FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE

JOSÉ WIRES SANTOS SILVA

IP SECURITY(IPSEC): AGREGANDO CONFIABILIDADE E SEGURANÇA À REDES VIRTUAIS PRIVADAS(VPN'S)

ARACAJU/SE

2017

FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE

JOSÉ WIRES SANTOS SILVA

IP SECURITY(IPSEC): AGREGANDO CONFIABILIDADE E SEGURANÇA À REDES VIRTUAIS PRIVADAS(VPN'S)

Artigo Científico apresentado a Faculdade de Administração e Negócios de Sergipe como requisito para conclusão MBA em Redes de Computadores 3.0.
Prof. Esp. Fernando Alves de Carvalho Filho.

ARACAJU/SE
2017/02

AGRADECIMENTOS

Agradeço à Deus na sua infinita bondade e pelo dom do conhecimento e sabedoria. Aos meus pais um agradecimento mais que especial por terem sempre me ensinado com dedicação e paciência e apoiado durante todo esse tempo. Aos professores Adriano Márcio Silva de Lima, Alércio Bressano e a mestra Maria José de Azevedo. Agradeço também aos amigos que estiveram presentes durante o período do curso em especial Adilson Oliveira, Ellinson Viana e Elytonyo Amorim pelos conselhos durante o período, pelos conhecimentos que adquiri com todos no desenvolvimento dos projetos acadêmicos. Agradeço à equipe de trabalho (Wagner Alves, Carla Almeida e Vitor Vaz) presentes no meu cotidiano e que veem contribuindo bastante para o meu saber, em especial à Mestranda Rita de Cássia Cardoso pela orientação e paciência.

"O êxito da vida não se mede pelo caminho que você conquistou, mas sim pelas dificuldades que superou no caminho" Abraham Lincoln.

IP SECURITY(IPSEC): AGREGANDO CONFIABILIDADE E SEGURANÇA À REDES VIRTUAIS PRIVADAS(VPN'S)

José Wires Santos Silva[1]

RESUMO

Este artigo tem o objetivo de analisar como surgiram as principais ideias que levaram a criação do IPSec bem como situar o leitor sobre o momento que verificou-se a necessidade de se ter um meio virtual mais seguro. O estudo será bibliográfico sobre a luz de **Douglas Falsarella 2008**, também empírico e será feito uma análise documental. o trabalho está dividido da seguinte forma: será abordado os critérios de estudos na primeira reunião do grupo e os principais temas discutidos; Em seguida será abordado sobre as reuniões definitivas que levaram a criação da tecnologia; Posteriormente será abordado o funcionamento da tecnologia, bem como suas principais aplicações nos dias atuais e por fim apresentados argumentos conclusivos que ratificam a boa aceitabilidade e usabilidade da tecnologia no cenário atual por grandes e pequenas empresas.

PALAVRAS CHAVES: Tunelamento, VPN, Criptografia, Segurança, Algoritmos.

1. INTRODUÇÃO

O IP Security (IPSec) é um conjunto de protocolos criado a partir da necessidade de garantir integridade, confiabilidade, confidencialidade e autenticidade para dados que fossem trafegados por meios digitais públicos. Inicialmente foi criado para ser suportado tanto no IPV4 quanto no IPV6, entretanto com o tempo a sua utilização ganhou um notório espaço com o advento e ascensão das redes virtuais privadas (VPN's).

Esta tecnologia vem ganhando espaços cada vez mais significativos no campo empresarial, uma vez que é uma tecnologia eficiente, fornece um alto nível de segurança tanto para usuários como para administradores de rede e possui um baixo custo de implantação, este último fator por si só já o coloca num patamar bastante elevado.

Com ascensão deste protocolo sobre outros descobertos na época, verificou-se também que era possível conectar redes distintas com a simples criação de uma Virtual Private Netwok(VPN), ou seja, a partir daí era possível criar conexões privadas dentro de conexões públicas. Porém, isto criava a falsa sensação de segurança, uma vez que este protocolo não implementa criptografia, ou seja, não havia garantia que o dado chegaria íntegro ao seu destinatário.

---

1 Graduado em Redes de Computadores pela Faculdade Estácio de Sá e certificado em ITIL Foundation.

Uma vez que o dado fosse enviado e fosse interceptado por terceiros, este dado poderia simplesmente ter suas informações alteradas e o destinatário nunca saberia, uma vez que o dado ao ser enviado não era criptografado.

Quando o protocolo IP (Internet Protocol) foi criado na década de 80, não se pensava ou esperava-se que o mesmo viesse a tornar-se tão essencial na comunicação entre dispositivos, visto que hoje todo e qualquer dispositivo que trabalha em rede utiliza a comunicação através do protocolo IP. Desta forma não houve uma preocupação nos algoritmos de criptografia do protocolo. Com a popularização deste protocolo na década de 90, verificou-se que por mais fácil que fosse a implementação, utilização e a eficiência do mesmo, ainda faltava um aspecto muito importante que era segurança.

Diante dos problemas citados acima foi criado o IP Security em meados da década de 90. Esta solução veio para entregar autenticidade, confiabilidade e integridade que os administradores de redes estavam buscando a muito tempo.

2. HISTÓRIA

Segundo a RFC 1636, vários especialistas foram reunidos pelo IAB (Internet Architecture Board) entre os dias 8 e 10 de fevereiro de 1994. Este workshop foi realizado no instituto de Ciências da Informação da Universidade do Sul da Califórnia em Marina Del Rey.

Além dos membros do IAB, foram convidados diversos outros especialistas num total de 15, vale ressaltar também que foram incluídos os Diretores do IESG (Internet Engineering Steering Group) para discussão de grandes áreas como: Roteamento, Mobilidade, Serviço em tempo Real, Requisitos de fornecedor e Segurança. O IAB tentou equilibrar o número de participantes de cada área de especialização.

A Logística limitou o atendimento a cerca de 30, o que infelizmente significou que muitos especialistas altamente qualificados foram omitidos na lista de convidados. Em síntese, os objetivos deste evento foram: Explorar interconexões entre a segurança e o restante da arquitetura da internet, desenvolver recomendações para a comunidade da internet em orientações futuras em relação à segurança. Estes objetivos surgiram de uma convicção da IAB de que as duas áreas problemáticas mais importantes para a arquitetura são a escalabilidade e a segurança.

A princípio os convidados chegaram ao workshop ansiosos para discutirem questões de segurança imediatistas, no entanto o foco da reunião eram as questões de longo prazo e princípios gerais. Desta forma, a reunião tinha uma clara regra de base ao ser iniciada: os tópicos válidos de discussão deveriam envolver tanto a segurança quanto pelo menos uma questão da lista: (a) roteamento (unicast e multicast), (b) mobilidade e (c) serviço em tempo real. Como base para a discussão inicial, os convidados se encontraram por e-mail para gerar um conjunto de cenários que satisfaçam esta regra de base.

Os 30 participantes foram divididos em três grupos "breakout", com cada grupo, incluindo especialistas em todas as áreas. A reunião foi então estruturada como reuniões plenárias alternadas com sessões de grupos paralelos. No terceiro dia, os grupos produziram textos resumindo os resultados de suas discussões. Este memorando é composto desses textos, um pouco reorganizados e editados em um único documento.

O processo de reunião determinou o caráter deste documento. Deve ser considerado como um conjunto de notas de trabalho produzidas por grupos principalmente autônomos, contendo alguma diversidade de opiniões, bem como a duplicação de ideias. Não é o resultado da "comunidade de segurança", mas sim representa ideias sobre a segurança desenvolvida por um amplo espectro de especialistas na Internet. É oferecido como um passo em um processo de desenvolvimento de mecanismos de segurança viáveis e procedimentos para a Internet.

Após esta reunião citada anteriormente foram realizadas diversas outras que tiveram como objetivos principais criar e aprimorar um protocolo ou melhor dizendo, um conjunto de protocolos como é denominado o IPSec, que fornecesse a segurança adequada na internet que o usuário tanto precisava. Abaixo podemos verificar a data das reuniões mais importantes, bem como os números dessas RFC’s criadas após cada reunião e os temas abordados:

> RFC 1825: “Este memorando descreve os mecanismos de segurança para IP versão 4 (IPV4) e IP versão 6 (IPV6) e os serviços que eles fornecem. Cada mecanismo de segurança é especificado em um documento separado. Este documento também descreve requisitos de gerenciamento de chaves para

sistemas implementando esses mecanismos de segurança. Este documento não é uma arquitetura de segurança geral para a Internet, ao invés disso, ele é focado na segurança da camada IP" (RFC 1825, 1995).

RFC 1826: "Este documento descreve um mecanismo para fornecer criptografia de autenticação para datagramas IPv4 e IPv6. Um cabeçalho de autenticação (AH) normalmente é inserido após um cabeçalho de IP e antes do outro informações autenticadas" (RFC 1826, 1995).

RFC 1827: "Este documento descreve o IP Encapsulating Security Payload (ESP). ESP é um mecanismo para fornecer integridade e confidencialidade ao IP datagramas. Em algumas circunstâncias, também pode fornecer autenticação para datagramas IP. O mecanismo funciona com IPv4 e IPv6" (RFC 1827, 1995).

RFC 2401: "Este memorando especifica a arquitetura base para conformidade entre o IPsec e sistemas. O objetivo da arquitetura é fornecer várias camadas de segurança, serviços para o tráfego na camada IP, tanto no IPv4 como no IPv6 ambientes. Este documento descreve os objetivos de tais sistemas, seus componentes e como eles se encaixam uns com os outros e o ambiente IP. Ele também descreve os serviços de segurança oferecidos pelos protocolos IPsec, e como esses serviços podem ser empregados no Ambiente IP. Este documento não aborda todos os aspectos do IPsec arquitetura. Os documentos subseqüentes abordarão Detalhes arquitetônicos de uma natureza mais avançada, por exemplo, uso de IPsec em ambientes NAT e suporte mais completo para multicast IP" (RFC 2401, 1998).

RFC 2412: "Este documento descreve um protocolo, chamado OAKLEY, pelo qual duas partes autenticadas podem concordar em trocar material, por meio de uma troca de chave

secreta e segura. O mecanismo básico é o algoritmo de troca de chaves Diffie-Hellman.

O protocolo OAKLEY suporta Perfect Forward Secrecy, compatibilidade com o protocolo ISAKMP para o gerenciamento de associações de segurança, estruturas de grupos abstratas definidas pelo usuário para uso com o algoritmo Diffie-Hellman , atualizações de chaves e incorporação de chaves distribuídas por mecanismos fora de banda" (RFC 2412, 1998).

RFC 6071: Segundo (RFC 6071, 2011) este documento descreve brevemente o IPSec e faz um apanhado das RFC's anteriores a ela.

3. FUNCIONAMENTO

"O IETF criou um conjunto de protocolos que oferece comunicação segura pela internet. Coletivamente conhecidos como IPsec (abreviação de IP security), os protocolos oferecem serviços de autenticação e privacidade na camada IP e podem ser usados com IPV4 e IPV6. Mais importante, em vez de especificar completamente a funcionalidade do algoritmo de criptografia a ser usado, o IETF escolheu tornar o sistema flexível e extensível.

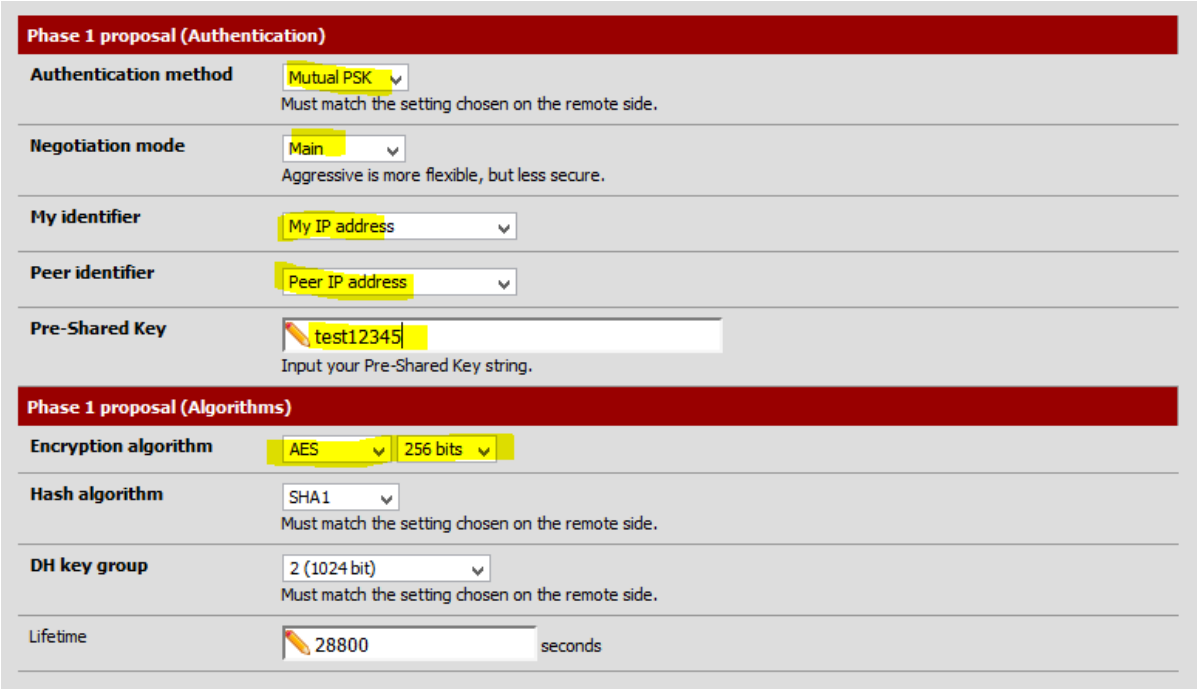
Por exemplo, uma aplicação que emprega IPsec pode escolher se usará uma facilidade de autenticação que valida o emissor ou uma facilidade de criptografia que também garante que o payload permanecerá confidencial; as opções podem ser assimétricas (por exemplo, autenticação em uma direção, mas na outra não). Além do mais, IPsec não restringe o usuário a um algoritmo de criptografia ou autenticação específico.

Em vez disso, IPsec fornece uma estrutura geral que permite que cada par de extremidades em comunicação escolha algoritmos e parâmetros (por exemplo, tamanho da chave). Para garantir a interoperabilidade, o IPsec inclui um

> conjunto de algoritmos de criptografia que todas as implementações precisam reconhecer. O ponto importante é: IPsec não é um protocolo de segurança isolado. Em vez disso, IPsec fornece um conjunto de algoritmos de segurança e mais uma estrutura geral que permite que um par de entidades em comunicação utilize quaisquer algoritmos que ofereçam segurança apropriada para a comunicação "(COMER, 2006, p.360).

Podemos confirmar estas informações na imagem 1.0 onde temos uma tela da appliance do firewall PFsense 2.2.4(IKE V2) que mostra no campo "Authentication" e "Authentication method" a opção "Mutual PSK", onde tanto o transmissor quanto o receptor devem ser autenticados por meio de um usuário e senha:

Figura 1.0
MÉTODO DE AUTENTICAÇÃO

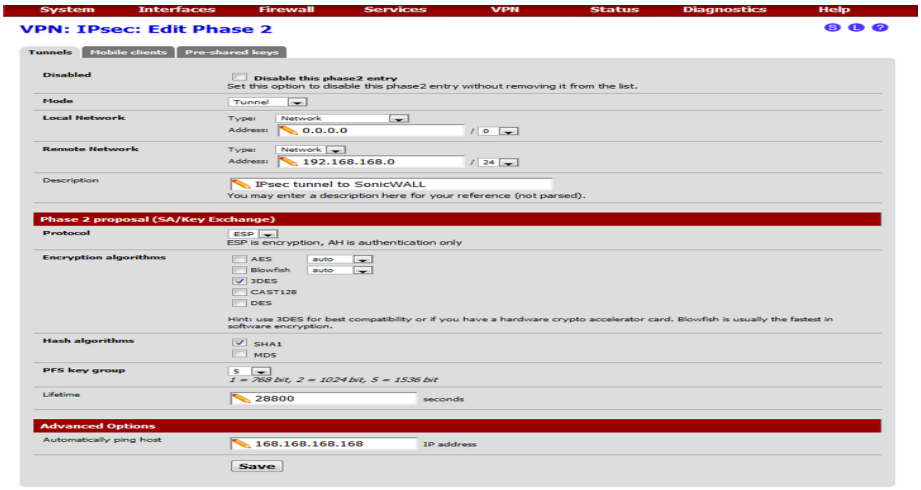


Fonte: https://blog.linoxide.com/wp-content/uploads/2016/10/step-1-b.png

Mais abaixo na figura 1.1 podemos verificar o processo de escolha do algoritmo, o tamanho da chave e o protocolo para criptografia. Neste exemplo também foi usado a appliance do PFsense 2.2.4 para demonstração:

Figura 1.1

PROCESSO DE ESCOLHA DE CHAVES, TIPO DE PROTOCOLO E ALGORITMOS.

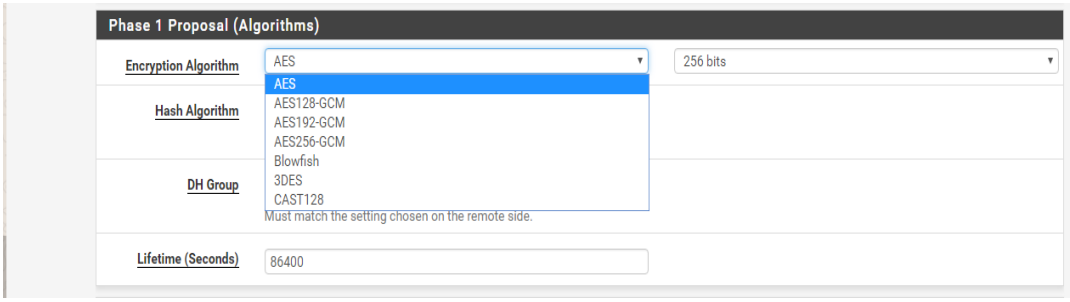


Fonte:https://doc.pfsense.org/images/thumb/a/a4/Ipsec-s2s-vork-13.png/700px-Ipsec-s2s-vork-13.png

Respectivamente nas figuras 1.2 e 1.3 podemos verificar também outros tipos de algoritmos de encriptação:

Figura 1.2

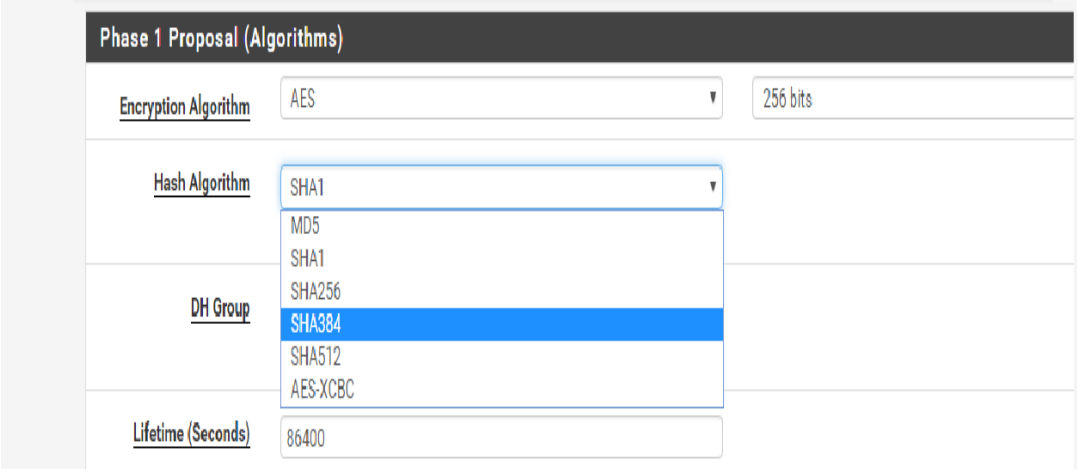
ALGORITMOS DE ENCRIPTAÇÃO



Fonte: Autoria própria, 2017. pfSense, versão 2.3.4

Figura 1.3

ALGORITMOS DE ENCRIPTAÇÃO



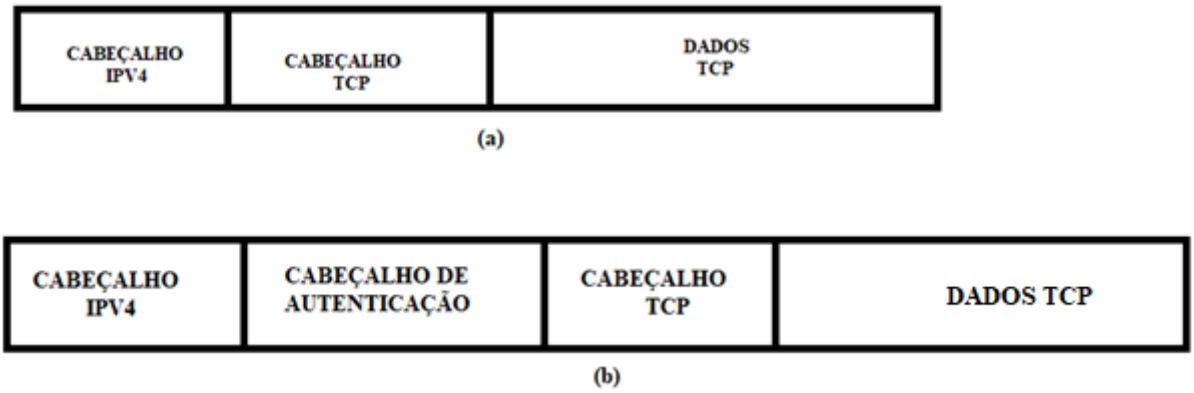
Fonte: Autoria própria, 2017. pfSense, versão 2.3.4

4. CABEÇALHO DE AUTENTICAÇÃO IPSEC

Desse modo, ao invés de alterar o cabeçalho do datagrama básico ou criar uma opção IP, o IPsec usa um cabeçalho de autenticação (Authentication Header - AH) separado para transportar informações de autenticação. Podemos verificar as informações na figura 1.4 que aborda estes campos da melhor forma possível:

Figura 1.4

CABEÇALHO DE AUTENTICAÇÃO IPSEC



Fonte: (Interligação de Redes com TCP/IP - vol.1, Princípios, Protocolos e Arquitetura, 2006).

Conforme mostrado na figura acima, é possível notar a inserção de um cabeçalho de autenticação logo após o cabeçalho IP original, antes claro do cabeçalho de transporte.

5. DEFINIÇÕES

Nesse contexto, podemos verificar que o porquê do IPSec ser tão seguro, mas antes de mais nada é necessário compreender a importância de algumas funções garantidas pelo IPSec. São elas:

5.1 Privacidade: É a garantia que usuários não autorizadas não irão ter acesso de leitura ou visualização do conteúdo. Em outras palavras, o remetente precisa garantir que a mensagem enviada pode ser lida somente pelo destinatário. Vale ressaltar que a privacidade pode ser obtida por meio da utilização de criptografia (FALSARELLA, 2008).

5.2 Integridade por sua vez é a garantia que as mensagens trocadas entre o remetente e o destinatário não serão alteradas no caminho entre origem e destino. Este recurso pode ser obtido através do uso do hashing (FALSARELLA, 2008).

5.3 Autenticidade: É a garantia que terceiros enviem mensagens falsas passando-se pelo remetente original. Este recurso pode ser obtido através de assinaturas digitais (FALSARELLA, 2008).

5.4 Criptografia é a forma de proteger a mensagem enviada de modo que esta somente por ser lida ou interpretada pelo destinatário que possui a o segredo (a chave) correta em poder (FALSARELLA, 2008).

5.5 Algoritmo de Criptografia: Composto por uma complexa seqüências de operações matemáticas em que uma chave é combinada com o conteúdo cleartext resultando em um texto criptografado. Exemplos de algoritmos de criptografia são o DES (Data Encryption Standard) e o AES (Advanced Encryption Standard). (FALSARELLA, 2008)

5.6 Key Strength: É uma métrica utilizada para medir a dificuldade que pessoas não autorizadas teriam para ler o conteúdo de um pacote quando o algoritmo de criptografia é conhecido e a chave desconhecida. É correto afirmar que o “Key Strength” é uma função do tamanho da chave (FALSARELLA, 2008).

5.7 Hashing: Podemos afirmar que um hash é cálculo baseado no tamanho da mensagem, onde este resultado unicamente pode ser utilizado para identificar a mensagem. Vale ressaltar que uma mínima alteração na mensagem pode acarretar um número de hash completamente diferente (FALSARELLA, 2008).

5.8 Assinatura Digital: Conforme foi dito (FALSARELLA, 2008) é importante afirmar que assinatura digital é um texto que somente pode ser criado por alguém que conhece uma chave específica. A criptografia de um texto pode ser utilizada como assinatura digital pois somente o “signer” conhece a chave utilizada (FALSARELLA, 2008).

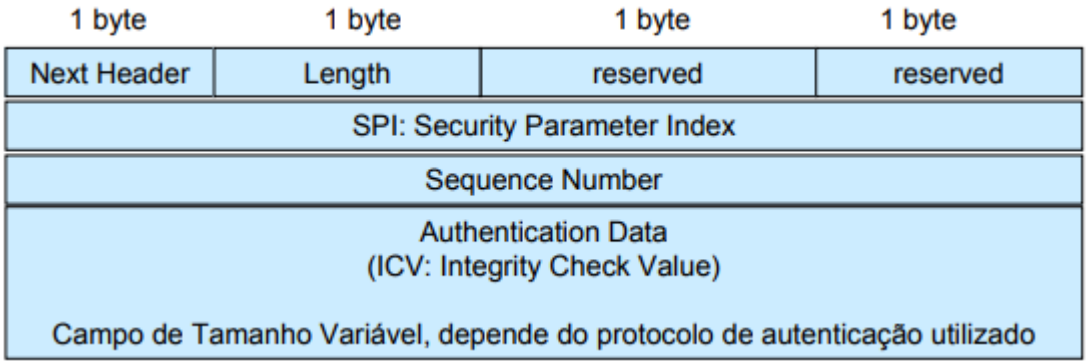
6. PROTOCOLOS QUE COMPÕEM O IPSEC

Agora que compreendemos a importância das funções do IPSec é necessário compreender a composição do núcleo. O núcleo do IPSec é composto três protocolos de extrema importância:

6.1 Authentication Header (AH) - Este protocolo responsabiliza-se por prover a integridade e autenticidade dos dados que são trocados entre receptor e transmissor. Vale ressaltar que este protocolo possui uma limitação técnica conforme será abordada adiante. Estas informações podem ser verificadas na figura 1.5:

Figura 1.5

Cabeçalho do AH

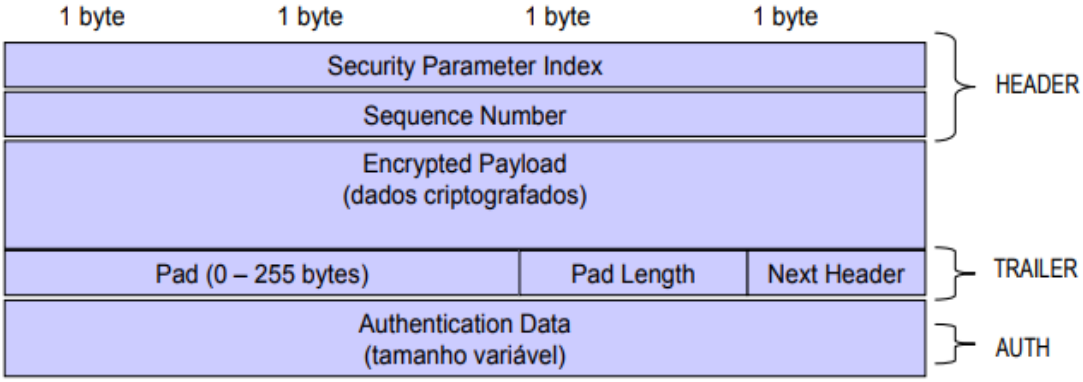


Fonte: (JAMHOUR, 2009)

6.2 Encapsulating security payload (ESP) - Este protocolo por sua vez, possui capacidade de criptografar os dados que são transmitidos, proporcionando assim uma maior integridade dos dados em relação ao AH citado anteriormente.

Figura 1.6

Cabeçalho do ESP



Fonte: JAMHOUR, 2009.

6.3 Internet Key Exchange (IKE) - Este protocolo é o grande responsável por resolver os problemas adicionais de proporcionar aos nós terminais do canal seguro as chaves necessárias para a operação dos protocolos de autenticação e criptografia de dados.

Após este breve descritivo é possível concluir que o protocolo ESP supera em todos os aspectos o AH, tendo em vista que o ESP além de agregar uma melhor integridade graças a criptografia também possui o recurso de autenticação tornando-se assim um protocolo mais robusto e eficaz.

Segundo (OLIFER; OLIFER, 2006, p.533), a distribuição de funções de segurança entre o AH e o ESP (tabela 1.5) justifica-se pela limitação da exportação, importação ou de ambas, para as ferramentas de criptografia, prática adotada por

muitos países. Esses protocolos podem ser usados de maneira independente ou juntos. Essa prática é conveniente quando é impossível empregar criptografia devido às limitações existentes. Nesse caso é possível proporcionar ao sistema somente o protocolo AH. Naturalmente, a proteção de dados proporcionando somente o AH será insuficiente em muitos casos.

Nesses casos, a parte receptora só pode verificar se os dados foram enviados pelo nó do qual eram esperados e se foram entregues da mesma maneira como foram enviados. O protocolo AH não pode proteger as informações contra uma visão não autorizada quando essas informações trafegam através da rede. Isso acontece porque o protocolo AH não criptografa dados conforme dito anteriormente. Para criptografar dados é necessário usar o protocolo ESP. Na figura 1.7 podemos observar as funções de cada protocolo:

Figura 1.7

Tabela 1.5 Distribuição de Funções entre Protoclos IPSec

Funções	**Protocolo**	
Proporcionar integridade	AH	ESP
Proporcionar autenticidade		
Proporcionar confidencialidade (Criptografia)		
Distribuição de chaves privadas	IKE	

Fonte: OLIFER;OLIFER, 2006, p.534

Quando o IPSec recebe um pacote IP, a primeira coisa que é feita é a adição de um header ou um cabeçalho em outras palavras, em resumo um “AH”. Este cabeçalho fica responsável por três funções de extrema importância:

- É utilizado para autenticação entre Hosts.
- É importante para verificação da integridade dos dados.
- É peça chave para impedir ataques de repetição.
- Vale ressaltar que este cabeçalho não é criptografado.

7. TIPOS DE UTILIZAÇÕES DO IPSEC

Segundo (FALSARELLA, 2008) o IPSec pode ser usado de dois modos:

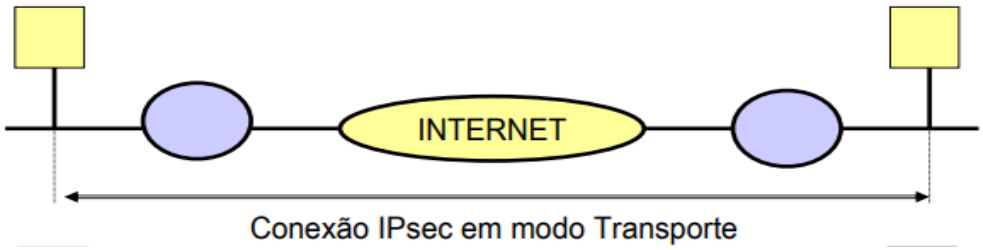
- Modo transporte

Este modo garante a segurança apenas dos dados provenientes das camadas superiores.

Geralmente faz-se uso deste modo sempre que há necessidade de uma comunicação “fim-a-fim” entre computadores conforme observado na figura 1.8:

FIGURA: 1.8

Modo Transporte



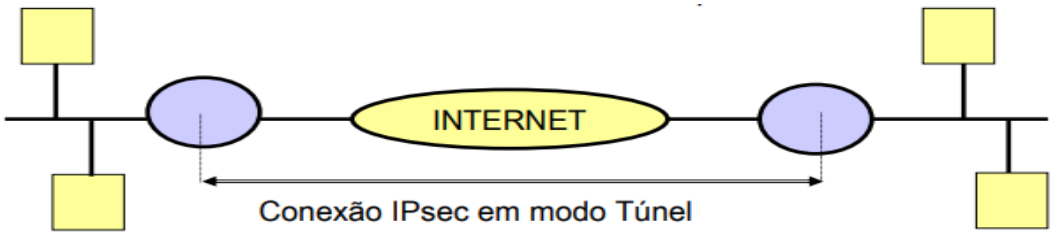
Fonte: FALSARELLA, 2008, p. 5

- Modo tunel

“Fornece segurança também para a camada IP. Utilizado geralmente para comunicação entre roteadores” (JAMHOUR, 2009). Podemos observar este modo na figura 1.9:

FIGURA: 1.9

Modo Túnel



Fonte: JAMHOUR, 2009, p. 5

8 O QUE É TUNELAMENTO?

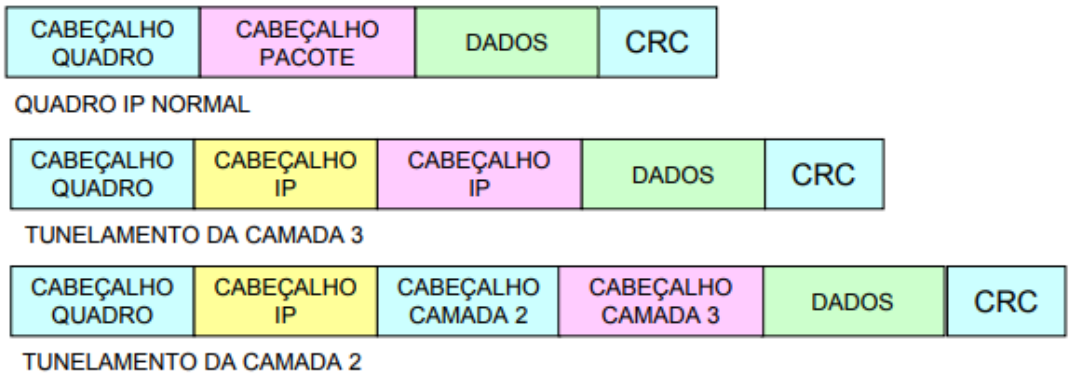
Ligeiramente falando, o termo “Tunelar” significa introduzir dados de uma determinada camada do modelo OSI dentro de outra camada ou protocolo de forma segura utilizando os mecanismos adequados para fornecer essa segurança obviamente.

Segundo (JAMHOUR, 2009), existem dois tipos de Tunelamento:

- Tunelamento de camada 3: Transporta apenas pacotes IP.
- Tunelamento de camada 2: Permite transportar outros protocolos de rede: IP, NetBEUI, IPX.

Figura 2.0

Tunelamento



Fonte: JAMHOUR, 2009, p.8

9. VPN'S E SEUS PROTOCOLOS

Conforme afirmam os autores (OLIFER e OLIFER, 2006, p. 545), o IPSec é a principal tecnologia VPN com base em criptografia. Ele é usado para criação de uma infraestrutura de canais seguros conectando os sites pertencentes a uma só empresa(intranet) ou a várias delas(extranet). Abaixo estão apresentados alguns dos principais protocolos de VPN's:

-L2F

Layer 2 Fowarding Protocol(Cisco).

Não é mais utilizado.

-PPTP

Tunelamento de camada 2.

Point-to-Point tunneling Protocol.

-L2TP

Tunelamento de camada 2.

Level 2 Tunneling Protocol(L2TP).

Combinação do L2F e PPTP.

-IPSEC

Tunelamento de Camada 3.

IETF(Internet Engneerung Task Force).

Podemos melhor observar as diferenças de cada protocolo observando a figura 2.1 abaixo:

Figura 2.1

Protocolos VPN

Protocolo	Tunelamento	Criptografia	Autenticação	Aplicação Típica
PPTP	Camada 2	Sim	Sim	Host - Host Host - Rede
L2TP	Camada 2	Não	Sim	Host - Rede (iniciado pelo NAS)
IPsec	Camada 3	Sim	Sim	Host - Host Host - Rede Rede - Rede
IPsec e L2TP	Camada 2	Sim	Sim	Host - Host Host - Rede Rede - Rede

Fonte: (JAMHOUR, 2009, p.12)

10. APLICAÇÕES DO IPSEC

O autor (STALLINGS, 2005, p. 397), afirma que o IPSec fornece a capacidade de proteger comunicações por meio de uma LAN, por meio de WANs públicas e privadas e através da internet. Exemplos do seu uso incluem:

- Proteção da conectividade de filiais por meio da internet: Uma empresa pode construir uma rede privada virtual por meio da Internet ou de uma WAN pública. Isso permite que a empresa utilize intensamente a internet e reduza sua necessidade de redes privadas, reduzindo custos e overhead de gerenciamento de rede. É importante ressaltar que devido à esta enorme aceitação do IPSec e sua segurança é correto afirmar que em alguns casos o uso de tecnologias de longa distância como MPLS, Metro Ethernet ou qualquer outra tecnologia vem sendo descartado principalmente pelo alto custo de implantação e manutenção.
- Acesso remoto seguro através da Internet: Um usuário final cujo sistema esteja equipado com protocolos de segurança IP pode fazer uma chamada local para um provedor de internet (ISP) e ganhar acesso seguro à rede de uma empresa. Isso reduz o custo com despesas de viagem de funcionários e tele comutadores.
- Estabelecimento de conectividade de extranet e intranet com parceiros: O IPSec pode ser usado para proteger comunicação entre outras organizações, garantindo autenticação e privacidade e fornecendo um mecanismo de troca de chaves.
- Melhoria da segurança no comércio eletrônico: Ainda que algumas aplicações da Web e de comércio eletrônico tenham protocolos de segurança embutidos, o uso do IPSec aumenta essa segurança. O IPSec garante que todo o tráfego designado pelo administrador de rede seja criptografado e autenticado,

acrescentando uma camada extra de segurança no que quer que seja fornecido na camada de aplicação.

11 VANTAGENS DO IPSEC

Ainda segundo o autor (STALLINGS, 2005), é possível afirmar dentre as algumas das principais vantagens do IPSec estão:

- Quando o IPSec é implementado em um firewall ou roteador, ele proporciona forte segurança para ser aplicada em todo o tráfego que cruza o perímetro. O tráfego dentro de uma empresa ou grupo de trabalho não incorre no overhead do processamento relacionado à segurança.
- O IPSec em um firewall é resistente ao bypass, se todo o tráfego do exterior precisar usar IP e o firewall for o único meio de entrada da internet para a organização.
- O IPSec está abaixo da camada de transporte (TCP, UDP) e, portanto, é transparente às aplicações. Não há a necessidade mudar o software em um sistema de usuário ou servidor quando o IPSec é implementado no firewall ou roteador. Mesmo se o IPSec for implementado em sistemas finais, o software de camada superior, incluindo as aplicações, não é afetado.
- O IPSec pode ser transparente aos usuários finais. Não há necessidade de treinar usuários nos mecanismos de segurança, publicar material codificado para cada usuário ou invalidar material codificado quando os usuários deixam organização.
- O IPSec pode fornecer segurança para usuários individuais, se necessário. Isso é útil para trabalhadores externos e para configurar uma sub-rede virtual segura dentro de uma organização para aplicações críticas.

12 CONSIDERAÇÕES FINAIS

Com base nas informações abordadas anteriormente podemos concluir que o IPSec veio com a proposta de solucionar os problemas enfrentados pelo IPV4 e realmente solucionou. Com a elaboração deste estudo foi possível também compreender a importância da criptografia sempre que dois ou mais computadores necessitam estabelecer uma comunicação em uma rede. Foi possível verificar também que o IPSec possui um ótimo custo benefício, uma vez boa parte dos dispositivos de rede que são comercializados no mundo suportam a tecnologia. Vale ressaltar que o IPSec se comparado à outras tecnologias como MPLS, Frame Relay,

Metro Ethernet possui um custo bastante reduzido ou nenhum. Diante destas informações podemos concluir que todos os objetivos foram atingidos.

SUMMARY

This article aims to analyze how the main ideas that led to the creation of IPSec as well as to situate the reader about the moment that the need to have a more secure virtual environment. The study will be bibliographical on the light of Douglas Falsarella 2008, also empirical and will be done a documentary analysis. the paper is divided as follows: the study criteria will be addressed in the first group meeting and the main topics discussed; Then it will be discussed about the definitive meetings that led to the creation of the technology; Later will be approached the operation of technology, as well as its main applications in the present day and finally presented conclusive arguments that ratify the good acceptability and usability of the technology in the current scenario by large and small companies.

KEY WORDS

IPSec, Tunneling, VPN, Encryption, Security, Keys, Algorithms.

Glossário

WAN- Rede de longa distância.

Roteador- Equipamento utilizado para conectar redes distintas.

Firewall- Em português pode ser traduzido como "parede de fogo". Este dispositivo tem como objetivo proteger uma rede, aplicar uma política de segurança, funcionar como roteador, etc.

REFERENCIAS

1. COMER, E. **Interligação de Redes com TCP/IP**. Tradução de Daniel Vieira. [S.l.]: Elsevier Editora Ltda, v. 1, 2006.

2. FALSARELLA, D. Conceitos de IPSec. I**masters**, 16 jul. 2008. Disponivel em: <https://imasters.com.br/artigo/9325/redes-e-servidores/conceitos-de-ipsec/?trace=1519021197&source=single>. Acesso em: 10 set. 2017.

3. JAMHOUR, E. IPSec. **ppgia**, 02 set. 2009. Disponivel em: <https://www.ppgia.pucpr.br/~jamhour/Pessoal/Mestrado/TARC/IPsec.pdf>. Acesso em: 11 set. 2017.
4. OLIFER, N.; OLIFER, V. **Redes de Computadores:** Princípios, Tecnologias e Protocolos para o Projeto de Redes. Tradução de Dalton Conde de Alencar. 1. ed. [S.l.]: LTC - Livros Técnicos e Cientifícos Editora S.A., v. 1, 2006.

5. STALLINGS, W. **Redes e Sistemas de Comunicação de Dados:** Teoria e aplicações corporativas. Tradução de Daniel Vieira. 5ª. ed. 2005: Elsevier Editora Ltda, v. 1.

6. https://doc.pfsense.org/images/thumb/a/a4/Ipsec-s2s-vork-13.png/700px-Ipsec-s2s-vork-13.png

7. IAB (Internet Architecture Board). **Relatório do Workshop IAB sobre Segurança na Arquitetura da Internet 8 a 10 de fevereiro de 1994**. Disponível em: https://tools.ietf.org/html/rfc1636. Acesso em 10 de set. 2017.

8. Naval Research Laboratory**. Arquitetura de segurança para o protocolo da Internet** agosto de 1995. Disponível em: https://tools.ietf.org/rfc/rfc1825.txt. Acesso em 17 de outubro de 2017.

9. Naval Research Laboratory**. Cabeçalho de autenticação IP** agosto de 1995. Disponível em: https://tools.ietf.org/html/rfc1826. Acesso em 17 de outubro de 2017.

10. Naval Research Laboratory. **IP Encapsulating Security Payload (ESP)** agosto de 1995. Disponível em: https://tools.ietf.org/html/rfc1827. Acesso em 17 de outubro de 2017.

11. IETF(The Internet Engineering Task Force**). Arquitetura de segurança para o protocolo da Internet** Novembro de 1998. Disponível em: https://tools.ietf.org/html/rfc2401. Acesso em 18 de outubro de 2017.

12. Universidade Informativa do Arizona - Departamento de Ciência da Computação **O protocolo de determinação da chave OAKLEY**, Novembro de 1998. Disponível em: https://www.ietf.org/rfc/rfc2412.txt. Acesso em 18 de outubro de 2017.

13. IETF(The Internet Engineering Task Force). **Roteiro do documento de IP Security (IPsec) e Internet Key Exchange (IKE)** Fevereiro de 2011. Disponível em: https://tools.ietf.org/html/rfc6071. Acesso em 19 de outubro de 2017.