentication Header;*
ESP - *Encapsulating Security Payload;*
DES - *Digital Encryption Standard;*
3-DES - *Triple Digital Encryption Standard;*
AES - *Advanced Encryption Standard;*
IKE - *Internet Key Exchange;*
IKEv2 - *Internet Key Exchange version 2;*
PSK - *Pre-Shared Keys;*
RSA - *RSA public key cryptography algorithm;*
MD5 - *Message Digest 5;*
SHA - *Secure Hash Algorithm;*
HMAC - *Hashed Message Authentication Codes;*
SA - *Security Association;*
SAD-SA - *Security Association Database;*
ISAKMP - *Internet Security Association Key Management Protocol;*
OAKLEY - Oakley *Key Determination Protocol;*
SKEME - *Secure Key Exchange Mechanism;*
EAP - *Extensible Authentication Protocol;*
IOS - *Internetwork Operating Systems;*
RIPng - *Routing Information Protocol next generation.*
ACL - *Access Control List*
CEFv6 - Cisco *Express Forwarding for* IPv6
ULA - *Unique Local Address*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo será tradado o Tema, Delimitação da Pesquisa, Problemas e Premissas, o Objetivo Geral, os Objetivos Específicos, Justificativa, Procedimentos Metodológicos, Embasamento Teórico e a Estrutura deste trabalho.

1.1 TEMA

A necessidade de Organizações que muitas vezes precisam transferir dados entre filiais geograficamente separadas é cada vez maior, enquanto que as linhas privadas proporcionam uma maneira segura de se fazer isso, elas não são economicamente viáveis para as empresas de pequeno ou de médio porte.

Quando surgiram as redes públicas de dados e mais tarde a Internet, muitas empresas optaram por mover seu tráfego de dados para a rede pública, mas sem desistirem da segurança da rede privada. Essa demanda levou à criação de *Virtual Private Network* - Rede Privada Virtual (VPN), que são redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque é meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real (Tanenbaum, 2011).

O *Internet Protocol Security* – Protocolo de Segurança IP (IPSec) descrito na RFC 4301 é uma solução de segurança em nível de 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*. Atualmente, essa solução é mais comumente utilizada nos dispositivos da infraestrutura que têm suporte ao IPSec (Brito, 2013).

IPSec é uma estrutura de padrões abertos com o intuito de assegurar comunicações privadas seguras em protocolos *Internet Protocol* – protocolo de internet (IP). Ele garante confidencialidade, integridade e autenticidade de comunicação de dados em uma rede IP pública (Wenstrom, 2002).

- ✓ Confidencialidade: O principio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação (Campos, 2008).
- ✓ Integridade: O principio da integridade é respeitado quando a informação acessada esta completa sem alterações e, portanto, confiável (Campos, 2008).

- ✓ Disponibilidade: O principio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas sempre que necessário (Campos, 2008).

Esse recurso fornece um componente necessário de uma solução flexível baseada em padrões para implementar uma política de segurança por toda a rede. O IPSec pode ser usado para resguardar o trafego entre dois roteadores de perímetro em uma topologia de uma instalação física a outra criando uma VPN entre um local corporativo central e um local corporativo remoto, uma filial ou uma rede *extranet* (parceira). Todo o trafego entre os roteadores de perímetro pode ser criptografado, ou somente fluxos selecionados entre *hosts* ou redes por trás dos roteadores podem ser criptografados (Wenstrom, 2002).

O IPSec oferece exatamente essa solução. Se o IPSec for usado no tunelamento, será possível agregar todo o tráfego entre dois pares de escritórios quaisquer em uma única chave autenticada e criptografada, fornecendo assim controle de integridade, sigilo e até mesmo uma considerável imunidade à análise de tráfego.

Uma rede segura, econômica e expansível, VPN com IPSec oferece exatamente essa solução.

1.1.1 Delimitação de Pesquisa

Para um bom entendimento dessa pesquisa, será mostrado primeiramente às três primeiras camadas do modelo OSI, o funcionamento básico do protocolo IPv6, em seguida será abordado o conjunto do protocolo IPSec, como ele funciona e suas principais características, esta pesquisa será feita em um ambiente simulado utilizando roteadores Cisco.

Será feita a configuração de três roteadores, aonde um representara uma conexão publica, simulando um ambiente inseguro, permitindo assim a conectividade, de uma rede privada a outra através de uma VPN e demonstrando a configuração dos mesmos.

1.2 PROBLEMA E PREMISSAS.

A segurança pode ser aplicada em diferentes camadas do modelo OSI, na camada de enlace por exemplo oferece proteção, mas só é viável para uma rede privada não separadas por grandes distâncias geográficas. Na internet a segurança deve ser implementada em camadas mais elevadas. A solução está

em oferecer segurança na camada que é comum à grande infraestrutura da Internet, na camada de rede. Uma vez que a arquitetura da internet em partes é essencialmente o protocolo de Internet, para interligar os nós e os dispositivos na rede nesse caso é desejável que uma solução de segurança seja aplicada uniformemente nesta camada

1.3 OBJETIVOS

Nesta sessão serão apresentados o objetivo geral e objetivos específicos, que se pretende atingir com este projeto de pesquisa.

1.3.1 Objetivo Geral

Implementar e analisar o protocolo de segurança IPSec e sua implementação em roteadores Cisco, verificando as suas características, assim como realizar testes simulados de seu funcionamento verificando os requisitos fundamentais da tecnologia.

1.3.2 Objetivos Específicos

- Estudar o funcionamento do IPSec;
- Implementar uma topologia demonstrando o funcionamento de uma rede com roteador Cisco e IPSec;
- Fazer a análise das informações;

1.4 JUSTIFICATIVA

Utilizar roteadores com conexões de internet e banda larga proporcionando a transferência de informação com segurança para empresas de pequeno e médio porte.

A Redução de custos de comunicação e proporcionar uma maior flexibilidade. Gerenciamento simplificado com fácil provisionamento e gerenciamento de usuários através de uma interface de gerenciamento centralizada de políticas.

Alta escalabilidade e agrupamento de características dinâmicas que se estendem a uma rede privada. Os clientes VPN por *Hardware*: Independência do *software* do *host* e a implementação de uma VPN simples e de apoio. Fornecimento de comunicações seguras com direitos de acesso adaptados para usuários individuais e departamentos, tais como empregados, prestadores de serviços ou parceiros. Melhora na produtividade, estendendo a rede e aplicativos corporativos.

1.5 PROCEDIMENTOS METODOLÓGICOS,

Para o estudo utilizar-se-á referências bibliográficas, pesquisa em *Request For Comments* - Requisições para Comentários (RFC) e em documentações técnicas relacionadas à segurança de rede referentes ao tema tratado. Com os dados necessários obtidos a parte pratica terá inicio. Serão utilizados roteadores em ambiente simulado demonstrando os processos de configuração utilizando o protocolo IPSec e terão como base documentação provenientes da Cisco, para sua implantação.

1.6 EMBASAMENTO TEÓRICO

Para descrever sobre conceitos de rede destacam-se os trabalhos bibliográficos de Tanenbaum (2011) e Santos (2008). Para descrever os conceitos sobre IPSec, criptografia de camada de rede com protocolos IPSec destacam-se os trabalho bibliográficos de Wenstrom (2002) e artigos regulamentadores da tecnologia como RFC regulamentada pela *Internet Engineering Task Force* – Força Tarefa de Engenharia para a Internet (IETF).

2 REFERÊNCIAL TEÓRICO

Este capítulo apresenta uma visão geral do modelo de referencia OSI, uma visão geral do endereçamento e cabeçalhos do protocolo IPv6, e das etapas e funcionamento básico da IPSec usados para criar uma VPN.

2.1 O MODELO DE REFERÊNCIA OSI

O *Open Systems Interconnection* – Modelo de Referência ISO OSI (OSI) é baseado em uma proposta desenvolvida pela *International Standards Organization* (ISO) em 1983 e foi atualizado em 1995, normalmente denominado simplesmente de modelo OSI, trata da interconexão de sistemas abertos (Tanenbaum, 2011).

O modelo OSI possui sete camadas, com seu formato de funcionamento ilustrado na figura 1.

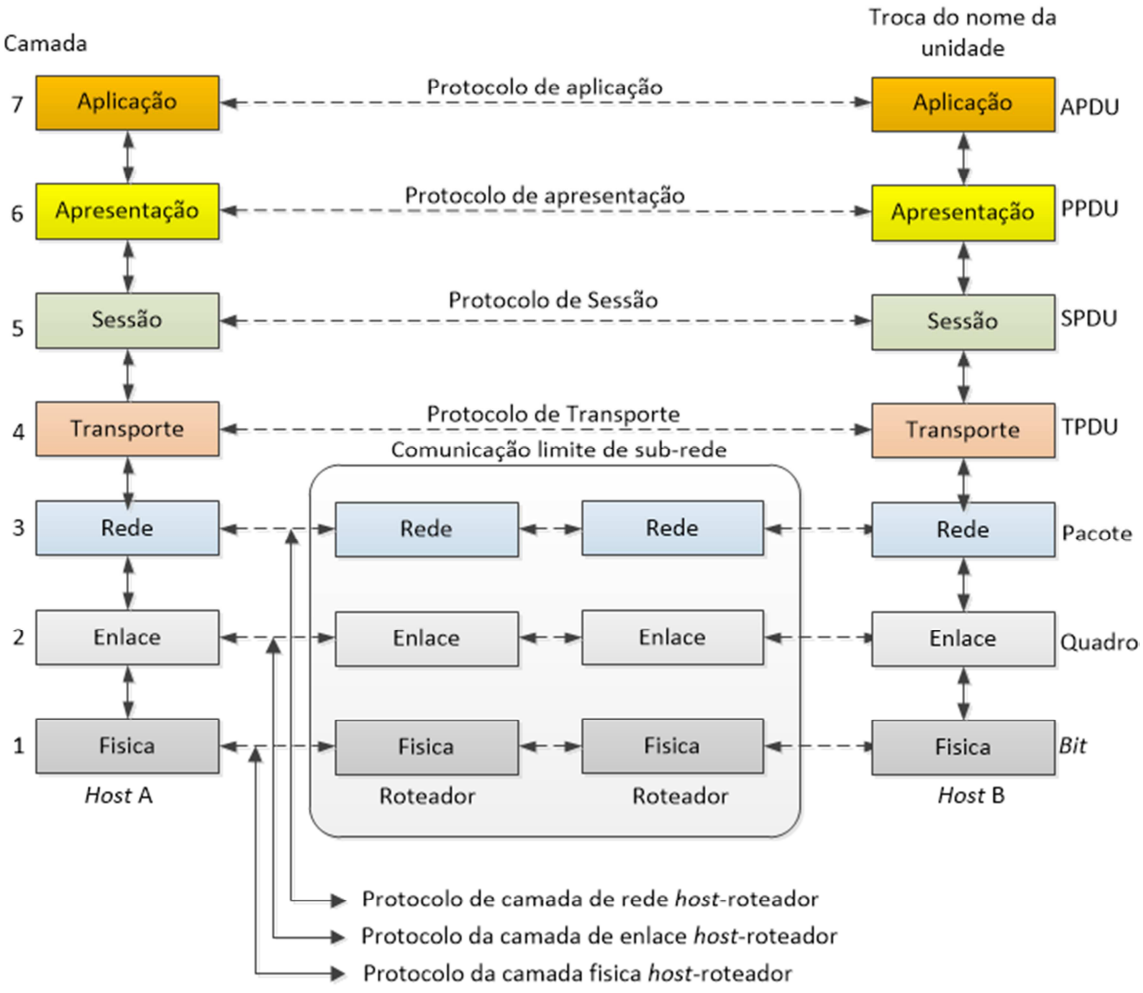

Figura 1 - O funcionamento do modelo de referência OSI.
Fonte: Adaptado de Tanenbaum, 2011.

- A camada física é a camada inferior do modelo OSI que está encarregada da transmissão e recepção dos dados através de um meio físico. Ela basicamente é as interfaces elétricas ou óticas, mecânicas e funcionais que interagem com o meio físico e transporta os sinais para as camadas superiores.
- A camada de enlace proporciona a transferência de quadros de dados de um nó para outro através da camada física.
- A camada de rede é responsável por controlar a operação da sub-rede, decidindo o caminho físico que os dados devem seguir ela é responsável por rotear quadros entre redes, controlar o tráfego da sub-rede, fragmentação de quadros quando necessário, mapear os endereços lógicos para físicos e manter o controle dos quadros encaminhados por sistemas intermediários da sub-rede e é nessa camada que o protocolo IP se encontra.

2.2 PROTOCOLO IPV6

O IPv6 foi concebido para inicialmente trabalhar simultaneamente com o IPv4 em pilha dupla e gradualmente substituir o IPv4, o IPv6 foi apresentado na RFC 1883 de dezembro de 1995 e em dezembro de 1998 e está RFC foi substituída pela RFC 2460 (IPv6.br 2012).

A principal diferença é a quantidade de endereços disponíveis. O IPv4 permite até 4 bilhões de combinações, enquanto o IPv6 disponibiliza 3,4x1038 chegando a trilhões de trilhões endereços.

Destaca-se no protocolo IPv6 a simplificação do formato do cabeçalho, pois foram removidos alguns campos do cabeçalho IPv4 ou tornaram-se opcionais, com a intenção de reduzir o processamento dos pacotes nos roteadores. A escalabilidade do roteamento *multicast* foi melhorada através da adição do campo "escopo" no endereço *multicast* e a adição do campo *anycast*.

As principais diferenças entre o protocolo IPv4 e o protocolo IPv6 podem ser visualizadas na tabela 1.

Tabela 1 - Principais diferenças entre IPv4 e o IPv6

IPv4	IPv6
Endereços de 32 *bits* (4 bytes).	Endereços de 128 *bits* (16 bytes).
Forma de representação Notação decimal pontuada.	Forma de representação Hexadecimal.
Suporte opcional de IPSec.	Suporte ao IPSec, sendo necessária a configuração explicita.
Agrupamento de *Bits* de 8 em 8.	Agrupamento de *Bits* de 16 em 16.
Cabeçalho não possui referência a fluxo de pacotes *Class of Services* - Qualidade de serviço (QoS) para o manuseio de roteadores.	O cabeçalho contém o campo *Flow Label*, que identifica fluxo de pacotes QoS para o manuseio de roteadores.
Ambos os roteadores e o *host* fragmentam os pacotes.	Roteadores não suportam fragmentação dos pacotes Envio de pacotes fragmentados pelo *host*.
Cabeçalho inclui uma verificação de *checksum*.	Cabeçalho não inclui uma verificação de *checksum*.
O cabeçalho inclui os campos de opção.	Campo de opção movido para o campo cabeçalhos de extensão.
O *Address Resolution Protocol* - protocolo de resolução de endereços (ARP), utiliza requisitos do tipo *Broadcast* ARP *request* para resolver endereço IP para endereço de *Media Access Control* (MAC) /*Hardware*.	Solicita o *Multicast Neighbor* para resolver endereços IP para endereços MAC.
Internet Group Management Protocol (IGMP) gerencia relações locais de grupos de sub-redes.	*Multicast Listner Discovery* (MLD) gerencia relações locais de grupos de sub-redes através do campo *Scopo*.
Os Endereços de *Broadcast* são utilizados para enviar tráfego para todos os *hosts* presentes em uma sub-rede.	IPv6 deixa de utilizar o *Broadcast* e passa a usar *multicast* para a rede local.
Endereçamento configurado manualmente ou através de *Dynamic Host Configuration Protocol* (DHCP).	Não requer configuração manual de endereço ou via DHCP com adição de funcionalidades de auto configuração.
Deve suportar um tamanho de pacote de 576 *bytes* (possivelmente fragmentado).	Deve suportar um tamanho de pacote de 1280 *bytes* (sem fragmentação).

Fonte: Autoria Própria, 2014.

2.2.1 Endereçamento IPv6

O endereço do IPv6 é dividido em oito grupos de 16 *bits* sendo separados por ":",cada caractere representa 4 *bits* com um total de 16 combinações e é representados de forma hexadecimal(0-F).

Na representação de um endereço IPv6, é permitido utilizar tanto caracteres maiúsculos quanto minúsculos possuindo regras de abreviação que podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos, e ainda é permitido omitir os zeros a esquerda de cada bloco de 16

bits, além de substituir uma sequência longa de zeros por "::" o endereço 2001:0DB8:AC10:FE01::3EF0 é ilustrado na figura 2.

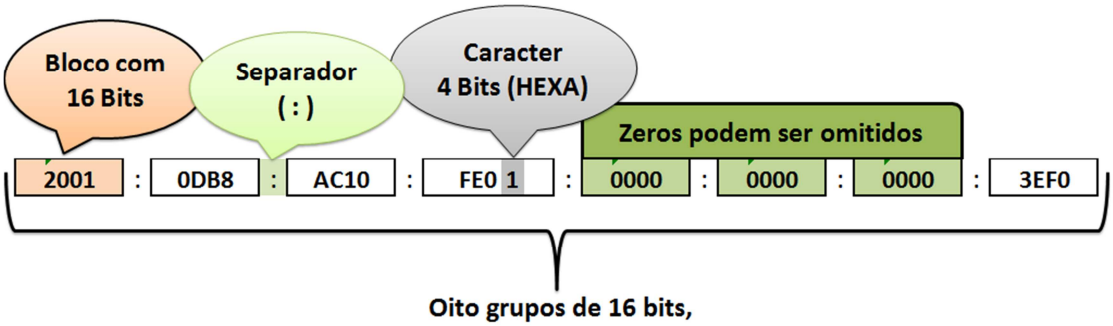

Figura 2 - Representação dos endereços IPv6.
Fonte: Autoria Própria, 2014.

A representação dos prefixos de rede em endereços IPv6 continua sendo escrita do mesmo modo que no IPv4, utilizando a notação *Classless Inter Domain Routing* CIDR, representada da forma "endereço-IPv6/tamanho do prefixo", onde "tamanho do prefixo" é de valor decimal especificando a quantidade de *bits* à esquerda do endereço. O prefixo de sub-rede apresentado a seguir indica que dos 128 *bits* do endereço, 64 *bits* são utilizados na identificação da sub-rede.

- Prefixo 2001:0DB8:AC10:FE01:: /64
- Prefixo global 2001:0DB8::/32
- ID da sub-rede AC10:FE01

Não se costuma informar uma máscara de sub-rede para fazer a operação de *AND* binário como ocorre no IPv4, a notação de *bit count* foi mantida e um provedor de Internet geralmente recebe um bloco /32 para subdividir e entregar aos seus clientes, de um modo geral, é recomendável utilizar uma rede /128 quando houver absoluta certeza que apenas uma interface será conectada, por exemplo uma dial-up via *Point-to-Point Protocol* - Protocolo Ponto a Ponto (PPP), redes /48 são recomendadas para todos os tipos de usuário e redes /64 é recomendada quando se houver certeza que apenas uma sub rede é necessária (IPv6.br, 2011).

2.2.1.1 Tipos de Endereços IPv6

São três tipos de endereços definidos no IPv6, o *unicast*, *anycast* e o *multicast*.

Endereço *unicast* - é usado para identificar uma única interface, o pacote é enviado ao endereço *unicast* e é entregue a uma única interface de

rede, o endereço global *unicast* é roteável e acessível na Internet como um endereço IP valido em IPv6. Ele é constituído por três partes distintas, o prefixo de roteamento global, a identificação da sub-rede e a identificação da interface. Foi projetado para utilizar os 64 *bits* alocados a esquerda para identificar a rede e os 64 *bits* alocados a direita para identificar a interface, exceto em casos específicos, todas as sub-redes baseadas em IPv6 tem o tamanho de prefixo alocado de 64 *bits* representado usualmente como /64.

Endereços *anycast* é a identificação de um grupo de interfaces de rede, um pacote que é enviado ao endereço *anycast* é encaminhado apenas a interface do grupo que mais se aproxima da origem do pacote. Os endereços *anycast* são atribuídos a partir da faixa de endereços *unicast* e não possui diferenças sintáticas entre eles. Este método de endereçamento pode ser utilizado para localizar serviços na rede, por exemplo, o servidor de *Domain Name System* (DNS), o *Proxy, o Hypertext Transfer Protocol* (HTTP).

Endereços *multicast* - é utilizado para identificar grupos de interfaces aonde cada uma das interfaces pode pertencer a mais de um grupo. Os pacotes enviados para esses endereço são entregues a todas as interfaces que compõe o grupo, sendo o seu funcionamento similar ao do *broadcast*, aonde um único pacote é enviado para todos os *hosts* . Os endereços *Multicast* derivam do bloco FF00::/8, onde o prefixo FF é precedido por quatro *bits*, representando quatro *flags*, e ainda um valor de quatro *bits* que define o escopo do grupo *multicast e por ultimo* 112 *bits* para identificar o grupo *multicast.* A tabela 2 demonstra alguns dos endereços *multicast* permanentes.

Tabela 2 - Endereços *multicast* permanentes.

Escopo	Endereço	Descrição
Interface	FF01::1	Todas as interfaces
Interface	FF01::2	Todos os roteadores
Enlace	FF02::1	Todos os nós
Enlace	FF02::2	Todos os roteadores
Enlace	FF02::5	Roteadores OSPF
Enlace	FF02::6	Roteadores OSPF designados
Enlace	FF02::9	Roteadores RIP
Enlace	FF02::D	Roteadores PIM
Enlace	FF02::1:2	Agentes DHCP
Enlace	FF02::1:FFXX:XXXX	*Solicited-node*
Site	FF05::3	Todos os roteadores
Site	FF05::1:3	Servidores DHCP em um site
Site	FF05::1:4	Agentes DHCP em um site
Variado	FF0X::101	*Network Time Protocol* - NTP

Fonte: Adaptado de IPv6.br, 2012).

Entre os tipos de endereçamentos no protocolo IPv6 deixou de existir o endereço de *broadcast*, responsável por direcionar um pacote para todos os nós de um mesma sub-rede, sendo que essa função foi atribuída ao *multicast*.

2.2.2 Campos do Cabeçalho IPv6

Algumas modificações foram realizadas no formato do cabeçalho. O número de campos foi reduzido para oito e o tamanho foi fixado de 40 Bytes, mais flexível e eficiente sendo adicionado os cabeçalhos de extensão que não precisam ser processados por roteadores intermediários, a divisão dos campos do cabeçalho IPv6 pode ser vista na figura 3.

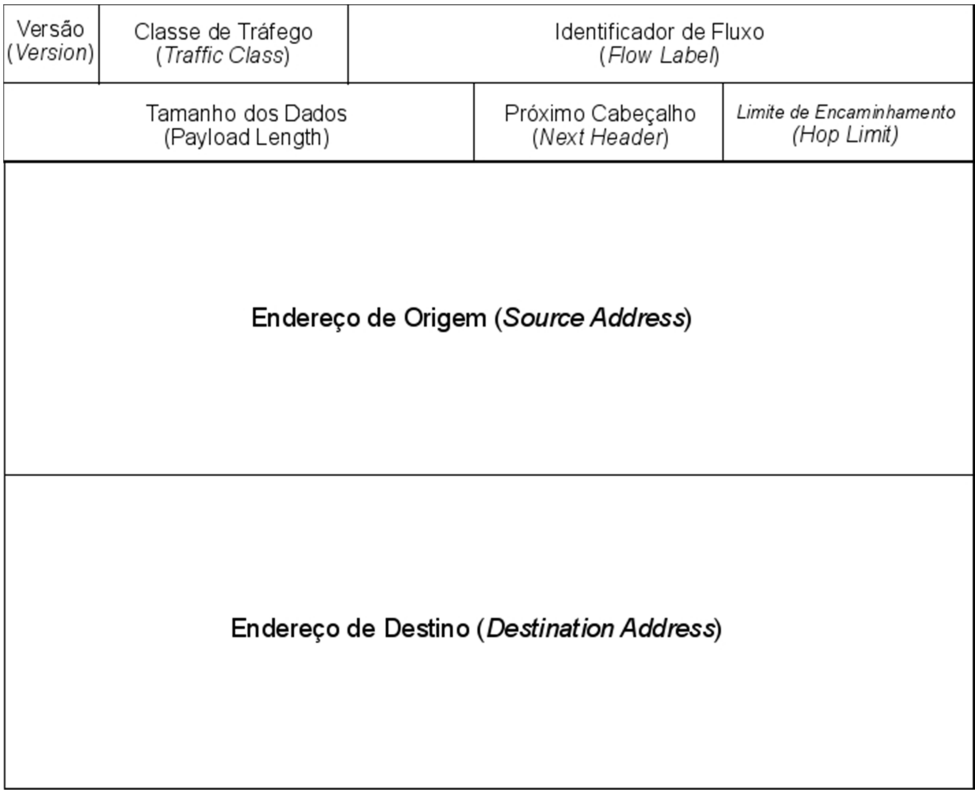

Figura 3 - Cabeçalho IPv6.
Fonte: IPv6.br, 2012.

- Versão - Campo com 4 *bits* identificando a versão do protocolo utilizado. Sendo o 6 alocado como valor nesse campo na versão IPv6.
- Classe de Tráfego - Campo com 8 *bits* identificando os pacotes por prioridade ou classes de serviços. Com as funções e definições idênticas do campo “Tipo de Serviço do IPv4”.

- Identificador de Fluxo - Campo contendo 20 *bits,* responsável pela identificação dos pacotes do fluxo de comunicação de rede, sendo configurado pelo endereço de destino para separar os fluxos das aplicações e os nós intermediários de rede, para poder utilizá-lo de forma agregada, com endereços de origem e destino para o tratamento dos pacotes.
- Tamanho de Dados - Campo com 16 *bits* indicando o tamanho dos dados enviados junto ao cabeçalho IPv6 em *Bytes*, o tamanho dos cabeçalhos de extensão também são somados nesse campo. Substituiu o campo Tamanho Total do IPv4.
- Próximo Cabeçalho - Campo com 8 *bits* identificando o cabeçalho de extensão. No IPv4 chamava-se Protocolo e deixou de conter os valores referentes a outros protocolos.
- Limite de Encaminhamento - Campo com 8 *bits* aonde é decrementado em cada salto do roteamento, indicando o número máximo de roteadores que o pacote pode passar antes de ser descartado. Ele padronizou o modo como o campo Time to live - Tempo de Vida (TTL).
- Endereço de origem - Campo com 128 *bits* indicando o endereço de origem do pacote.
- Endereço de Destino - Campo contendo 128 *bits* indicando o endereço de destino do pacote.

A figura 4 ilustra um comparativo entre os cabeçalhos do protocolo IPv4 e IPv6.

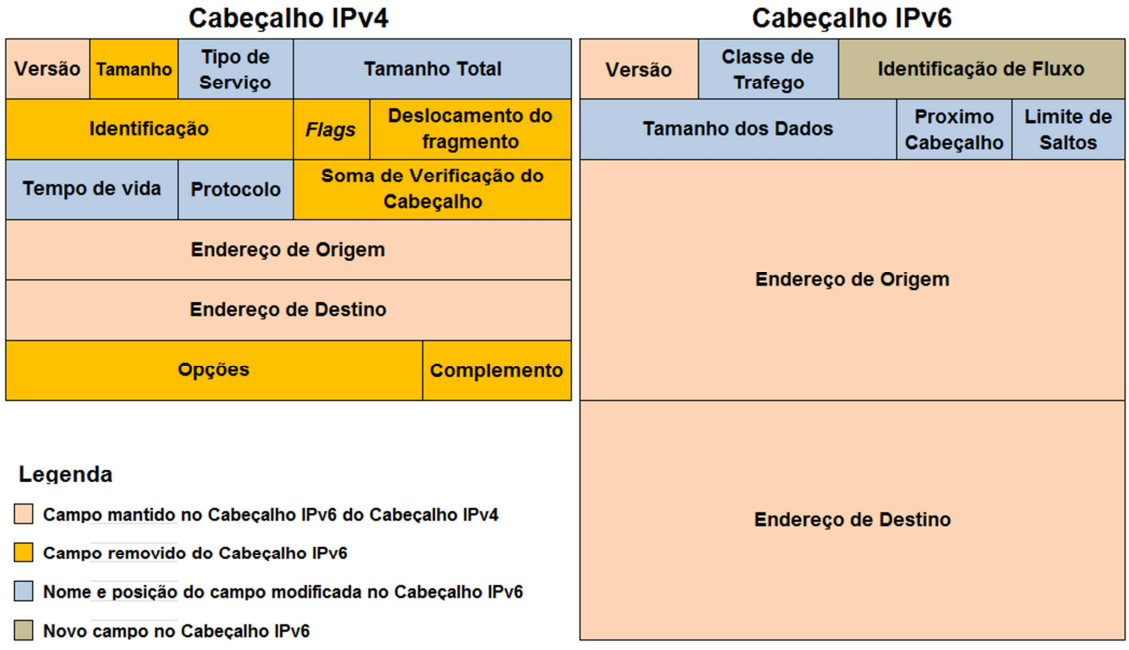

Figura 4 - Cabeçalho IPv4 e o IPv6.
Fonte: Adaptado de Cisco, 2006.

2.2.2.1 Cabeçalhos de Extensão IPv6

No IPv6 comumente são utilizados seis cabeçalhos de extensão, o *Hop-by-Hop Options*, *Destination Options*, *Routing, Fragmentation*, *Authentication Header* (AH) e *Encapsulating Security Payload* (ESP).

O IPv6 utiliza essas informações por meio dos cabeçalhos de extensão, diferente do IPv4, localizando-se entre o cabeçalho base e o cabeçalho da camada imediatamente acima não possuindo quantidade ou tamanho fixo. Caso o mesmo pacote possua múltiplos cabeçalhos de extensão, será adicionado a eles uma lista de prioridade, adicionados em série, formando uma cadeia de cabeçalhos exemplificada na figura 5.

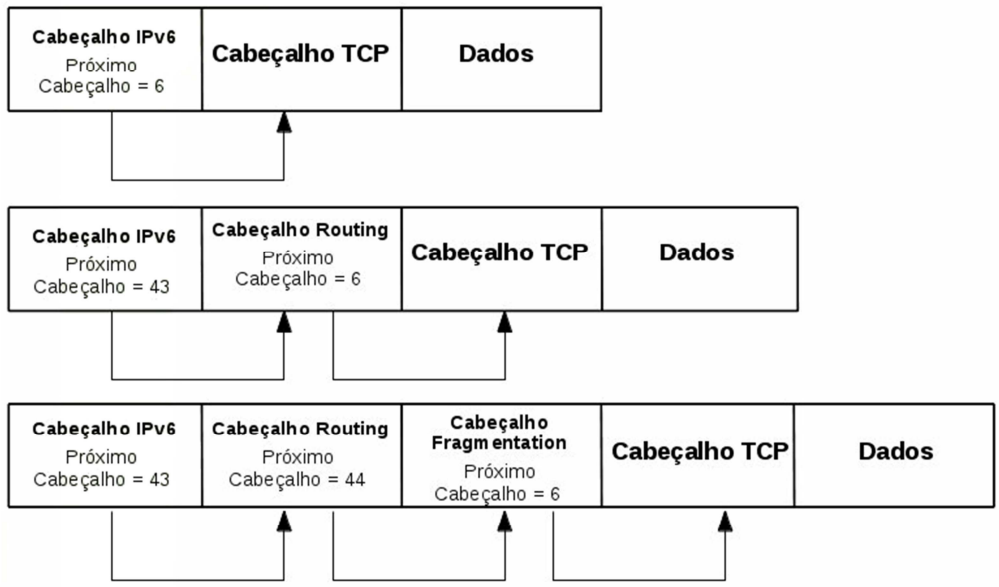

Figura 5 - Cadeia de cabeçalhos.
Fonte: IPv6.br, 2012.

2.2.2.2 Aspectos dos Cabeçalhos de Extensão

Inicialmente, estes cabeçalhos necessitam ser enviados em uma determinada ordem com a intenção de evitar que nós intermediários tenham a necessidade de processar por completo a cadeia de cabeçalhos para decidir quais deverão ser tratados, desta forma os cabeçalhos importantes para os nós envolvidos no roteamento devem ser colocados antes daqueles que são relevantes somente para o destinatário final. A vantagem, é que um nó pode parar de analisar cabeçalhos assim que encontrar algum dedicado ao destino, a sequência a ser seguida é apresentada na tabela 3.

Tabela 3 - IPv6 sequencia dos cabeçalhos de extensão.

Ordem	Tipo de Cabeçalho	Próximo Cabeçalho
1	*Basic IPv6 Header*	-
2	*Hop-by-Hop Options*	0
3	*Destination Options*	60
4	*Routing Header*	43
5	*Fragment Header*	44
6	*Authentication Header*	51
7	*Encapsulation Security Payload Header*	50
8	*Destination Options*	60
9	*Mobility Header*	135
	No next Header	59
Camada superior	TCP	6
Camada superior	UDP	17
Camada superior	ICMPv6	58

Fonte: Adaptado de Cisco, 2006.

Observando que, se um pacote for enviado para um endereço *multicast*, os cabeçalhos de extensão serão examinados por todos os nós do grupo (ipv6.br, 2012).

2.3 IPSEC

O *IP Security* - Segurança IP (IPSec), projetado para ser usado opcionalmente em conjunto com o IPv4 para fornecer segurança para a transmissão de informações confidenciais através de redes desprotegidas como a Internet, passou a ser um componente obrigatório para IPv6. O IPSec age na camada de rede, fornecendo proteção e autenticação de pacotes IP entre dispositivos IPSec. Para se utilizar o IPSec é necessário configurá-lo. Isso foi necessário para que dispositivos com processamento e memórias limitados possam utilizar IPv6 sem fugir a especificação do protocolo. O IPSec oferece os seguintes serviços opcionais de segurança de rede:

- Confidencialidade de dados - O remetente IPSec pode criptografar os pacotes antes de enviá-los através de uma rede.
- A integridade dos dados - O receptor IPSec pode autenticar os pacotes enviados pelo remetente IPSec para assegurar que os dados não foram alterados durante a transmissão.
- Autenticação da origem dos dados - O receptor IPSec pode autenticar a origem dos pacotes IPSec enviados. Este serviço depende do serviço de integridade de dados.

- Proteção *Antireplay* - O receptor IPSec pode detectar e rejeitar pacotes repetidos.

Quando IPSec é implementado e implantado de forma correta, não afeta usuários, *hosts* e outros componentes da Internet que não empregam o IPSec para proteção de tráfego e em geral, a política de segurança é que determina a utilização de um ou mais destes serviços. Estes serviços são fornecidos na camada de rede do modelo OSI oferecendo proteção numa forma padrão para todos os protocolos que podem ser realizadas sobre IP, incluindo o IP em si, o IPSec é apenas uma parte de uma arquitetura de segurança geral do sistema (RFC 4301).

As principais tecnologias que compõem a IPSec são:

- *Authentication Header* - AH.
- *Encapsulating Security Payload* - ESP.
- *Digital Encryption Standard* - DES.
- *Triple Digital Encryption Standard* - 3DES.
- *Advanced Encryption Standard* (AES).
- *Internet Key Exchange* - IKE.
- Acordos de chave *Diffie-Hellman.*
- Códigos de autenticação de mensagens com *hash.*
- Segurança RSA.
- Autoridade de certificação.

2.3.1 Criptografia

Para criptografia poder trabalhar, tanto o emissor e o receptor precisa saber as regras que foram usadas para criptografar a mensagem original a dois tipos de criptografia.

- Simétrica - cada ponto usa a mesma chave para criptografar e remover a criptografia dos dados.
- Assimétrico - cada ponto utiliza uma chave diferente para criptografar e remover a criptografia da mensagem.

A troca de chaves permite uma forma para os usuários estabelecerem uma chave secreta compartilhada, que só eles sabem, embora esteja sendo enviada através de um canal inseguro. Tanto o Data Encryption Standard (DES) e Triple DES (3DES) exigem uma chave secreta simétrica compartilhada . O método mais fácil de trocar as chaves públicas é *Diffie-Hellman* (Ciscosecurity, 2014).

2.3.1.1 *Data Encryption Standard* (DES)

Data Encryption Standard (DES) - padrão de criptografia de dados, é considerado o menos seguro de todos, é um algoritmo matemático de chave simétrica, aonde o texto simples é criptografado em blocos de 64 *bits*, produzindo 64 *bits* de texto cifrado, usando como parâmetro uma chave de 56 *bits*, possui 19 estágios, aonde o primeiro deles é uma transposição de forma independente da chave no texto simples que possui 64 *bits* e no ultimo exatamente o inverso. No penúltimo estágio troca os 32 *bits* mais à esquerda pelos 32 *bits* mais à direita. Os 16 estados restantes é parametrizado por diferentes funções da chave, mais são funcionalmente idênticos, Na decodificação as etapas são simplesmente executadas na ordem inversa. Foi amplamente adotada para uso em produtos de segurança em informática. Ela já não é mais segura em sua forma original, porem. em uma forma modificada ela ainda pode ser utilizada (Tanenbaum, 2011).

2.3.1.2 *Triple Data Encryption Standard* (3-DES)

O *Triple Data Encryption Standard* (3-DES) - pode utilizar de duas a três chaves de 64 *bits*, totalizando 192 *bits* embora como no DES, só são utilizados 56 *bits* por chave. Na forma de operação com duas chaves, ele é dividido em três estágios. No primeiro estágio, o texto simples é criptografado com a primeira chave da maneira usual do DES. No segundo estágio, o DES é executado no modo de descriptografia, com o uso da segunda chave e, por fim, outra criptografia é feita com a primeira chave (Tanenbaum, 2011).

2.3.1.3 *Advanced Encryption Standard* (AES)

O Advanced Encryption Standard (AES) é baseado na cifra Rijndael, é considerado o mais seguro. O AES admite tamanhos de blocos e tamanhos de chaves variados desde 128 *bits* até 256 *bits* em intervalos de 32 *bits*. O comprimento da chave e o do bloco pode ser escolhido independentemente. O AES especifica que o tamanho do bloco deve ser 128 *bits* e o comprimento da chave deve ser 128, 192 ou 256 *bits*. Usualmente o AES utiliza duas variantes: um bloco de 128 *bits* com uma chave de 128 *bits* e um bloco de 128 *bits* com uma chave de 256 *bits* (Tanenbaum, 2011).

2.3.1.4 Message Digest 5 (MD5)

O *Message Digest 5* (MD5) é a quinta versão de uma série de sumários de mensagens criadas por Ronald Rivest. A função começa gerando um exponencial o tamanho da mensagem até chegar a 448 *bits* e em seguida, o tamanho original é anexado como um inteiro de 64 *bits*, a fim de gerar uma entrada total cujo tamanho seja um múltiplo de 512 *bits* e na ultima etapa os é iniciado um buffer de 128 *bits* com um valor fixo (Tanenbaum, 2011).

2.3.1.5 *Secure Hash Algorithm*-1 (SHA-1)

A exemplo do MD5, esse algoritmo processa os dados de entrada em blocos de 512 *bits*, e ao contrário do MD5, ele gera um sumário de 160 *bits*. Inicia preenchendo a mensagem com a adição de um bit 1 ao final, seguido pelo número de *bits* 0 necessários para tornar o tamanho um múltiplo de 512 *bits*. Em seguida, um número de 64 *bits* contendo o tamanho da mensagem antes do preenchimento é submetido a uma operação OR nos 64 *bits* de baixa ordem. O SHA-1 sempre preenche o fim da mensagem, o SHA-1 mantém cinco variáveis de 32 *bits*, de H0 a H4, onde o *hash* se acumula, Elas são inicializadas como constantes especificadas no padrão, cada um dos blocos é processado. Após os blocos da mensagem de 512 *bits* serem processados. Quando o último bloco é concluído, as cinco palavras de 32 *bits* armazenadas no array são transmitidas como saída, formando o *hash* criptográfico de 160 *bits*, o código C completo para SHA-1 é encontrado na RFC 3174 (Tanenbaum, 2011).

2.3.1.6 *Diffie-Hellman*

O algoritmo de chave pública *Diffie-Hellman* trocam as chaves públicas entre o usuário A e o usuário B e combiná-los com suas chaves privadas, o resultado final deve ser o mesmo. como ilustra a figura 6. É muito simplificada para assegurar que o conceito de troca clara de chaves existe diferentes variações para este algoritmo, conhecido como grupos DH de 1 a 7. Durante a configuração do túnel, os pares VPN irão negociar que DH o grupo ira utilizar (Ciscosecurity, 2014).

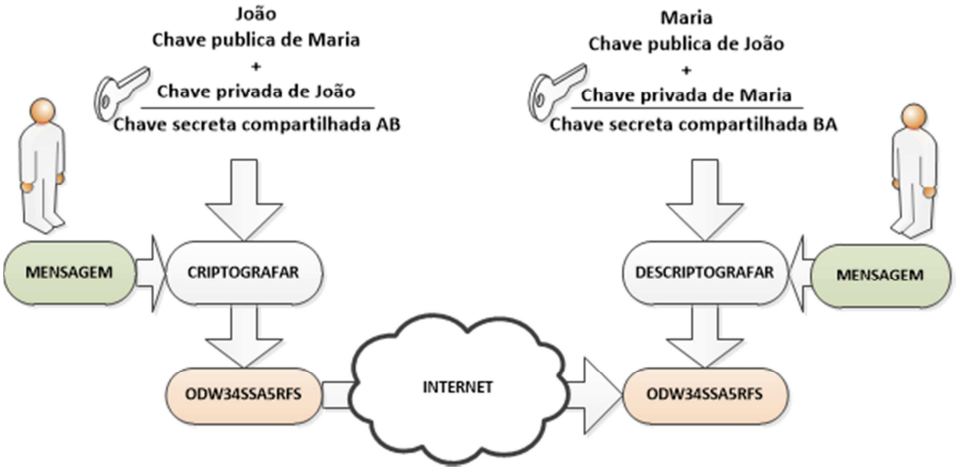

Figura 6 - Funcionamento do *Diffie-Hellman*.
Fonte: Adaptado de Ciscosecurity, 2014.

2.3.2 Integridade dos Dados

A integridade dos dados é também uma função crítica de VPN, porque os dados são enviados através de uma rede pública e podem ser interceptados e modificados. Para se proteger contra essa interceptação, cada mensagem tem um *hash* anexado. Isso garante a integridade da mensagem. O receptor verifica isso comparando o *hash* recebido com o *hash* calculado a partir da própria mensagem. Se ambos os valores forem iguais, a mensagem não foi alterada. E se não houver uma correspondência, o receptor sabe que a mensagem foi alterada.

IPSec utiliza o protocolo *Hashed Message Authentication Codes* (HMAC) para calcular o *hash*. A mensagem e a chave compartilhada são enviados através de um algoritmo *hash* que produz um valor *hash*. É importante entender que esta é uma função de sentido único. Uma mensagem pode produzir um *hash*, mas um *hash* não pode produzir a mensagem original. Após o *hash* ser calculado, ele é enviado através da rede, juntamente com a mensagem. Na outra extremidade, o receptor realiza a mesma ação. Ele envia a mensagem e a chave compartilhada através do algoritmo de *hash* e compara os dois *hashes* para verificar se elas correspondem (Wenstrom, 2002).

Dois algoritmos HMAC são comumente usados:

- HMAC-MD5 Este protocolo utiliza uma chave compartilhada de 128 *bits*. A chave e a mensagem são combinadas para um *hash* de 128 *bits*.
- HMAC-SHA-1 Este protocolo utiliza uma chave compartilhada de 160 *bits*. O comprimento do *hash* é 160 *bits*. Este protocolo é considerado mais forte devido ao comprimento da chave ser mais longo (RFC 3174, 2001).

2.3.2.1 Autenticação de Origem

O documento é assinado com a chave de criptografia privada do remetente. Isto é também chamado de uma assinatura digital. Esta assinatura pode ser autenticada removendo a criptografia da chave pública do remetente, na VPN, os dispositivos na outra extremidade do túnel, devem ser autenticados antes do caminho ser considerado seguro. Existem três métodos de autenticação de pares:

- Chaves pré-compartilhadas - A chave secreta é inserida em cada *peer* manualmente.
- As assinaturas RSA - Troca os certificados digitais e autentica os pares.
- A criptografia RSA - Gera um numero aleatório são criptografados e trocados entre pares. Os dois valores aleatórios são utilizados durante o processo de autenticação pelos pares.

2.3.2.2 Chave Pré Compartilhada

Se forem usadas chaves pré-compartilhadas, a mesma chave é configurada nos pares IPSec. Em cada extremidade, as chaves pré compartilhadas são combinadas com as informações específicas do dispositivo, para formar a chave de autenticação. Ambas são enviadas através de um algoritmo de *hash* para formar um *hash* e, em seguida, o *hash* é enviado para outro local, ilustrada na figura 7.

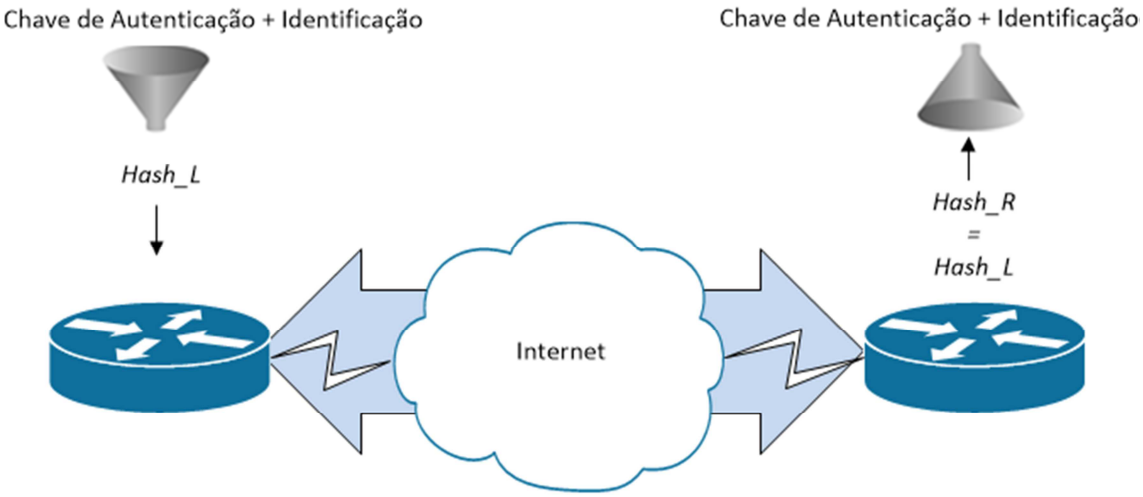

Figura 7 - Funcionamento da chave pré compartilhada.
Fonte: Adaptado de Wenstrom, 2002.

Se o ponto remoto é capaz de criar de forma independente o mesmo *hash*, o mesmo nível local é autenticado. Depois disso, o processo de autenticação continua na direção oposta. O ponto remoto combina a sua informação específica com a chave pré-compartilhada e envia o *hash* resultante para o ponto local. Se este ponto pode criar o mesmo *hash* de sua informação armazenada e a chave pré-compartilhada, o ponto remoto é autenticado. Cada ponto deve autenticar seu par oposto antes do túnel e é considerado seguro. Cada ponto IPSec deve ser configurado com a chave pré-compartilhada de todos os outros colegas com os quais quer se comunicar.

2.3.3 *Frameworks* de Segurança

No IPv6, o IPSec é implementado utilizando o cabeçalho de autenticação (AH) e o cabeçalho de extensão (ESP) e pode ser utilizado de duas forma, em Modo Túnel ou Modo Transporte.

2.3.3.1 *Authentication Header* (AH)

Os cabeçalhos de extensão AH, representado pelo valor 51 no campo próximo cabeçalho, definido na RFC2402, fazem parte do cabeçalho IPSec e é ilustrado na figura 8.

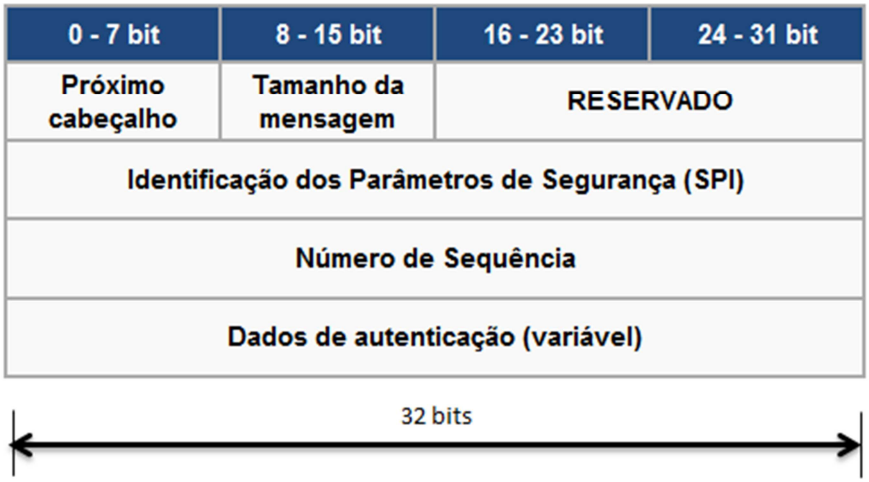

Figura 8 - Cabeçalho AH.
Fonte: Autoria própria, 2014.

O AH é o protocolo a ser usado quando não se exige confidencialidade, fornecendo integridade e autenticação da fonte e protegendo a maior parte dos campos do cabeçalho IP, autenticando a fonte por meio de um algoritmo baseado em assinatura e também oferecendo proteção opcional contra pacotes repetidos.

A autenticação é obtida pela aplicação de uma função *hash* unidirecional ao pacote para criar uma síntese de mensagem, qualquer alteração em qualquer parte do pacote é detectada pelo receptor, a função *hash* esta ilustrada na figura 9 e são definidas nas seguintes etapas:

Passo 1 - O cabeçalho IP e carga de dados sofrem *hash*.

Passo 2 - O *hash* é usado para construir o cabeçalho AH, que é inserido no pacote original, entre o novo cabeçalho AH e a carga de dados.

Passo 3 - O pacote modificado é enviado para o par IPSec.

Passo 4 - O par IPSec faz o *hash* do cabeçalho IP e dos dados.

Passo 5 - O roteador extrai o *hash* transmitido a partir do cabeçalho AH.

Passo 6 - O par IPSec compara os dois *hash*es. Os *hash*es tem que ser idênticos, para provar que o pacote não foi modificado durante o transporte.

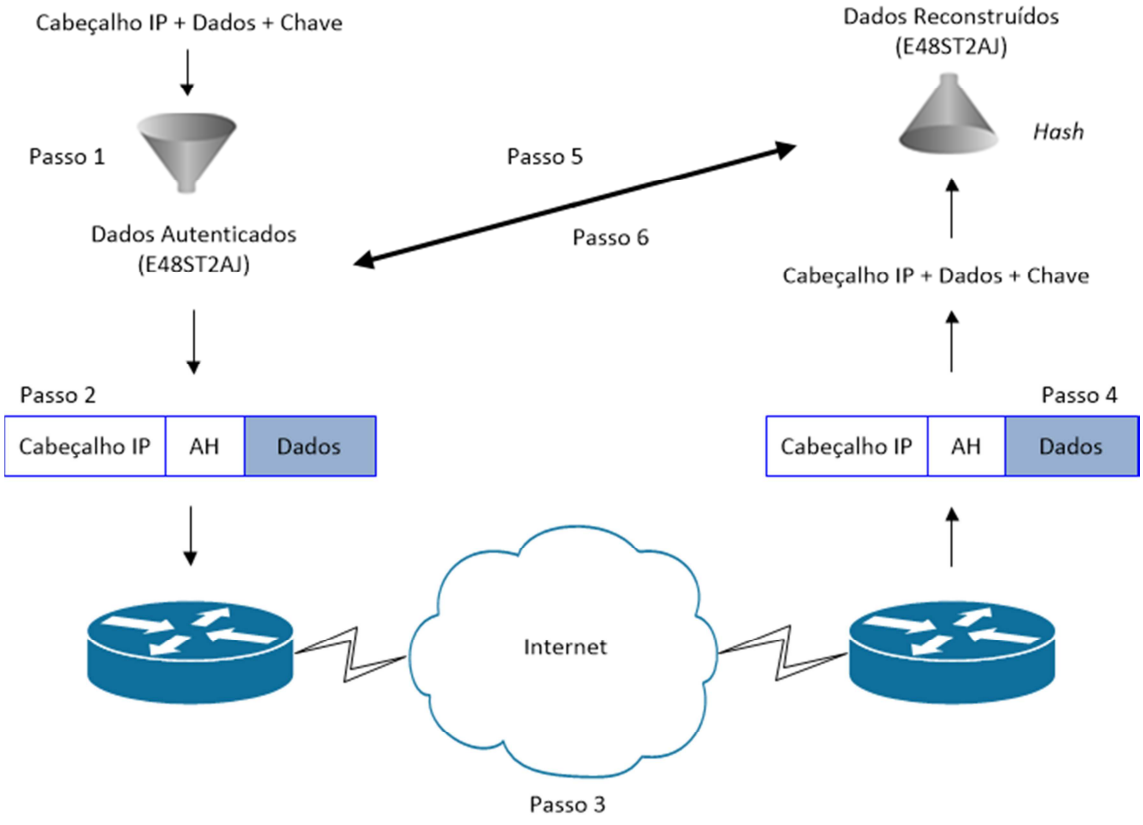

Figura 9 - Funcionamento do cabeçalho AH.
Fonte: Adaptado de Ciscosecurity, 2014.

2.3.3.2 *Encapsulating Security Payload* (ESP)

O cabeçalho ESP, definido na RFC2406, com o valor 50 no campo próximo cabeçalho fornece confidencialidade, autenticação da origem, a integridade, evita a reprodução, e gera a confidencialidade do fluxo de tráfego.

O ESP pode ser utilizado para fornecer criptografia e autenticação. Fornece confidencialidade, criptografando a carga útil através da realização de criptografia na camada 3 do modelo OSI. O ESP fornece autenticação para a carga do pacote IP e o cabeçalho ESP. Da mesma forma como acontece com o cabeçalho AH, o cabeçalho ESP verifica o seguinte: que pacote foi originado e a partir de onde ele declara que o fez se é o que declara que é, e que o pacote não foi modificado durante o transporte, a figura 10 ilustra o cabeçalho ESP.

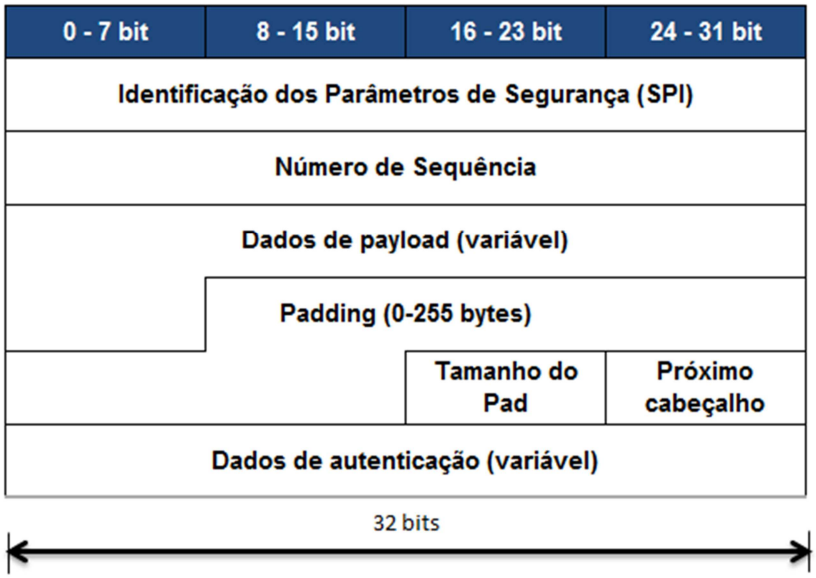

Figura 10 - Cabeçalho ESP.
Fonte: Autoria própria, 2014.

Ele suporta vários algoritmos de criptografia simétrica. O padrão para IPSec é DES de 56 *bits*, mas os produtos da Cisco também suportam 3DES e AES. A confidencialidade pode ser selecionada independentemente de todos os outros serviços. O ESP pode ser usado sozinho ou em combinação com AH. Entre os *gateways* de segurança, os dados originais são protegidos porque todo o pacote IP é criptografado. Um cabeçalho de ESP e a carga de dados são acrescentados a criptografia, como ilustra a figura 11.

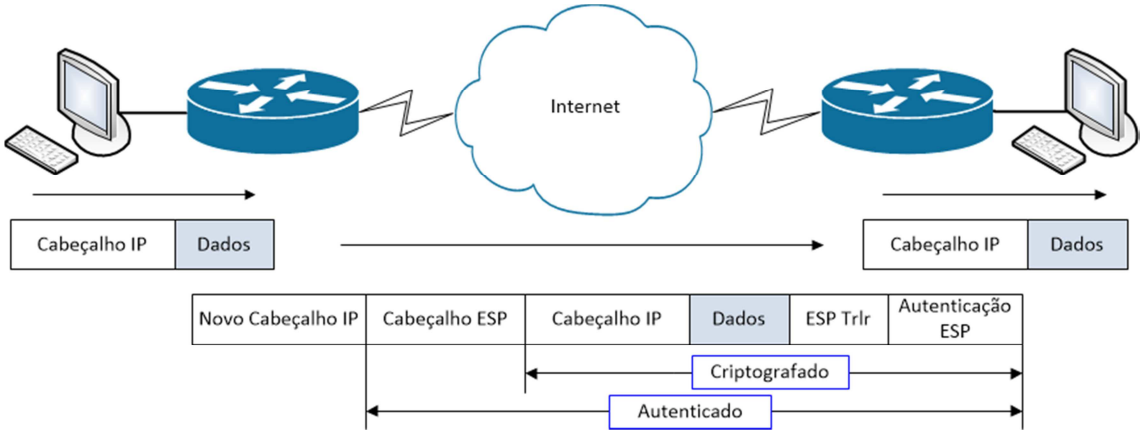

Figura 11 - Cabeçalho ESP e a carga de dados.
Fonte: Adaptado de Cisco, 2012.

2.3.3.3 O modo de transporte AH e ESP

Este modo é usado principalmente para conexões fim-a-fim entre *hosts* ou dispositivos que atuam como hospedeiros. O modo de transporte protege a carga útil do pacote, mas deixa o endereço IP original intacto e legível. Este endereço é usado para rotear um pacote através da Internet. O modo de transporte fornece segurança apenas para os protocolos das camadas superiores.

No modo transporte com AH, o cabeçalho AH IPSec é adicionado entre a camada 3 e a camada 4 do cabeçalho, este modo tem a vantagem de adicionar somente alguns *bytes* a cada pacote. A figura 12 ilustra o modo de transporte com cabeçalho AH do IPSec.

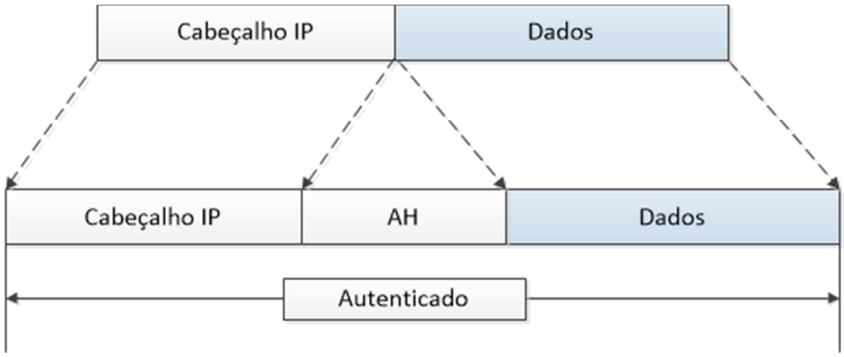

Figura 12 - Modo de transporte com cabeçalho AH.
Fonte: Adaptado de Ciscosecurity, 2014.

No modo transporte com ESP o cabeçalho IP é deslocado para a esquerda, e é inserido o cabeçalho ESP. O ESP e a autenticação ESP são então anexados ao fim do pacote. Na figura 13 ilustra o modo de transporte ESP.

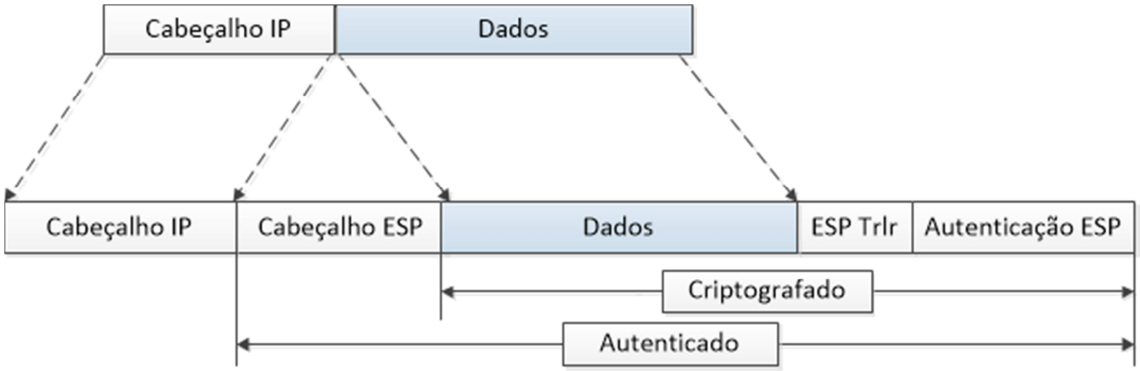

Figura 13 - Modo de transporte com cabeçalho ESP.
Fonte: Adaptado de Ciscosecurity, 2014.

2.3.3.4 Modo Túnel AH e ESP

O modo de túnel IPSec é usado entre *gateways* ou concentradores de VPN. O modo de túnel é utilizado quando o destino final não é um *host*, mas um *gateway* VPN. Neste modo, em vez de deslocar o cabeçalho IP original para a esquerda e inserir o cabeçalho IPSec, o cabeçalho original é copiado e deslocado para a esquerda, para formar um novo cabeçalho de IP. O cabeçalho IPSec então é colocado entre o novo cabeçalho e os cabeçalhos IP originais. O datagrama original é deixado intacto. A figura 14 ilustra o modo de túnel com AH.

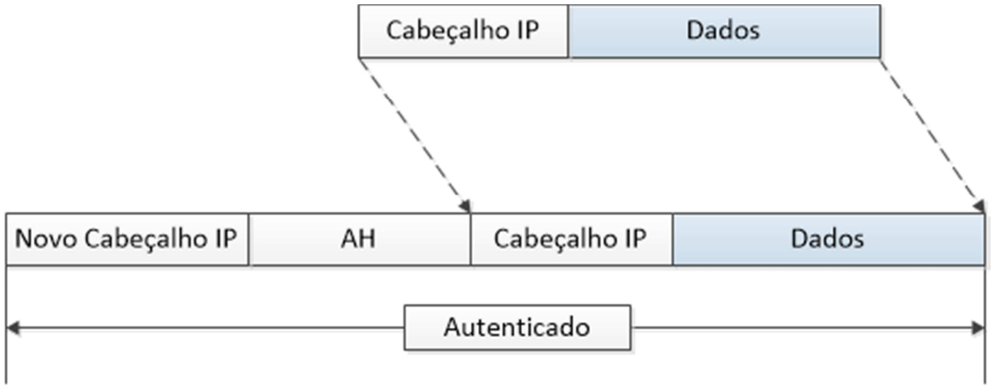

Figura 14 - Modo de Túnel com cabeçalho AH.
Fonte: Adaptado de Ciscosecurity, 2014.

No modo túnel com ESP Todo o datagrama original podem ser criptografados e autenticados. Quando ambos são necessários a criptografia tem de ser efetuada em primeiro lugar. Isso permite que a autenticação seja feita com a garantia de que o remetente não alterou o datagrama antes da transmissão, e o receptor pode autenticar o datagrama antes de remover a criptografia do pacote. A figura 15 ilustra o modo túnel com ESP.

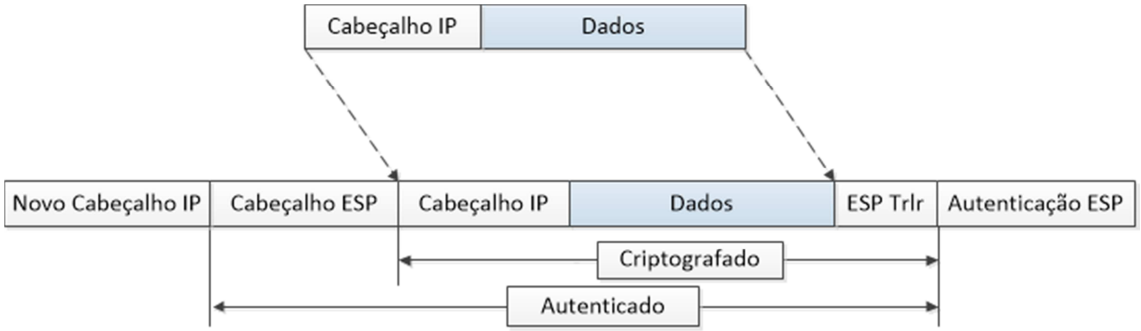

Figura 15 - Modo Túnel com cabeçalho ESP.
Fonte: Adaptado de Ciscosecurity, 2014.

2.3.4 *Security Association* (SA)

Uma *Security Association* - associação de segurança (SA) é uma política negociada ou um meio estabelecido de tratamento dos dados que serão trocados entre o transmissor e o receptor. Ambos usam o mesmo algoritmo para criptografia e descriptografia. Os parâmetros da SA ativos são armazenados em um *Security Association Database* (SAD-SA) - banco de dados SA nos pares.

A tabela 4 apresenta as combinações IPSec permitidas.

Tabela 4 - Combinações de transformação IPSec permitidas.

Tipo	Transformação	Descrição
Transformação AH	ah-md5-hmac	AH com autenticação MD5 (Variante do HMAC)
Transformação AH	ah-sha-hmac	AH com autenticação SHA (variante do HMAC)
Criptografia ESP	esp-des	ESP com criptografia 56-bit DES
Criptografia ESP	esp-3des	ESP com criptografia DES 168 *bit* (3DES)
Criptografia ESP	esp-null	Algoritmo de criptografia nulo
Autenticação ESP	esp-md5-hmac	ESP com autenticação MD5 (Variante do HMAC)
Autenticação ESP	esp-sha-hmac	ESP com autenticação SHA (Variante do HMAC)
Compressão IP	comp-lzs	Compressão IP com o algoritmo LZS.

Fonte: Adaptado de cisco, 2014).

A SA é unilateral, se o transmissor precisa se comunicar com o receptor é requerida duas SA's. Uma para envio e outra para recebimento, definindo o cabeçalho a ser utilizado, se será AH ou ESP, definindo os algoritmos de autenticação, e ou criptográficos, se será modo túnel ou transporte e o tempo de duração.

2.3.5 *Internet key Exchange* (IKE)

O *Internet Key Exchange* (IKE) é um protocolo híbrido e é o protocolo de gerenciamento de chave que é usado em conjunto com IPSec, baseado em partes do sistema de troca de chaves de três protocolos, o Oakley *Key Determination Protocol* - OAKLEY, o *Secure Key Exchange Mechanism* - SKEME e *Internet Security Association Key Management Protocol* (ISAKMP).

O IPSec pode ser configurado sem o IKE, mas o IKE aumenta a segurança do IPSec, fornecendo recursos adicionais para o padrão IPSec.

O IKE utiliza somente um subconjunto necessário dos protocolos OAKLEY, SKEME e ISAKPM para satisfazer seus objetivos. Ele não tem a pretensão de conformidade com todo o protocolo OAKLEY, e nem é dependente de qualquer forma do protocolo OAKLEY, do protocolo SKEME utiliza somente o método de criptografia de chave pública para a autenticação e o seu conceito de rápida re-digitação usando uma troca de valores aleatórios, não sendo dependente de qualquer forma com o mesmo e ambos trabalhando em conjunto com o ISAKPM (RFC 2409).

No IKEv1, é claramente demarcada a troca na Fase 1, que possui seis pacotes seguidos por uma troca de IKE fase 2 que é composta por três pacotes.

IKEv2 é a segunda e mais recente versão do protocolo IKE. A adoção para este protocolo começou em 2006. A necessidade e a intenção de uma revisão do protocolo IKE foi descrito no Apêndice A do Internet Key Exchange (IKEv2) Protocolo na RFC 4306

A troca IKEv2 é variável. Na melhor das hipóteses, pode trocar somente quatro pacotes. No pior dos casos, isto pode aumentar para um máximo de 30 pacotes ou mais, dependendo da complexidade da autenticação, o número de atributos utilizados no *Extensible Authentication Protocol* (EAP), ou como o número de SA's formadas. IKEv2 combina a informação de Fase 2 em IKEv1 para a troca IKE_AUTH, e isso garante que, após a troca do IKE_AUTH estiver concluída, ambos os pares já tem uma SA construída e preparada para criptografar o tráfego. Esta SA só é construída para as identidades de *proxy* que correspondem o pacote de acionamento. Qualquer tráfego posterior que coincida com outras identidades de *proxy* aciona a troca CREATE_CHILD_SA, que é o equivalente a troca de Fase 2 no IKEv1. No IKEv2 não há modo agressivo ou o modo principal (Cisco, 2013).

2.3.6 *Pre-Shared Keys* (PSK)

PSKs é uma sequencia de chave criptográfica pré-definida em cada par utilizado para identificar um ao outro. Usando o PSK, os dois pares de criptografia são capazes de negociar e estabelecer uma ISAKMP SA. A PSK geralmente contém um endereço IP de host ou sub-rede e a máscara, que é considerado válido particularmente para aquela PSK. A *wildcard PSK* é um tipo especial de PSK, cuja rede e a máscara pode ser qualquer endereço IP (Cisco, 2014).

2.4 FUNCIONAMENTO DA IPSEC

Os protocolos de segurança do IPSec, o cabeçalho ESP, o cabeçalho AH e o IKE, que são concebidos para serem algoritmos criptográficos independentes, sua operação pode ser dividida em cinco etapas principais ilustrada na figura 16.

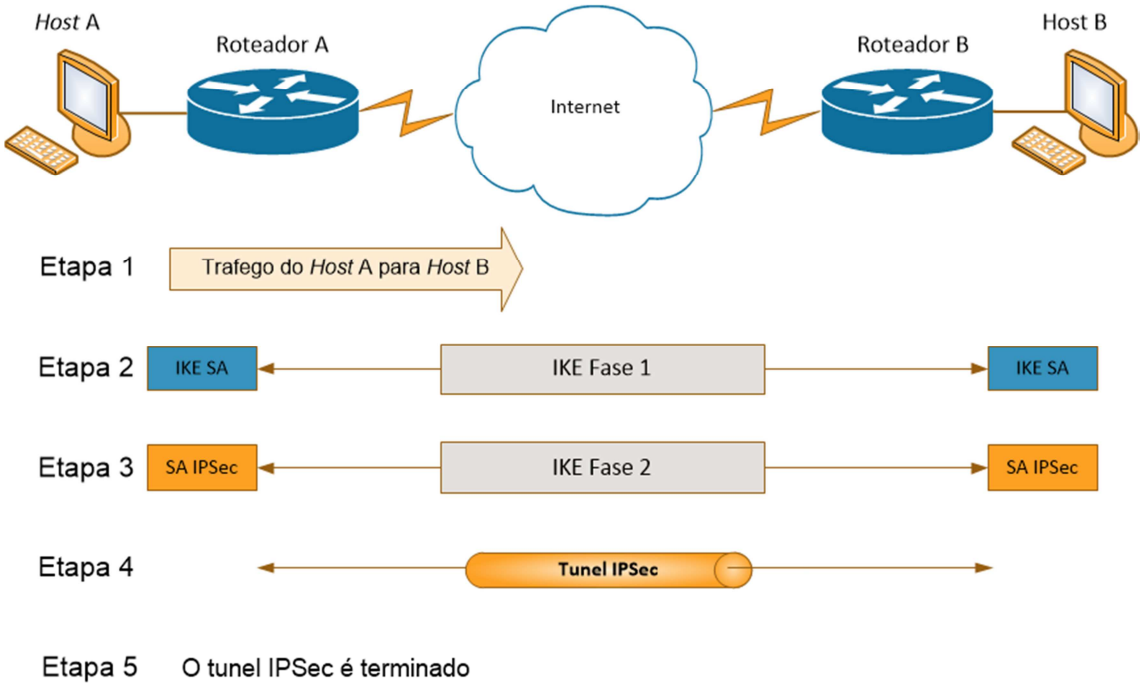

Figura 16 - Modo Túnel com cabeçalho ESP.
Fonte: Adaptado de Wenstrom, 2002.

Etapa 1 - Inicia o processo do IPSec, após você determinar qual tipo de trafego deve ser protegido como parte da política de segurança para o uso com uma VPN, a política de segurança é implementada na interface de configuração para cada par IPSec especifico.

As listas de acessos são usadas para determinar qual o trafego a ser criptografado e qual não deve ser criptografado nos pares, quando o trafego é gerado ou passa pelo cliente IPSec o cliente inicia o processo negociando uma troca IKE fase 1.

Etapa 2 - O IKE fase 1, tem como finalidade básica de autenticar os pares e configurar um canal seguro para ativar trocas IKE

IKE fase 1 pode ocorrer em dois modos, no modo principal e modo agressivo:

- No IKE, no modo principal, há a correspondência de SA's IKE entre pares, sendo que cada par opera de modo bidirecional, para fornecer um canal de comunicação protegido para as trocas IKE.
- No IKEv1 no modo agressivo, são feitas menos trocas com menos pacotes, com uma diminuição resultante no tempo que se leva para estabelecer a sessão, a desvantagem é que ambos os lados trocam informações antes que seja configurado um canal seguro, não sendo recomendável o uso do modo agressivo.

Inicia negociando uma política ISAKMP SA entre os pares para proteger a troca IKE, a ISAKMP SA especifica parâmetros IKE negociados de forma bidirecional.

Executa uma troca *Diffie-Hellman* autenticada com o resultado final de ter chaves secretas compartilhadas correspondentes. Autentica e protege as identidades dos pares.

A informação ISAKMP SA é armazenada localmente no banco de dados SA de cada ponto do par e configura um túnel seguro para negociação de parâmetros com o IKE fase 2 (Cisco, 2014).

Etapa 3 - IKE Fase 2, o IKE negocia os parâmetros das SA´s IPSec e configura SA's IPSec correspondente nos pares executando as seguintes funções:

- Negocia os parâmetros SA IPSec protegidos por uma SA IKE existente;
- Estabelece SA's IPSec;
- Renegocia periodicamente as SA's IPSec para garantir segurança;
- Realiza opcionalmente uma troca *Diffie-Hellman* Adicional

Após o IKE fase 1 tem um modo, o modo rápido, que ocorre depois que o IKE estabelece o túnel seguro na Fase 1. O modo rápido troca números aleatórios e é utilizada para renegociar uma nova SA IPSec quando expirada, fornecendo proteção de reprodução negociando uma política IPSec compartilhada derivada do material de chaveamento secreto compartilhado

usado nos algoritmos de segurança IPSec e estabelece SA's IPSec, os dados são transferidos entre os pares IPSec de acordo com os parâmetros do IPSec e as chaves são armazenadas no banco de dados SA (Westron, 2002).

O modo rápido básico é usado para atualizar o material de chaveamento usado na criação da chave secreta compartilhada com base no material de chaveamento derivado da troca *Diffie-Hellman* na Fase 1. As identidades das SA's negociadas no modo rápido são os endereços IP dos pares IKE.

A IPSec tem uma opção chamada *Perfect Forward Secrecy* (PFS), se a PFS for especificada na política IPSec, uma nova troca *Diffie-Hellman* será executada com cada modo rápido, fornecendo material de chaveamento com maior duração e maior resistência a ataques criptográficos (Westron, 2002).

Etapa 4 - Os dados são transferidos entre os pares IPSec nos parâmetros IPSec e as chave são armazenadas no banco de dados SA.

Etapa 5 - A terminação do túnel IPSec se da através de exclusão ou expiração, quando as SA's terminam as chaves são descartadas.

Esta forma modular permite a seleção de forma apropriada a diferentes conjuntos de algoritmos criptográficos, sem afetar as outras partes da aplicação.

3 SIMULAÇÃO PRÁTICA

Para a simulação será utilizado o software GNS3 versão 1.1. O GNS3 é um simulador gráfico de rede que permite a emulação de redes complexas e inclusive permite a emulação do sistema operacional de roteadores Cisco, Cisco *Internetwork Operating System* (IOS), o motivo da escolha do software foi devido ao *software* simulador da Cisco, o Cisco *Packet Tracer,* não dar suporte a todos os comandos utilizados.

Será configurado dois roteadores para suportar uma rede privada virtual IPSec para o tráfego que flui da sua respectivas redes. O trafego VPN IPSec passará através outro roteador que não tem conhecimento da VPN. O IPSec fornecera a transmissão segura de informações confidenciais em redes não protegidas, tais como a Internet agindo na camada de rede, com a proteção e autenticação de pacotes IP entre os dispositivos pares IPSec , com os seguintes objetivos;

- Inicialmente será definida a topologia a ser utilizada;
- Serão definidas as políticas a serem utilizadas;
- Serão configuradas as interfaces nos roteadores;
- Em seguida serão habilitadas as configurações de segurança;
- Será executado as configurações dos parâmetros de segurança IPSec no roteador R1 e no roteador R2;
- Verificar a conectividade da VPN IPSec criada.

O roteamento IPv6 é desabilitado por padrão nos roteadores cisco e é necessário ativa-lo, neste caso foi utilizado o *Routing Information Protocol next generation* - RIPng.

Para comunicação entre os roteadores, foi utilizada a conexão entre as portas seriais. Não foi implementado e configurado na topologia o endereçamento IPv4 e também não foi criada uma senha de aceso aos roteadores, o que seria recomendável em um ambiente não simulado.

3.1 TOPOLOGIA

A topologia utilizada é constituída por três roteadores Cisco, cada um contendo uma placa com quatro interfaces seriais e duas interfaces de rede.

As configuração dos endereços IPv6 foram alocados endereços globais *unicast* utilizando o endereço iniciado com 2001:db8 e nas interfaces seriais dos roteadores foi aplicado o RIPng para simular o ambiente da internet, foi incluída uma interface de rede em R2 para efeitos de teste e em todas as interfaces de rede dos roteadores foi utilizado um endereço IPv6 iniciado com

FD que é um conhecido como *Unique Local Address* (ULA) ou endereços locais únicos, equivalente aos endereços IPv4 privados, inclusive nas pontas do túnel IPSec, isso para demonstrar que endereços privados não roteados na internet podem ser utilizados na configuração de conexões VPN. A figura 17 ilustra a topologia e o endereçamento IPv6 a ser implementado.

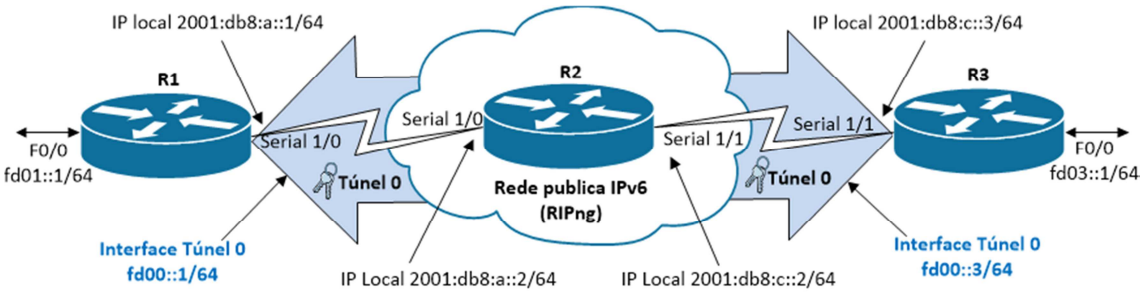

Figura 17 - Topologia
Fonte: Autoria própria, 2014.

O detalhamento dos endereços IPv6 utilizados nas respectivas interfaces dos roteadores assim como a sub-rede, e as interfaces que foi ativado o RIPng na topologia são apresentados na tabela 5 .

Tabela 5 - Endereçamento IPv6 das interfaces.

Dispositivo	Interface	Endereço IP	*Sub-Rede*	RIPng
Roteador R1	Serial 1/0	2001:db8:a::1	64	Sim
Roteador R1	FE0/0	fd01::1	64	-
Roteador R1	Túnel 0	fd00::1	64	-
Roteador R2	Serial 1/0	2001:db8:a::2	64	Sim
Roteador R2	Serial 1/1	2001:db8:c::2	64	Sim
Roteador R2	FE0/0	fd02::1	64	-
Roteador R3	Serial 1/1	2001:db8:c::3	64	Sim
Roteador R3	FE0/0	fd03::1	64	-
Roteador R3	Túnel 0	fd00::3	64	-

Fonte: Autoria própria.

3.2 CONFIGURAÇÃO DE ENDEREÇOS E ROTAS

Os comandos básicos utilizados para a configuração do roteador R1 pode ser visto no Quadro 1, a interface serial é configurada a partir da linha 5, na linha 8 é configurado o RIPng, e a configuração da interface de rede a partir da linha 11 até a linha 15.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)#ipv6 unicast-routing
5.  R1(config)#interface serial1/0
6.  R1(config-if)#ipv6 enable
7.  R1(config-if)#ipv6 address 2001:db8:a::1/64
8.  R1(config-if)#ipv6 rip PROCESSO1 enable
9.  R1(config-if)#no shutdown
10. R1(config-if)#exit
11. R1(config)#interface fastethernet 0/0
12. R1(config-if)#ipv6 enable
13. R1(config-if)#ipv6 address FD01::1/64
14. R1(config-if)#no shutdown
15. R1(config-if)#exit
16. R1(config)#end
```

Quadro 1 - Comandos para a configuração das interfaces em R1.

Os comandos básicos utilizados para a configuração do roteador R2 pode ser visto no Quadro 2, a interface serial 1/0 é configurada a partir da linha 5 ate a linha 10, na linha 8 é configurado o RIPng, a configuração da interface serial 1/1 a partir da linha 11 ate a linha 16, na linha 14 é configurado o RIPng, a interface de rede a partir da linha 17 ate a linha 21.

```
1.  R2#enable
2.  R2#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R2(config)#ipv6 unicast-routing
5.  R2(config)#interface serial1/0
6.  R2(config-if)#ipv6 enable
7.  R2(config-if)#ipv6 address 2001:db8:a::2/64
8.  R2(config-if)#ipv6 rip PROCESSO1 enable
9.  R2(config-if)#no shutdown
10. R2(config-if)#exit
11. R2(config)#interface serial1/1
12. R2(config-if)#ipv6 enable
13. R2(config-if)#ipv6 address 2001:db8:c::2/64
14. R2(config-if)#ipv6 rip PROCESSO1 enable
15. R2(config-if)#no shutdown
16. R2(config-if)#exit
17. R2(config)#interface fastethernet 0/0
18. R2(config-if)#ipv6 enable
19. R2(config-if)#ipv6 address FD02::1/64
20. R2(config-if)#no shutdown
21. R2(config-if)#exit
22. R2(config)#end
```

Quadro 2 - Comandos para a configuração das interfaces em R2.

Os comandos básicos utilizados para a configuração do roteador R3 pode ser visto no Quadro 3, a interface serial é configurada a partir da linha 5, na linha 8 é configurado o RIPng, a configuração da interface de rede a partir da linha 11 até a linha 15.

```
1.  R3#enable
2.  R3#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R3(config)#ipv6 unicast-routing
5.  R3(config)#interface serial1/1
6.  R3(config-if)#ipv6 enable
7.  R3(config-if)#ipv6 address 2001:db8:c::3/64
8.  R3(config-if)#ipv6 rip PROCESSO1 enable
9.  R3(config-if)#no shutdown
10. R3(config-if)#exit
11. R3(config)#interface fastethernet 0/0
12. R3(config-if)#ipv6 enable
13. R3(config-if)#ipv6 address FD03::1/64
14. R3(config-if)#no shutdown
15. R3(config-if)#exit
16. R3(config)#end
```

Quadro 3 - Comandos para configuração das interfaces em R3.

Para verificar a configuração e a conectividade das interfaces, a figura 18 apresenta o resultado do comando *ping* do roteador R1 para o roteador R2, um resumo das interfaces configuradas utilizando o comando *show ipv6 interface brief*, e o banco de dados das rotas criadas com o comando *show ipv6 rip database*.

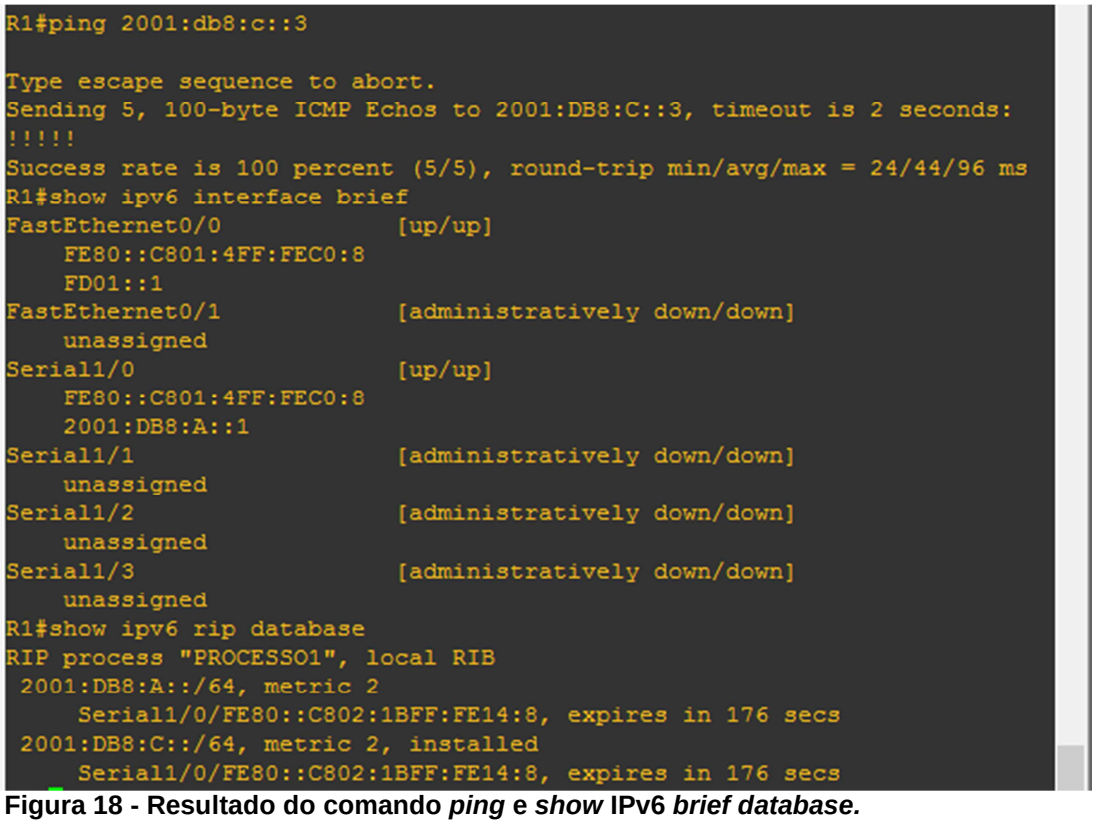

Figura 18 - Resultado do comando *ping* e *show* IPv6 *brief database.*
Fonte: Autoria própria, 2014.

3.3 ATIVANDO O MODULO *SECURITYK9*

O passo seguinte é necessário ser executado em ambos os roteadores pares, pois é preciso que o módulo de segurança esteja ativo no roteador R1 e no roteador R2, para que se possa utilizar os recursos avançados de criptografia, IPS, IPSec e VPN. O nome do modulo de segurança é o *securityk9*, ou *Security Technology Package license.* O mesmo não vem ativado por padrão nos roteadores Cisco, e é necessário instalar o pacote que pode ser executado tanto no modo EXEC ou no modo EXEC privilegiado.

Sua instalação é descrita na linha 4 do quadro 4, após o comando, é necessário aceitar a licença de uso, nas linhas 5 e 6 é descrito o comando que representa a finalização, seguido do comando para salvar as configurações do roteador e na linha 7 o comando para reiniciar o mesmo.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)# license boot module c2900 technology-package
securityk9
5.  R1(config-isakmp)# end
6.  R1# copy running-config startup-config
7.  R1# reload
```

Quadro 4 - Comandos para instalação do modulo securityk9 nos roteadores.

Após o reinicio do mesmo pode ser verificado se o modulo se encontra instalado executando o comando “*show version”.*

O *securityk9* não se encontra em todos os modelos disponíveis, e no status é possível verificar qual a licença que se encontra ativa no roteador, A licença tem descrito no resultado do comando “*show”*, como *Active* - Ativo, In Use - Em Uso ou *Inactive*-Inativo e são elas:

Evaluation - Avaliação, o que significa estará disponível com todas as funcionalidades para um período experimental com um total de 60 dias.

Permanent License - Licença Permanente, disponível para executá-lo permanentemente.

3.4 POLITICAS

Aqui serão definidas as politicas ISAKMP e a transformação IPSec e aplicadas no roteador R1 e no roteador R2

3.4.1 Politica ISAKMP

Por padrão, a os parâmetros da Fase 1 tem valores pré-definidos, ou seja se não for explicitado o valor, ela determinara que o valor padrão que devera ser utilizado, na a tabela 6 apresenta os parâmetros, as opções disponíveis, o padrão do comando, e o que será utilizado em cada roteador.

Tabela 6 - Parâmetros da Política ISAKMP Fase 1.

Parâmetro	Opções	Padrão	R1	R2
Método de distribuição	Manual ou ISAKPM	ISAKMP	ISAKPM	ISAKPM
Algoritmo de criptografia	DES, 3DES ou AES	DES	AES	AES
Algoritmo de *HASH*	MD5 ou SHA-1	SHA-1	SHA-1	SHA-1
Método de autenticação	PSK ou RSA	RSA	PSK	PSK
Troca de Chaves	DH1, 2, ou 5	DH1	DH2	DH2
Tempo de vida IKE SA	86400s ou menos	86400	43200	43200
Chave ISAKMP			chave_isakmp	chave_isakmp

Fonte: Autoria própria.

Foi substituída a criptografia de DES para AES, o método de autenticação foi alterado para PSK, o grupo *Diffie-Hellman* que por padrão era 1 foi alterado para 2, o tempo de vida da chave foi reduzido pela metade e definida a chave ISAKMP.

É necessário configurar a mesma política IKE e chave nos roteadores R1 e R2. Cada roteador devera ser configurado com a mesma chave, mais o endereço IPv6 da interface responsável pela conexão com o par.

Os comandos executados no roteador R1 podem ser acompanhados no quadro 5, na linha 4 é o comando definindo a politica ISAKMP, definida com o numero decimal 1, na linha 5 a definição do algoritmo de criptografia no caso AES, na linha 6 o método de autenticação PSK, na linha 7 a definição do grupo de trocas de chaves *Diffie-Hellman*, na linha 8 o tempo de vida definido para 12 horas, na linha 10 é aplicada a chave ISAKMP, com o numero da chave definido, no caso o numero 0, e a chave em si, seguida do endereço IPv6 do roteador R3 que é o roteador de destino, e por ultimo, na linha 11 o comando que permite estabelecer um intervalo de repetição independentemente do tráfego a ser enviado através do túnel, no caso após 30 segundos seguido de 30 tentativas caso não tenha sucesso de conexão.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)#crypto isakmp policy 1
5.  R1(config-isakmp)#encryption aes
6.  R1(config-isakmp)#authentication pre-share
7.  R1(config-isakmp)#group 2
8.  R1(config-isakmp)#lifetime 43200
9.  R1(config-isakmp)#exit
10.  R1(config)#crypto isakmp key 0 chave_isakmp address ipv6
2001:db8:c::3/64
11.  R1(config)#crypto isakmp keepalive 30 30
12.  R1(config)#end
```

Quadro 5 - Comandos para a politica ISAKMP em R1.

No quadro 6 mostra os comandos que foram executados no roteador R3 que são praticamente idênticos aos executados no roteador R1, com apenas uma diferença, na linha 10, no comando muda-se o endereço de destino que agora passa a ser o endereço do roteador R1.

```
1.  R3#enable
2.  R3#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R3(config)#crypto isakmp policy 1
5.  R3(config-isakmp)#encryption aes
6.  R3(config-isakmp)#authentication pre-share
7.  R3(config-isakmp)#group 2
8.  R3(config-isakmp)#lifetime 43200
9.  R3(config-isakmp)#exit
10.  R3(config)#crypto isakmp key 0 chave_isakmp address ipv6
2001:db8:a::1/64
11.  R3(config)#crypto isakmp keepalive 30 30
12.  R3(config)#end
```

Quadro 6 - Comandos para a politica ISAKMP em R3.

3.4.2 Transformação IPSec

Durante a segurança IPSec, na negociação de associação com o ISAKMP, os roteadores pares concordam em utilizar um determinado conjunto de criptografia para proteger o fluxo de dados que deve ser o mesmo para ambos os pares e proteger os fluxos de dados para a lista de acesso especificado na entrada *crypto-map* associada, combinando um método de criptografia e um método de autenticação, a tabela 7 lista os métodos de criptografia e autenticação válidos.

Tabela 7 - Métodos de criptografia e autenticação válidos.

Métodos de criptografia válidos	Métodos de autenticação válidos
esp-des	esp-md5-hmac
esp-3des (Padrão)	esp-sha-hmac (Padrão)
esp-aes (criptografia 128-bits)	
esp-aes-192 (criptografia 192-bits)	
esp-aes-256 (criptografia 256-bits)	
esp-null	

Fonte: Autoria própria.

No caso, será utilizada no método de criptografia e no método de autenticação a opção padrão. O quadro 7 mostra os comando que devem ser executados em ambos os roteadores pares, ou seja, no roteador R1 e no roteador R3, note que na linha 4 é determinado o nome da transformação, no caso nomeada como Tunel_VPN, e logo em seguida o método de criptografia e por ultimo o método de autenticação determinados para a transformação.

```
1.  #enable
2.  #configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  (config)#crypto ipsec transform-set Tunel_VPN esp-3des esp-sha-
hmac
5.  (cfg-crypto-trans)#mode tunnel
```

Quadro 7 - Comandos para Transformação IPSec em R1 e R3.

3.5 CRIANDO O PERFIL IPSEC

No quadro 8 é possível visualizar o comando utilizado para a criação do perfil IPSec, note que na linha 4 o perfil criado é nomeado como Mapa_VPN, e na linha 5 ele é associado a transformação IPSec definida que foi nomeada como Tunel_VPN, lembrando que os comandos do quadro 7 devem ser executados em ambos os roteadores pares, ou seja, no roteador R1 e no roteador R3.

```
1.  #enable
2.  #configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  (config)#crypto ipsec profile Mapa_VPN
5.  (ipsec-profile)#set transform-set Tunel_VPN
6.  (ipsec-profile)#end
```

Quadro 8 - Comandos para criação do Perfil IPSec em R1 e R3.

3.6 CRIANDO O PERFIL ISAKMP

O perfil ISAKMP deve estar configurado tanto nos roteadores R1 e R3 assegurando que a declaração de configuração deve designar o endereço de identidade da interface apropriada no roteador par.

A configuração do roteador R1 pode ser vista no quadro 9, a linha 4 mostra a criação do perfil com o nome perfil_isakmp, a linha 6 define a identidade que o roteador local utilizara para se identificar para o roteador remoto, na linha 7 o comando que corresponde a uma identidade par a partir de um ponto remoto no perfil ISAKMP, note que o endereço IPv6 que se encontra é do roteador R3.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)#crypto isakmp profile perfil_isakmp
5.  % A profile is deemed incomplete until it has match identity
statements
6.  R1(conf-isa-prof)#self-identity address ipv6
7.  R1(conf-isa-prof)#match identity address ipv6 2001:db8:c::3/64
8.  R1(conf-isa-prof)#keyring default
9.  R1(conf-isa-prof)#end
```

Quadro 9 - Comandos para criação do Perfil ISAKMP em R1.

A configuração do roteador R3 pode ser vista no quadro 10, praticamente idêntico ao aplicado em R1, com a diferença apenas na linha 7 referente ao endereço IPv6 do roteador R1

```
1.  R3#enable
2.  R3#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R3(config)#crypto isakmp profile perfil_isakmp
5.  % A profile is deemed incomplete until it has match identity
statements
6.  R3(conf-isa-prof)#self-identity address ipv6
7.  R3(conf-isa-prof)#match identity address ipv6 2001:db8:a::1/64
8.  R3(conf-isa-prof)#keyring default
9.  R3(conf-isa-prof)#end
```

Quadro 10 - Comandos para criação do Perfil ISAKMP em R3.

3.7 CONFIGURANDO O TÚNEL

Configurar o IPSec IPv6 VTI no roteador é bem simples, para facilitar o entendimento a tabela 8 traz as informações que foram utilizadas na configuração do túnel.

Tabela 8 - Parâmetros para o túnel IPSec.

Parâmetros	Roteador R1	Roteador R3
Interface do túnel	0	0
Nome do roteador par	R3	R1
Endereço do par	2001:db8:c::3	2001:db8:a::1
Nome do Crypto-map	Mapa_VPN	Mapa_VPN
Endereço de Rede	fd00::	fd00::
Endereço da Interface	fd00::1/64	fd00::3/64

Fonte: Autoria própria.

O quadro 11 apresenta os comandos utilizados para a configuração do túnel, na linha 4 o comando possibilita a criação do túnel chamado de 0 (zero), e funciona de forma similar com a configuração de uma interface física do roteador, o comando na linha 5 habilita o IPv6 na interface, na linha 6 o comando habilita o Cisco *Express Forwarding for* IPv6 (CEFv6) para estatísticas de tráfego IPv6 distribuídos na interface, a linha 6 define o endereço IPv6 que será utilizado na interface do túnel, na linha na linha 7 define o endereço do local do túnel, na linha 8 a definição da interface de origem, note que aqui poderia ser utilizado o endereço IPv6 respectivo da interface, na linha 9 o endereço do roteador par, no caso o endereço IPv6 da interface de destino no roteador R3, na linha 9 é ativado o IPSec sobre o IPv6 no túnel e na linha 10 é apontado o perfil IPSec previamente criado e que será utilizado.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)#interface tunnel 0
5.  R1(config-if)#ipv6 enable
6.  R1(config-if)#ipv6 cef
7.  R1(config-if)#ipv6 address fd00::1/64
8.  R1(config-if)#tunnel source serial1/0
9.  R1(config-if)#tunnel destination 2001:db8:c::3
10. R1(config-if)#tunnel mode ipsec ipv6
11. R1(config-if)#tunnel protection ipsec profile Mapa_VPN
12. R1(config-if)#end
```

Quadro 11 - Comandos para configuração do túnel em R1.

O quadro 12 apresenta os comandos executados no roteador R3 as diferenças com relação a configuração executadas no roteador R1 são os endereços IPv6 da interface do túnel local encontrada na linha 7 , o endereço ou a interface de origem dos dados na linha 8, e na linha 9 o endereço IPv6 do destino, no caso o roteador R1.

```
1.  R3#enable
2.  R3#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R3(config)#interface tunnel 0
5.  R3(config-if)#ipv6 enable
6.  R3(config-if)#ipv6 cef
7.  R3(config-if)#ipv6 address fd00::3/64
8.  R3(config-if)#tunnel source serial1/1
9.  R3(config-if)#tunnel destination 2001:db8:a::1
10. R3(config-if)#tunnel mode ipsec ipv6
12. R3(config-if)#tunnel protection ipsec profile Mapa_VPN
13. R3(config-if)#end
```

Quadro 12 - Comandos para configuração do túnel em R1.

3.8 CONFIGURANDO ROTAS

Para definir o túnel como melhor caminho para a rede local remota, foi configurado as rotas estáticas no roteador R1 e no roteador R2.

O quadro 13, na linha 4 mostra os comandos utilizados para configuração da rota estática em R1, note que o endereço utilizado é o endereço IPv6 da interface de rede F0/0 do roteador R3 através do endereço IPv6 da interface do túnel de R3.

```
1.  R1#enable
2.  R1#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R1(config)#ipv6 route FD03::/64 fd00::3
5.  R1(config)#end
```

Quadro 13 - Comandos para configuração de rota estática em R1.

O quadro 14, na linha 4 mostra os comandos utilizados para configuração da rota estática em R3, note que o endereço utilizado é o endereço IPv6 da interface de rede F0/0 do roteador R1 através do endereço IPv6 da interface do túnel de R1.

```
1.  R3#enable
2.  R3#configure terminal
3.  Enter configuration commands, one per line.  End with CNTL/Z.
4.  R3(config)#ipv6 route FD01::/64 fd00::1
5.  R3(config)#end
```

Quadro 14 - Comandos para configuração de rota estática em R3.

3.9 O TESTE DE CONECTIVIDADE DO TÚNEL

Após a configuração dos roteadores a conexão entre os pares deve estar estabelecida, os comandos a seguir ajudam a averiguar a conectividade e detalhes referente tanto ao IPv6 quanto ao IPSec

Com o comando "*show crypto ipsec sa"* é possível acompanhar detalhes referente a conexão como a quantidade de pacotes criptografados, erros de envio, os endereços dos pares e o tipo de transformação escolhida, tanto de entrada como de saída, a figura 19 demonstra o resultado do comando no roteador R1.

```
R1#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 2001:DB8:A::1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:DB8:C::3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
    #pkts decaps: 23, #pkts decrypt: 23, #pkts verify: 23
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:DB8:A::1,
     remote crypto endpt.: 2001:DB8:C::3
     path mtu 1460, ip mtu 1460, ip mtu idb Tunnel0
     current outbound spi: 0xE0F41D43(3774094659)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x9E15968E(2652214926)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80000046, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4498561/491)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xE0F41D43(3774094659)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, sibling_flags 80000046, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4498562/491)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
R1#
```

Figura 19 - Resultado do comando *show crypto ipsec as.*
Fonte: Autoria própria, 2014.

Com o comando “*show ipv6 interface brief* “é possível verificar os detalhes referente as interfaces de conexão, incluindo o próprio túnel, com o comando “*ping”* é possível fazer um teste de conectividade do túnel, o comando deve ser utilizado da seguinte forma, “*ping* versão endereço_de_destino *source* endereço_de_origem”, apesar da sintaxe “*ipv6*” na posição de versão ter sido adicionada ao comando ela não é mandatória e através da adição da sintaxe “*source”* o pacote inicia diretamente do endereço da interface escolhida, tanto a forma empregada como o uso correto de ambos os comandos se encontra ilustrado na figura 20.

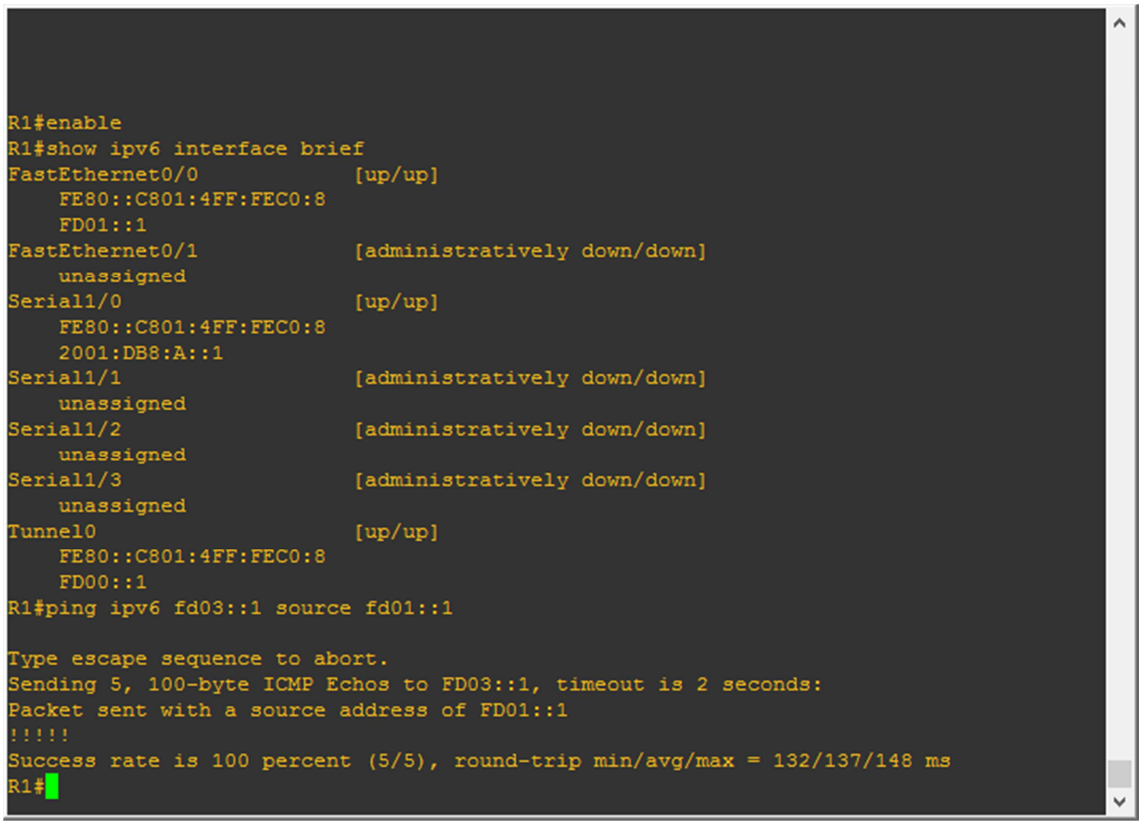

Figura 20 - Resultado do comando *show* IPv6 *interface brief e ping* IPv6.
Fonte: Autoria própria, 2014.

Com o comando “*show crypto isakmp sa*” é possível visualizar o ISAKMP e as associações de segurança construídas entre os pares além do estado do serviço indicando se se encontra ativo ou não. O resultado do comando é ilustrado na figura 21.

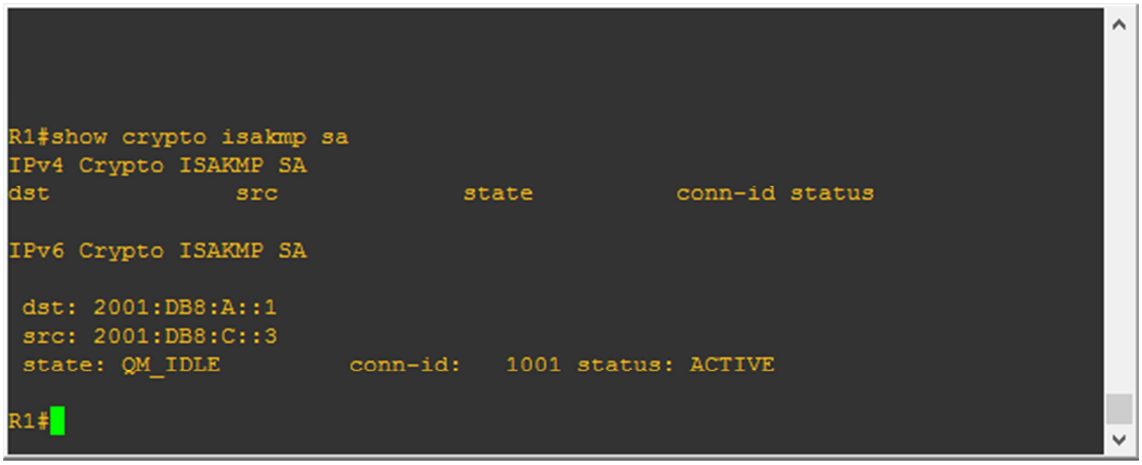

Figura 21 - Resultado do comando *show crypto isakmp sa*.
Fonte: Autoria própria, 2014.

O comando "*show crypto engine connection active*" mostra cada fase 2 das SA construídas e da quantidade de tráfego enviada. A partir da fase 2 as associações de segurança SAs são unidirecionais, cada SA mostra o tráfego em apenas um sentido, as criptografadas são de saída da interface e as descriptografadas são as de entrada da mesma, a figura 22 ilustra o resultado do comando.

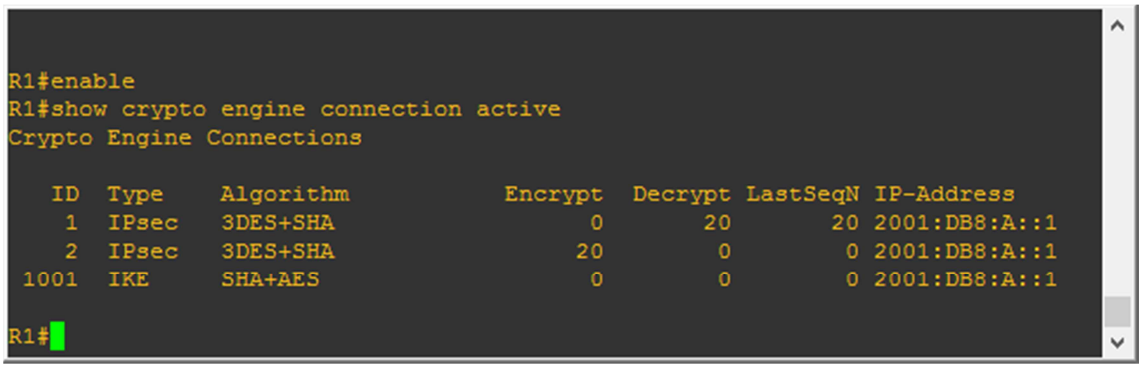

Figura 22 - Resultado do comando *show crypto engine connection active*.
Fonte: Autoria própria, 2014.

O comando "*traceroute*" foi utilizado apenas para teste de conectividade demonstrando que para a interface de rede o salto é apenas o destino do túnel, como é ilustrado na figura 23.

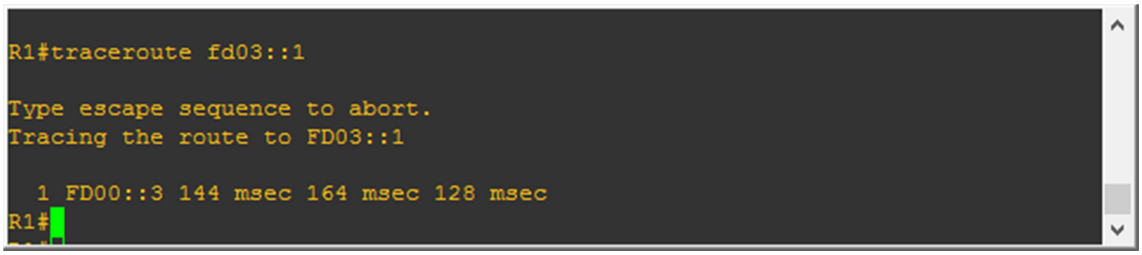

Figura 23 - Resultado do comando *traceroute*.
Fonte: Autoria própria, 2014.

3.9.1 Analise dos Pacotes com o Wireshark.

Foi utilizado o Wireshark para verificar a conexão serial entre o roteador R2 e o roteador R3, após o trafego ser gerado com o comando "*ping*" no roteador R1, no resultado ilustrado na figura 23 pode ser visto, o ESP como próximo pacote, comprovando a criptografia e o túnel entre o roteador R1 e o roteador R2.

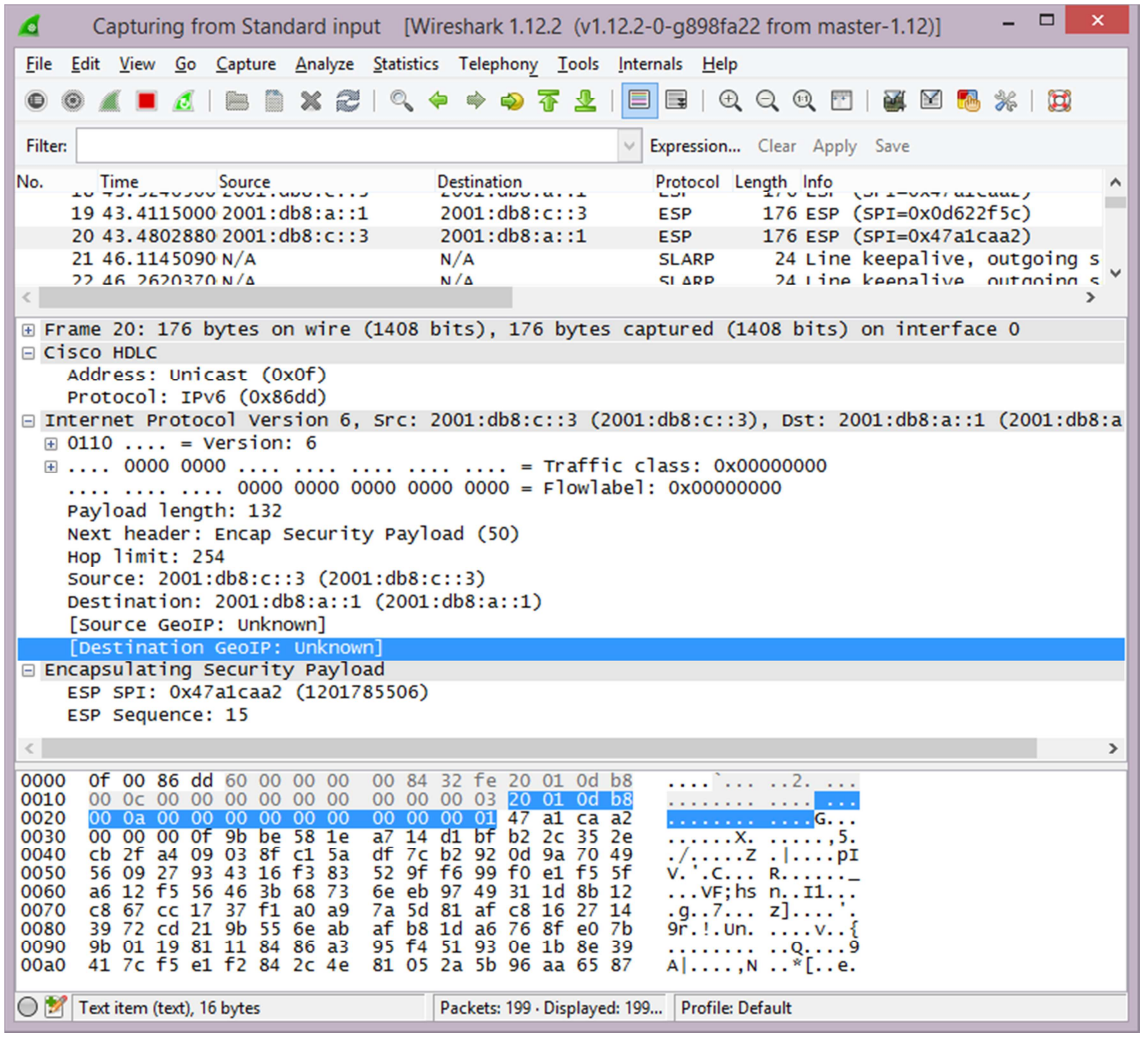

Figura 24 – Verificação do ESP com Wireshark.
Fonte: Autoria própria, 2014.

4 CONCLUSÃO

Através desta pesquisa foi possível verificar que mesmo que estruturas de grande porte necessitem de padrões de segurança mais elevados e definidos, como *firewalls*, a configuração de roteadores de borda utilizando o IPSec sobre o IPv6 traz uma forma barata e eficiente de pequenas empresas terem seus dados trafegando sobre a rede-publica e com segurança elevada, a criptografia dos pacotes IP na camada de rede oferecendo uma solução robusta.

O IPSec não somente tem a vantagem de disponibilizar o acesso a redes privadas em locais fixos implementadas com os roteadores, pois pode também ser configurado no modo transporte e ter acesso a uma rede privada virtualmente de qualquer lugar do mundo, através da internet, utilizando a infraestrutura pré-existente no local.

Apesar de em um primeiro momento a configuração tenha a aparência de complexidade, ela é bem definida, com regras são claras, depois de definidas as politicas de segurança, a configuração por completo do roteador fica relativamente simples de ser aplicada, e traz uma grande vantagem, após ser configurado, o túnel passa a operar de forma transparente, sem nenhuma necessidade de intervenção dos usuários da rede, ou configuração adicional nos dispositivos que utilizam a rede privada, como, por exemplo, servidores e computadores locais.

Uma desvantagem do tema atual é que apesar de novos dispositivos e equipamentos de redes possuam hoje em dia em sua grande maioria o suporte ao IPv6, é possível encontrar equipamentos incompatíveis, trazendo uma necessidade de substituição dos mesmos ou a configuração em pilha dupla.

A viabilidade que após ser configurado o túnel, e estabelecida a conexão e o trafego da rede privada se encontrar na rede pública, sem a possibilidade de observação provida pela confidencialidade dos dados, sem a possibilidade de ser modificado provido pelos serviços de autenticação, com controle de integridade e sigilo trazendo a garantia de que a informação esta segura, e só terá acesso a ela somente a quem for permitido.

REFERÊNCIAS

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

CAMPOS, André**. Auditoria em Tecnologia da Informação,** 2008. Disponível em: <http://www.slideshare.net/NLDT/auditoria-em-segurana-da-informao-andre-campos> Acesso em 05/10/2014

Cisco. **IKEv2 Packet Exchange and Protocol Level Debugging**, 2013. Disponível em: <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html> Acesso em 14/11/2014

Cisco. **Implementing IPsec in IPv6 Security**, 2012. Disponível em: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book/ip6-ipsec.html> Acesso em 12/10/2014

Cisco. **IPSec VPN WAN Design Overview**, 2014. Disponível em: <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html> Acesso em 25/09/2014

Cisco. **IPv6 Extension Headers Review and Considerations**, 2006. Disponível em: <http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html> Acesso em 14/10/2014

Ciscosecurity. **IP Security.** Disponível em: <http://ciscosecurity.org.ua/1587051672/ch12lev1sec2.html> Acesso em 23/09/2014

IPv6.br. **Endereçamento IPv6**, 2011. Disponível em: <http://ipv6.br/enderecamento-ipv6/> Acesso em 17/10/2014

IPv6.br. **IPv6 Básico,** 2014. Disponível em: Disponível em: <http://ipv6.br/download/> Acesso em 12/10/2014

IPv6.br. **IPv6 Cabeçalho IPv6**, 2012. Disponível em: <http://ipv6.br/entenda/cabecalho/> Acesso em 12/10/2014

RFC 2409. **The Internet Key Exchange (IKE)**, 1998. Disponível em: <https://www.ietf.org/rfc/rfc2409.txt> Acesso em 10/10/2014

RFC 4301. **Security Architecture for the Internet Protocol**. 2005. Disponível em: <https://www.ietf.org/rfc/rfc4301.txt> Acesso em 02/10/2014

RFC 3174. **US Secure Hash Algorithm 1 (SHA1)**, 2001. Disponível em: <https://tools.ietf.org/html/rfc3174> Acesso em 02/10/2014

TANENBAUM, Andrew S. **Redes de Computadores.** 5ª ed. São Paulo: Pearson Prentice Hall, 2011.

WENSTROM, Michael. **Managing Cisco Network Security (Gerenciando a segurança de redes CISCO).** Alta Books. 2002