Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Fabrício Soares Martins

VPN: Protocolos, utilização e implementação segura

Rio de Janeiro

2009

Fabrício Soares Martins

VPN: Protocolos, utilização e implementação segura

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique, M.Sc, COPPE/UFRJ, Brasil

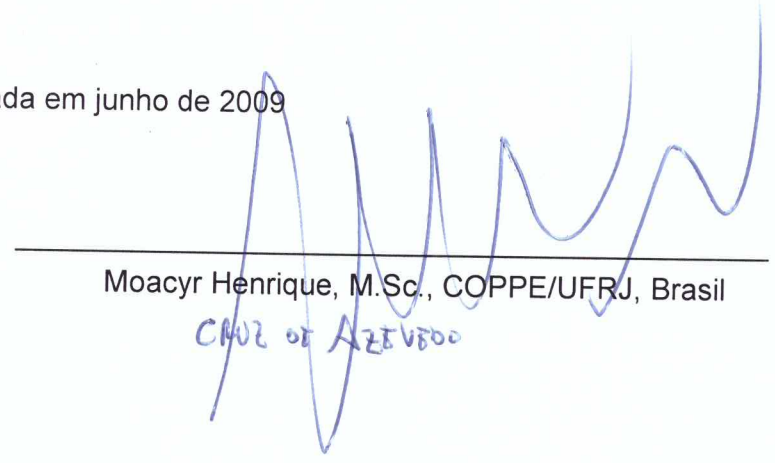
Rio de Janeiro
2009

Fabrício Soares Martins

VPN: Protocolos, Utilização e Implementação Segura

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em junho de 2009



Moacyr Henrique, M.Sc., COPPE/UFRJ, Brasil

CRUZ DE AZEVEDO

Dedico em memória do meu avô Antonio Ferreira Soares.

AGRADECIMENTOS

Agradeço a minha família e a todos os meus amigos pela e pelo apoio que sempre dispensaram.

RESUMO

MARTINS, Fabrício Soares. **VPN: Protocolos, utilização e implementação.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Este trabalho tem o objetivo de mostrar as funcionalidades, utilidades e facilidades da tecnologia VPN que cada vez mais tem sido utilizada pelas empresas de todo o mundo. O entendimento dos métodos de autenticação, protocolos, pontos fortes e fracos de todo o sistema que engloba sua utilização, constitui valiosa informação para sua implementação segura em lugares que prezam pela segurança da informação e que não abrem mão da flexibilidade de terem acesso a elas quando necessário

A economia de quem utiliza uma VPN é uma das vantagens mais marcantes, pois sua implementação não requer uma linha usada para interligar os pontos desejados. Ela própria faz uma simulação de uma Rede Privada na Rede Pública que conhecemos como internet.

Como o acesso à internet está cada vez mais barato e usual, soluções como a VPN que conseguem garantir privacidade e segurança sobre um meio de acesso público complexo (com várias ramificações, cabos, fibra óticas, redes wireless, roteadores etc), são cada vez mais valorizadas no mercado e importantes na agilidade e no crescimento do tráfego e acesso de informações.

ABSTRACT

MARTINS, Fabrício Soares. **VPN: Protocols, use and implementation.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

This work aims to show the features, utilities and facilities of VPN technology that has been increasingly used by companies around the world. The understanding of authentication methods, protocols, strengths and weaknesses of the system which includes its use is valuable information for its implementation in safe places that value for the security of information and not open-hand the flexibility of having access to them when required.

The economy of those who use a VPN is one of the most significant advantage, because its implementation does not require a line used to link the desired points. Itself is a simulation of a Private Network in public what we know as the Internet.

As Internet access is becoming cheaper and more commonplace, such as VPN solutions that can ensure privacy and security on a complex means of public access (with several branches, cable, fiber optics, wireless networks, routers, etc.) are increasingly most valued and important in the market agility and growth of traffic and access of information.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Uma Rede Privada Virtual (VPN) é uma rede de comunicação privada montada em cima de uma rede de comunicação pública através de protocolos padrão, não necessariamente seguros.

Antigamente existia uma divisão entre redes públicas e privadas. Uma rede pública era uma larga coleção de computadores sem correlação que trocavam informação mais ou menos livremente um com o outro.

Uma rede privada é composta por computadores de uma mesma organização que compartilham informações específicas com cada um dos outros.

Uma rede local (LAN) e uma rede geograficamente distribuída (WAN) são exemplos de uma rede privada e pública respectivamente.

Com a VPN essa separação praticamente acabou. VPNs permitem a criação de uma rede privada segura sobre a rede pública. Isto é feito através de criptografia, autenticação, tunelamento de pacotes e firewalls.

Dessa maneira, um sistema de comunicação por VPN tem um custo de implementação e manutenção muito baixos, possibilitando sua larga utilização.

Um exemplo de economia é sua utilização para trafegar Voz sobre IP (VoIP) reduzindo assim gastos com ligações interurbanas ou internacionais.

Entretanto, alguns cuidados devem ser tomados ao implementar uma VPN. Deve-se conhecer os pontos vulneráveis de implementação e funcionamento para evitar que dados particulares importantíssimos caiam em domínio público.

2 CONCEITO

A VPN, além de ser uma rede de comunicação privada montada em cima de uma rede de comunicação pública através de protocolos padrão, pode ser analogamente comparada a uma ligação por um túnel entre duas pontas que desejam trocar informações entre si sem que ninguém veja o conteúdo.

Os principais elementos de uma conexão VPN são o *tunelamento,* que é a forma com que os dados trafegam pela VPN; *autenticação das extremidades,* que garante a autenticidade de usuários válidos através de algoritmos tipo *hash* (como o MD5); e o *transporte subjacente,* que adiciona alguns campos ao protocolo IP que historicamente não é muito seguro.

A VPN é uma extensão da rede interna utilizando os meios físicos que não dispõe (meio público) para alcançar seu meio comum (sua rede privada).

Esse meio geralmente está associado à Intranet da empresa que possui o conteúdo sensível a ser trafegado pela VPN. Daí a necessidade de uma implementação de VPN segura.

2.1 SURGIMENTO DE INTRANETS

As empresas têm utilizado portais que disponibilizam informações sigilosas para seus funcionários, coordenadores, gerentes, diretores etc, em forma de páginas web, e utilizam-se dessas páginas de uma forma participativa e colaborativa para a própria empresa, acessando essas informações confidenciais quando estão presentes na empresa.

A disponibilidade de informações na intranet geralmente gira em torno de políticas de acesso que possibilitam hierarquicamente a consulta de determinado conteúdo que não pode ser acessado, mesmo que numa mesma empresa, por qualquer funcionário.

Assim, mesmo na rede interna da empresa, existe um determinado conteúdo sensível que precisa ser protegido. Da mesma forma que quando o acesso torna-se remoto, o conteúdo não mais precisa ser protegido de determinados funcionários, mas sim dos internautas.

2.1.1 Relação VPN / Intranet

As VPNs podem ser usadas para expandir o alcance das intranets. Dadas as circunstâncias, um vendedor, por exemplo, poderia de fora da empresa consultar um banco de dados, que está disponível na Intranet da empresa, através de uma VPN.

Deste conceito originou a idéia da implementação de uma tecnologia que fosse capaz de resolver este problema. Problema porque envolve o acesso por meio físico, e não seria viável financeiramente a instalação de uma conexão ponto-a-ponto em todos os lugares em que os usuários precisariam conectar-se remotamente.

Ao utilizar o meio público esse problema é resolvido de maneira relativamente pouco custosa.

Entretanto, não haveria vantagem se qualquer um tivesse acesso a essas informações quando esses dados trafegam de maneira desprotegida pela internet.

Uma VPN bem configurada também pode evitar esse problema utilizando criptografia e autenticação na transferência de dados.

2.1.2 Riscos

Os riscos ao utilizar uma VPN para acessar dados confidenciais são os mesmos ao de utilizar um cartão de crédito com senha ao se comprar na internet.

Para empresas os riscos são mais graves: dados roubados ou apagados podem afetar a vida de muitas pessoas e custar muito dinheiro à companhia.

Como a internet é uma rede pública, sempre haverá o risco de ter alguém acessando o sistema em que se deseja proteger.

É preciso, antes de colocar dados privados acessíveis por uma VPN na internet, certificar-se de que a VPN é robusta suficiente para protegê-los.

2.1.3 O Que Proteger Na Rede

A primeira coisa que deveria ser feita é a proteção dos arquivos com informações mais relevantes e secretas nos computadores em uma rede privada, o que é muito difícil pois essas informações são geralmente solicitadas com freqüência pelas pessoas de cargos hierárquica superiores na empresa.

Dados pessoais, logins e senhas são informações muito sensíveis que precisam ter uma proteção privilegiada.

2.2 TECNOLOGIAS DA VPN

Existem várias tecnologias que a VPN usa para proteger dados que trafegam pela Internet. Os conceitos mais importantes são: firewalls, autenticação, criptografia e tunelamento.

2.2.1 Firewalls

De acordo com ZWICKY D., Elizabeth, COOPER, Simon, CHAPMAN. Brent D, um firewall é uma maneira de restringir o acesso entre a internet e a rede interna. É tipicamente instalada no ponto mais externo onde a rede interna acessa a internet. A existência de um firewall pode diminuir dramaticamente o risco de ataques externos conseguirem êxito na rede local. Um firewall pode ainda evitar que usuários da própria rede enviem dados perigosos ou sigilosos para fora.

Um firewall ajuda a prevenir ou a conter o dano causado caso haja uma tentativa de invasão, protegendo certas áreas, usando técnicas como o exame de

pacotes ou portas requisitadas de conexões abertas para decidir qual tráfego é aceito na rede.

Quase todas as tecnologias VPN não implementam firewalls diretamente, mas elas são uma parte integral da VPN. A idéia é usar um firewall para prevenir que visitantes não desejados entrem na rede.

O firewall mais comum é o de filtragem de pacote que pode ser configurado para bloquear certos tipos de endereços MAC e/ou IPs.

ZWICKY D., Elizabeth, COOPER, Simon, CHAPMAN. Brent D recomendam que o firewall deva ser encarado apenas como um componente de segurança dentro de um plano geral de política de segurança.

2.2.2 Autenticação

Autenticação é um processo que busca confirmar uma identificação digital de um usuário no sistema, normalmente no momento em que ele faz o login.

Técnicas de autenticação são essenciais nas VPNs para assegurarem que a comunicação está trocando dados com o host ou usuário correto.

A autenticação é análoga ao login em um sistema com “usuário” e “senha”. Entretanto, VPNs requerem mais autenticações para validar identidades.

Muitos sistemas de VPNs são baseadas em “sistema de troca de chaves”. As chaves são criadas através de um algoritmo de *hashing* que gera um determinado valor. A outra parte detém as chaves que gerarão seu próprio *hash* que será comparado com o enviado pelo outro equipamento. Esse valor do *hash,* se interceptado por alguém pela internet, torna-se inútil pois ele só faz sentido se essa pessoa detiver alguma parte da chave para “encaixá-lo”.

O CHAP (Challenge HandShake Authentication Protocol) é um bom exemplo de um método de autenticação que usa esse esquema. Outro sistema comum de autenticação é o R.S.A.

RSA é um algoritmo de encriptação de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da atual empresa RSA Data Security, Inc.), **R**on Rivest, Adi **S**hamir e Len **A**dleman.

A Autenticação é tipicamente feita no início de uma sessão, e randomicamente durante o seu andamento, para assegurar que nenhum intruso adentrou na conversa. A autenticação também pode ser usada para assegurar a integridade dos dados. Os dados podem ser enviados por um algoritmo de *hash* que deriva um valor que é incluído como uma verificação (*checksum*) na mensagem. Algoritmos de *hash* pegam arbitrariamente uma string grande e matematicamente a converte numa chave de tamanho fixo. Hashes são tipicamente usados para checar a validade de uma mensagem ou senha.

Qualquer desvio nessa verificação de um computador para o outro significa que os dados foram corrompidos durante a transmissão ou interceptados e modificados ao longo do caminho.

2.2.3 Criptografia Dos Dados

Criptografia (Do Grego kryptós, "escondido", e gráphein, "escrita") é o estudo dos princípios e técnicas que protegem uma informação de maneira que só o destinatário (o que detém a chave) possa decodificar seu conteúdo.

Todas as VPNs suportam algum tipo de tecnologia de criptografia. Criptografia é considerada tão essencial como é a autenticação, garantindo que os dados transmitidos sejam protegidos de “roubo” (*sniffing*). Existem dois tipos

populares de criptografia empregados em VPNs: secret key (chave secreta) e public key (chave pública).

Na criptografia de chave secreta existe uma senha compartilhada ou frase secreta sabida por todas as partes que precisam acessar a informação criptografada. Esta chave simples é usada tanto para criptografar quanto para descriptografar a informação.

Um problema de usar a chave secreta para dados compartilhados é que todas as partes que precisam acessar a informação criptografada precisa saber qual é a chave secreta. O que pode ser fácil controlar para um grupo pequeno, pode ser impossível para redes maiores. Se uma pessoa que utiliza essa chave deixar a empresa, é necessário revogar todas as chaves das outras pessoas e instituir uma nova para garantir a segurança.

Criptografia de chaves públicas envolve uma chave pública e uma chave privada. A chave pública é publicada para todos, enquanto só o receptor conhece a chave privada. Se for necessário enviar algum dado importante, esse dado é criptografado usando a chave pública. Quando a outra ponta receber esse dado, ela utilizará a sua chave privada para obter a informação descriptografada.

Dependendo do software utilizado, as chaves pública e privada podem ser bem grandes. Por causa disso, chaves privadas são tipicamente armazenadas usando o método de criptografia por chave secreta, como um DES (Data Encryption Standard) e uma senha ou uma frase que você possa lembrar. Com isso, mesmo que alguém entre no seu sistema, não poderá ver como sua chave privada se parece.

RSA é outro sistema de chave pública que é particularmente popular nos produtos comerciais. A principal desvantagem de criptografia de chave pública é que

para uma mesma quantidade de dados, o processo de criptografia é tipicamente mais lento que com a criptografia de chave secreta.

VPNs, entretanto, precisam criptografar dados em tempo real. Por causa disso, fluxos criptografados sobre a rede, como as da VPN, são criptografados usando criptografia de chave secreta com uma chave válida apenas para essa sessão de fluxo.

A sessão secreta em si (tipicamente menor que os dados) é criptografada usando uma chave pública e enviada pelo link. As chaves secretas são de tempos em tempos negociadas usando um protocolo de controle.

Existe uma proposta de um protocolo que provê uma criptografia mais forte, é o chamado IP seguro, ou IPSec. IPSec é uma série de propostas do IETF (Internet Engineering Task Force) para criar um protocolo seguro para o IPv4 e IPv6. O IPSec provê criptografia no protocolo IP em níveis maiores que os obtidos com SSL.

O IPSec criou um padrão aberto para VPNs. Atualmente, somente alguns criadores primários de VPN utilizam criptografia proprietária.

2.2.4 Tunelamento

A capacidade de criar um canal de comunicação virtual entre dois hosts cujas características são diferentes daquelas usadas no canal físico é chamada *tunneling* ou *tunelamento.*

Muitos pacotes VPNs usam tunelamento para criarem suas redes privadas como o AltaVista Tunnel, o Point-to-Point Protocol (PPTP), o Layer 2 Forwarding Protocol, e o IPSec Tunnel Mode. A VPN permite que você se conecte a uma rede remota sobre a internet, desde que seja uma rede IP. Entretanto, muitas corporações não utilizam exclusivamente o IP. Redes com servidores Windows NT utilizam NetBEUI, enquanto que servidores Novell usam IPX. O tunelamento permite

que se encapsule um pacote em outro pacote para acomodar protocolos incompatíveis.

Com o tunelamento pode-se encapsular um pacote IP dentro de outro. Isso significa que é possível enviar pacotes com códigos arbitrários e endereços de destinos sobre a Internet dentro de pacotes que são roteados pela Internet. O uso prático disso é que é possível usar os endereços reservados (que não são roteados pela internet) no espaço IP para as redes privadas de uma rede local e ainda acessar hosts pela Internet.

3 TECNOLOGIAS BÁSICAS DA VPN

Existem dois campos que competem entre si quando tratamos de conexão entre redes. O primeiro campo coloca em primeiro lugar a acessibilidade de dados em qualquer lugar disponível para o usuário. O segundo campo dá ênfase sobre a proteção dos dados em si: o conteúdo é o mais importante e precisa estar protegido para que pessoas não autorizadas não tenham acesso.

A proteção de dados privados é o coração de uma rede privada virtual e duas tecnologias relevantes (criptografia e firewalls) são o que fazem tudo isso ser possível.

3.1 INSTALAÇÃO DO FIREWALL VISANDO A SEGURANÇA DA VPN

Um firewall é um sistema que geralmente fica entre uma rede interna e o mundo lá fora, sendo um bom lugar para começar uma estratégia de segurança. Dependendo do tipo de VPN a ser utilizado, são necessárias algumas precauções de segurança no sentido de proteger determinadas portas e protocolos.

3.1.1 IPSec

O IETF desenvolveu um protocolo de segurança IP (IPSec) que é construído diretamente no protocolo IP e provê criptografia fim-a-fim para ambos IPv4 e IPv6. IPSec é um requerimento para toda implementação Ipv6 e é opcional para o IPv4. Desde que o IPv6 provê funcionalidades que não estão disponíveis no IPv4, as versões do IPSec para ambos é um pouco diferente. O IPSec vem sendo padronizado, e é suficientemente estável e padrão para as múltiplas implementações de interoperabilidade. De acordo com SCOTT, possivelmente a melhor implementação desse tipo é a implementação para Linux chamada OPENSWAN.

Pela implementação do IPSec sobre a camada IP, isso pode prover proteção para qualquer protocolo, incluindo TCP e UDP. Os serviços de segurança que o IPSec provêm são:

a) Controle de acesso

É a habilidade de estabelecer uma conexão IPSec controlada por uma política – a recusa de negociar parâmetros de segurança irá prevenir a comunicação.

b) Autenticação dos dados de origem

O receptor de um pacote pode ter a certeza de que esse pacote vem do remetente que diz que enviou.

c) Integridade da mensagem

Um intruso não pode modificar um pacote sem que isso seja notado.

d) Proteção de resposta

Um intruso não pode reenviar um pacote previamente enviado (uma cópia) de forma que isso não seja notado.

e) Confidencialidade

Um intruso não pode ler dados interceptados.

Ainda há proteções limitadas com analises de fluxo de tráfego. Em alguns casos isso impede que um intruso descubra quais hosts estão trocando dados e quais protocolos estão usando.

O IPSec é feito a partir de três protocolos, cada um dos quais é definido como um espaço de trabalho que define layouts de pacotes e tamanho de campos que possibilitam o uso de múltiplos algoritmos de criptografia. Os protocolos não definem por si só os algoritmos de criptografia que serão usados, mas é necessário que em

toda implementação seja suportado um conjunto desses algoritmos. Os protocolos que fazem o IPSec são:

a) Authentication Header (AH)

b) Encapsulating Security Payload (ESP)

c) Internet Security Association Key Management Protocol (ISAKMP)

3.1.1.1 Authentication Header (AH)

O Authentication Header (AH) provê a integridade da mensagem e da origem da autenticação dos dados. Também pode prover, opcionalmente, serviços de proteção de resposta (item 3.1.1.d).

Essa integridade protege o cabeçalho do pacote de alterações mal-intencionadas dos endereços de origem e destino. Existem exceções de parâmetros como os campos de cabeçalhos que são freqüentemente alterados pelos roteadores, como o TTL (Time to live) do IPv4 e o Hop-count do IPv6.

3.1.1.2 Encapsulation Security Payload (ESP)

O Encapsulating Security Payload (ESP) provê confidencialidade (criptografia) e proteção limitada contra análise de fluxo de tráfego. Tanto o ESP quanto o AH funcionam sobre a disponibilidade das chaves compartilhadas, mas nenhum dos dois pode movê-la de uma máquina para outra. A geração dessas chaves é de responsabilidade de um terceiro protocolo: o ISAKMP.

3.1.1.3 Internet Security Association Key Management Protocol (ISAKMP)

O ISAKMP é um protocolo para o estabelecimento de Associações de Segurança (SA) e de chaves criptográficas, em um ambiente Internet.

Ele define os procedimentos para autenticar uma comunicação entre pares, criação e gestão de Associações de Segurança.

O ISAKMP não define os algoritmos que gerarão as chaves para o AH e o ESP. O protocolo de troca de chaves da internet (Internet Key Exchange ou IKE) usa o ISAKMP com os algoritmos específicos de troca de chave para definir as chaves do AH e do ESP. Isso significa que no ISAKMP podem ser utilizados protocolos diferentes de criptografia selecionados pelo IKE.

3.1.1.4 Modos De Operação

O IPSec utiliza dois modos operacionais para AH e ESP: transporte e túnel. No modo de transporte, AH ou ESP acontecem imediatamente após o cabeçalho IP encapsular o pacote IP original. O modo de transporte trabalha somente entre hosts individuais: o pacote precisa ser interpretado pelo host que o recebe. O transporte é utilizado para proteger comunicações host-a-host. Os hosts podem usá-lo para proteger todo o tráfego para outros hosts cooperativos ou eles podem usar outro tipo de proteção de camadas específico para outros protocolos (Figura 1).

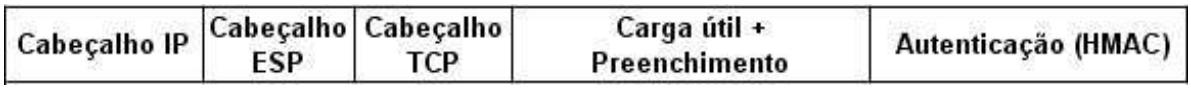


Figura 1 – Cabeçalho IPSec ESP no modo transporte

No modo de túnel todo o pacote original é encapsulado em um novo pacote, gerando um novo cabeçalho IP (Figura 2). O IPSec usa o termo gateway de segurança (*security gateway)* para qualquer componente que pode operar no modo túnel. Este termo aplica-se a todos os componentes que podem pegar pacotes IPs e enviá-los para sua origem ou seu destino, mesmo que eles sejam hosts ou roteadores dedicados. Como todo pacote IP é incluído, o destinatário pode encaminhar os pacotes até o destino final após processá-los. O modo túnel é utilizado quando dois gateways de segurança, ou um gateway e um host, se comunicam e isso é o que possibilita a construção de uma rede virtual privada usando o IPSec.

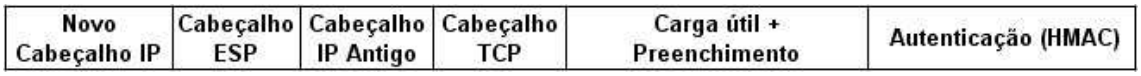


Figura 2 – Cabeçalho IPSec ESP no modo túnel

3.1.1.5 Security Parameter Index – SPI E Security Association – AS

Cada protocolo AH e ESP contém um valor de 32-bits chamado Índice do Parâmetro de Segurança, ou SPI. Este identificador é usado para distinguir a diferença entre as conversações que vão para o mesmo destino.

Cada implementação IPSec deve ser capaz de, independentemente, acompanhar os parâmetros de segurança pela combinação de um SPI, endereço IP de destino e o protocolo de segurança escolhido (AH ou ESP).

Esta combinação de parâmetros é chamada Associação de Segurança (SA). Ela é responsável pela associação específica do ISAKMP quanto à chave e escolher os parâmetros de criptografia, incluindo o SPI, para cada Associação de Segurança.

Um SA é efetivamente uma coleção de chaves criptográficas e parâmetros para uso dos AH e ESP:

a) AH

As chaves criptográficas e os identificadores do algoritmo usados para a proteção da integridade e os parâmetros de anti-resposta

b) ESP

As chaves criptográficas e os identificadores usados para criptografia, proteção de integridade e os parâmetros de anti-resposta

3.1.1.6 As Características Para A Filtragem Dos Pacotes IPSec

Os protocolos AH e ESP são implementados no topo da camada IP. O AH é o protocolo IP 51 e o ESP é o protocolo IP 50. O protocolo ISAKMP utiliza a porta 500 e o protocolo UDP para mandar e receber. Em ordem para permitir IPSec, é necessário um sistema de filtragem que possa filtrar tipos de protocolos IP. Como o

IPSec provê proteção fim-a-fim, um firewall não será capaz de modificar ou mesmo inspecionar o conteúdo de um pacote IPSec. O fluxo desses pacotes pode ser observado na tabela 1 a seguir:

Tabela 1 – Mapeamento do fluxo de pacotes em uma conversação IPSec

DIREÇÃO	ENDEREÇO ORIGEM	ENDEREÇO DESTINO	PROTOCOLO	PORTA ORIGEM	PORTA DESTINO	NOTAS
IN	EXT	INT	AH	[1]		AH entrante, clinte para servidor
OUT	INT	EXT	AH			AH entrante, servidor para cliente
IN	EXT	INT	ESP			ESP entrante, cliente para servidor
OUT	INT	EXT	ESP			ESP entrante, servidor para cliente
IN	EXT	INT	UDP	500	500	Requisição ISAKMP entrante
OUT	INT	EXT	UDP	500	500	Resposta ISAKMP
OUT	INT	EXT	AH			AH saindo, cliente para servidor
IN	EXT	INT	AH			AH saindo, servidor para cliente
OUT	INT	EXT	ESP			ESP saindo, cliente para servidor
IN	EXT	INT	ESP			ESP saindo, servidor para cliente
OUT	INT	EXT	UDP	500	500	Requisição ISAKMP saindo
IN	EXT	INT	UDP	500	500	Resposta ISAKMP

[1] AH e ESP não possuem portas de origem ou destino

3.1.1.7 Características De Proxying Do IPSec

Os protocolos AH e ESP provêm proteção de integridade das mensagens fim-a-fim que é calculada usando os dados do cabeçalho do pacote IP. Ao utilizar-se de um proxy, o cabeçalho dos dados será alterado, causando uma falha de verificação de integridade. Na teoria, é possível para a arquitetura IPSec permitir o uso de proxies intermediários nas comunicações fim-a-fim, desde que eles possam participar na negociação da integridade dos parâmetros de associação de segurança. Infelizmente, os detalhes desse funcionamento ainda não foram definidos e não é possível utilizar o IPSec através de proxies.

3.1.1.8 Características De Tradução De Endereços De Rede (NAT) Do IPSEC

NAT ou Network Address Translation permite o uso de uma gama de endereços IPs (endereços reservados) para uma rede interna e outra gama diferente (IPs válidos por exemplos) quando é preciso comunicar-se com redes externas.

O NAT por si só, não provê nenhuma segurança, mas força a passagem das conexões por um ponto de tradução de endereços. Neste caso, como o firewall, o NAT acaba fazendo um trabalho de roteamento, não só enviando pacotes como modificando-os. Quando uma máquina interna manda um pacote para fora, o NAT modifica a origem deste pacote para fazer parecer que ele vem de um endereço válido. Quando uma máquina externa manda um pacote para a rede interna, o NAT modifica o endereço destino para torná-lo visível no endereço interno correto (Figura 3). O NAT ainda pode modificar o número das portas origem e destino.

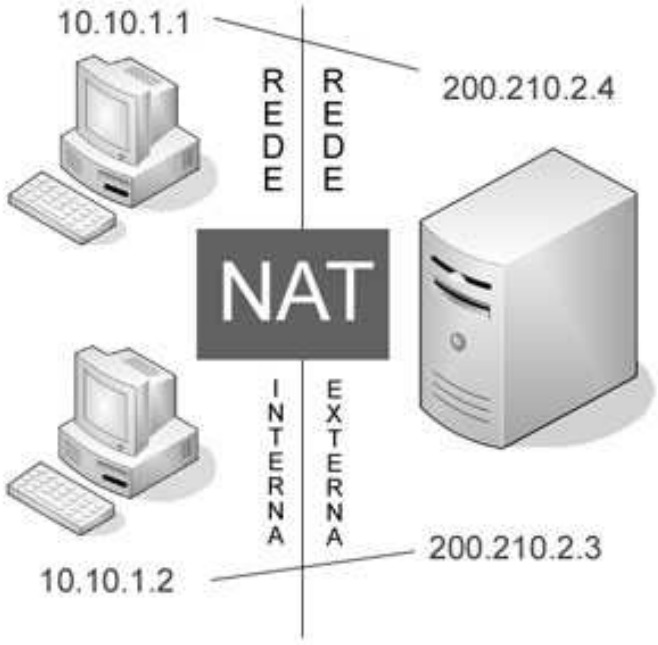


Figura 3 – Tradução de endereço de Rede (NAT). O IP 10.10.1.1 é traduzido para 200.210.2.4 e o IP 10.10.1.2 para 200.210.2.3 e vice-versa

Ambos os protocolos AH e ESP incluem proteções da integridade da mensagem para todo o pacote, incluindo o cabeçalho. Se for modificado o pacote como um todo, mesmo uma alteração no cabeçalho do endereçamento origem ou destino, isso tornará o pacote inválido.

Por isso, é impossível fazer NAT utilizando-se AH ou ESP. Entretanto é perfeitamente possível fazê-lo em pacotes que estão sofrendo tunelamento no AH ou ESP, ou seja: os pacotes dentro do túnel não sofrem alteração de cabeçalho, como ao utilizarmos o NAT alterando o IP origem, o que causaria falha no AH.

3.1.2 Serviço De Acesso Remoto (Remote Access Service - RAS)

O Serviço de Acesso Remoto, ou RAS é composto de bancos de linhas telefônicas que atendem *ondemand* por conexões de usuários remotos ou redes. Pode abranger um servidor terminal com muitos modems para um servidor RAS com linhas de entradas chamadas PRIs (PRIs são linhas digitais T1 divididas em canais para ISDN 23 ou conexões por modem). A figura abaixo mostra uma solução simplificada RAS, com um servidor RAS, redes conectadas e usuários.

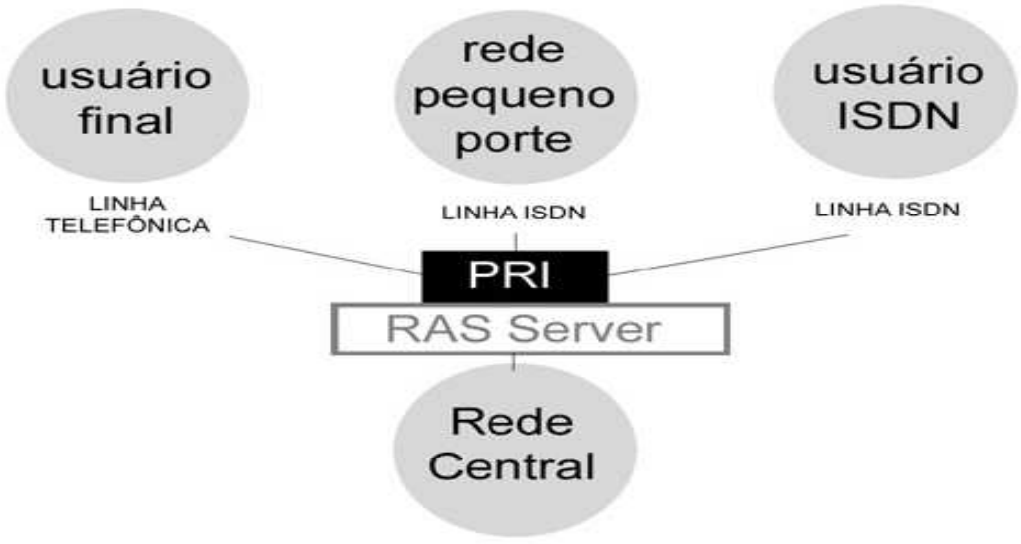


Figura 4 – Exemplos de conexões com um servidor RAS através de PRIs

O serviço de acesso remoto da Microsoft (RAS) oferece uma interface consistente para o usuário para uma larga variedade de protocolos usados para conectar uma máquina numa rede externa. Não é um serviço singular do ponto de vista de um firewall, mas múltiplos serviços diferentes.

O RAS pode ser usado em dois modos diferentes. Em um modo o cliente RAS acessa apenas o servidor RAS; no outro modo o servidor RAS atua como roteador e o cliente RAS tem acesso a toda rede. Permitindo acesso apenas para o servidor RAS, há um controle maior sobre o cliente, mas não provê muita funcionalidade.

Os clientes RAS podem usar diferentes protocolos para conectarem-se aos servidores RAS. Originalmente o RAS foi usado para suportar modems e conexões similares de baixo nível, pois suporta o uso de PPP sobre uma variedade de transportes diferentes, incluindo os mais populares modems, ISDN e X.25. Entretanto, agora o RAS é usado com freqüência para construir redes privadas virtuais (VPNs), usando protocolos de tunelamento ponto-a-ponto (PPTP), ou no Windows 2000 e posteriores, o Protocolo de transporte da camada 2 (Layer 2 Transport Protocol – L2TP).

As VPNs são mais complexas. O conceito de VPN permite usuários ou redes acessarem recursos privados centrais de rede via a internet. Existem três soluções básicas que copiam as implementações do RAS: point-to-network (um host se conecta a uma rede), network-to-network (uma rede se conecta a outra) e a solução integrada.

De acordo com SCOTT, Charlie, WOLFE, Paul, ERVWIN Mike, a solução point-to-network vai substituir o RAS como método de conexão primária para o usuário comum. Em vez de ligar e conectar-se a um ponto central RAS, o usuário

discará para um provedor de internet e se conectará a rede privada via algum protocolo seguro como o SSH, PPTP, L2TP etc.

A solução network-to-network é similar exceto que a rede remota conecta-se ao provedor (ISP) e envia sua conexão privada para um firewall central ou um servidor VPN equipado com um protocolo seguro.

A solução integrada é geralmente: servidores VPN, softwares de firewall, ou hardwares dedicados, ou a combinação dos três que permitem ambos rede e usuário final se conectarem na rede privada.

3.1.3 Protocolo De Tunelamento Ponto-A-Ponto (Point-To-Point Tunneling Protocol - PPTP)

O PPTP é um protocolo de encapsulamento baseado no Protocolo ponto-a-ponto (PPP) e o protocolo genérico roteado de encapsulamento (Generic Routing Encapsulation protocol - GRE). O PPP foi originalmente desenhado para facilitar o uso do IP e protocolos similares sobre conexões discadas e prover uma maneira geral de encapsular protocolos no nível IP. PPTP é uma extensão do PPP que pega pacotes PPP, criptografa-os e encapsula-os em pacotes GRE.

Como o PPP suporta encapsulamento de múltiplos protocolos, também o faz o PPTP (Figura 5). Ele é mais comumente usado para prover redes privadas virtuais, fazendo o tunelamento IP sobre IP. Mas também é usado para fazer o tunelamento de protocolos que não são IP como o IPX.

Figura 5 – Encapsulamento PPTP de um pacote TCP

Para que haja os túneis PPTP de pacotes pela Internet é necessário que exista uma conexão no nível IP entre os hosts. Em muitas situações essa conexão permite que os hosts sejam atacados usando outros protocolos. Nessa instância, se for o caso do uso do PPTP em uma rede privada virtual pela Internet, os hosts que têm algum tipo de conexão internet têm todas as vulnerabilidades normais de hosts conectados na grande rede. É necessário desabilitar todo tráfego de conexões que não sejam PPTP ou proteger as máquinas de outra maneira. De acordo com ZWICKY D., Elizabeth, COOPER, Simon, CHAPMAN. Brent D é recomendável evitar produtos PPTP que permitam tráfego “para” ou “de” em hosts que usam conexões subjacentes diretamente.

Existe uma grande controvérsia sobre a segurança do PPTP. Algumas delas vêm da fragilidade das implementações da Microsoft do PPTP, muitas já sanadas. Entretanto ainda restam algumas vulnerabilidades.

3.1.3.1 Fraquezas Do PPTP

Embora o PPTP seja um protocolo de criptografia, nem todas as partes da conversa são criptografadas. Antes de o servidor começar a aceitar pacotes GRE, há uma negociação usando o protocolo TCP. A criptografia PPTP protege a informação onde está sendo feito o tunelamento, mas não a negociação da configuração desse túnel. A negociação é feita em texto puro e inclui o endereço IP do servidor e do cliente, o nome e a versão do software utilizado sobre o cliente, o nome do usuário, e algumas vezes, a senha em hash usada para a autenticação. Toda essa informação pode ser exposta para alguma pessoa má intencionada. Essa negociação é feita antes do cliente autenticar-se, o que faz o servidor particularmente vulnerável a clientes hostis. Um intruso não precisa se autenticar

para se acoplar no servidor em negociação, consumindo recursos e potencialmente confundindo o servidor.

Em muitas versões do PPTP da Microsoft, o envio da autenticação em texto claro (sem criptografia) pode incluir o hash da LanMan (um dos formatos que a Microsoft usa para armazenar a senha do usuário) do usuário e senha, o que torna fácil a descoberta da senha por alguns programas especiais. É possível desabilitar a autenticação via LanMan e isso deverá ser feito em todos os clientes e servidores envolvidos. Isso forçará o uso de hash de senhas mais seguras na autenticação do Windows NT.

A implementação Microsoft também tem problemas com a criptografia. A Microsoft oferece dois níveis de criptografia, ambos usando o algoritmo de chaves simétricas chamado RC4. Um usa uma chave de 40 bits e o outro usa uma chave de 128 bits.

A chave de 40 bits não é muito forte para ser utilizada, mas a fraqueza da Microsoft consiste na utilização da mesma chave em várias sessões de usuário. Quanto mais tempo a mesma chave é utilizada, mais forte ela precisa ser.

Quando a chave de 128 bits é utilizada a Microsoft baseia-se na senha do usuário e num pseudo número randômico que é diferente para cada conexão. Esta foi uma grande implementação pois, utilizando a senha do usuário, reduz o número de prováveis chaves, tornando importante para o PPTP que os usuários tenham boas senhas.

Muitas implementações de PPTP, incluindo a da Microsoft, são susceptíveis a problemas com negociações de controle. Essas negociações ocorrem antes da autenticação do cliente, o que significa que qualquer intruso pode mandá-las. É extremamente importante que os servidores sejam hábeis para lidar com

negociações ruins, mas muitos servidores travam quando recebem negociações modificadas para serem inválidas.

A Microsoft oferece uma opção para controlar o acesso PPTP via origem do endereçamento IP, que é reforçado no túnel GRE e não na negociação baseada em TCP. Se for feita uma conexão PPTP em endereços conhecidos, é possível proteger os servidores PPTP colocando um filtro de pacotes à sua frente.

3.1.3.2 Características Para Um Filtro De Pacotes Do PPTP

A negociação PPTP acontece via TCP na porta 1723. O túnel é baseado em GRE, em que o protocolo é o 47, e usa o protocolo GRE hexadecimal 880B (indicando que estes pacotes tunelados são PPP).

A tabela 2 a seguir mostra um fluxo de uma conversação PPTP, aonde o pacote GRE do cliente leva informações sobre o túnel e o servidor responde. O servidor e o cliente configuram o túnel através das portas >1023 e 1723 utilizando-se os protocolos GRE e TCP. Todo esse fluxo de configuração não é criptografado, por isso é uma parte sensível no processo.

Tabela 2 – Mapeamento do fluxo de pacotes em uma conversação PPTP

DIREÇÃO	ENDEREÇO ORIGEM	ENDEREÇO DESTINO	PROTOCOLO	PORTA ORIGEM	PORTA DESTINO	ACK	NOTAS
IN	EXT	INT	GRE	[1]	[1]	[2]	Dados do túnel, cliente externo para o servidor interno
OUT	INT	EXT	GRE	[1]	[1]	[2]	Resposta do túnel, servidor interno para o cliente externo
IN	EXT	INT	GRE	>1023	1723	[3]	Requisição de configuração, cliente externo para o servidor interno
OUT	INT	EXT	TCP	1723	>1023	Sim	Resposta de configuração, servidor interno para o cliente externo
OUT	INT	EXT	GRE	[1]	[1]	[2]	Dados do túnel, cliente interno para o servidor externo
IN	EXT	INT	GRE	[1]	[1]	[1]	Resposta do túnel, servidor externo pra cliente interno
OUT	INT	EXT	TCP	>1023	1723	[3]	Requisição de configuração, cliente interno para servidor externo
IN	EXT	INT	TCP	1723	>1023	Sim	Resposta da configuração, servidor externo para cliente interno

[1] GRE não tem portas. GRE possui tipos de protocolos, e o tipo do PPTP é 880B

[2] GRE não tem um equivalente para o ACK

[3] O ACK não é enviado no primeiro pacote (estabelecendo conexão), mas será enviado nos demais

3.1.3.3 Características De Proxying Do PPTP

Na teoria, é possível fazer proxy no PPTP ao encontrar um sistema de proxy que aceite GRE. Um sistema de proxy não poderia aplicar muita segurança pois todo o tráfego está criptografado. A única coisa que um proxy poderia fazer é proteger o sistema contra ataques no servidor PPTP durante a fase de negociação do protocolo.

3.1.3.4 Características De Tradução De Endereços De Rede (NAT) Do PPTP

Em geral, traduções de endereços de rede não interferem no PPTP. É necessário um sistema de tradução de endereços de rede que suporte GRE, assim como TCP e UDP. O NAT não permitiria que fosse usado PPTP com duas redes que

usam o mesmo espaço de endereçamento, porque o endereço original estará visível uma vez que o encapsulamento PPTP é removido.

3.1.4 Protocolo De Transporte Na Camada 2 (Layer 2 Transport Protocol – L2TP)

O protocolo de transporte na camada 2 (L2TP) é outro exemplo de protocolo ge de encapsulamento criado para permitir um túnel IP na rede. Como o PPTP, é uma extensão do PPP. Existem duas grandes diferenças entre PPTP e L2TP. Primeiro, o PPTP sempre funciona no topo do IP pois é necessário que se tenha uma conexão IP de algum tipo. O L2TP pode rodar sobre um número de protocolos diferentes, incluindo linhas telefônicas (como o PPP). Segundo, o PPTP é um protocolo de criptografia que não criptografa tudo exceto a negociação inicial. O L2TP não é um protocolo de criptografia; ele não criptografa o corpo da mensagem. Por outro lado, o L2TP faz mútua autenticação nas negociações iniciais e é capaz de ocultar a informação da negociação inicial.

O L2TP é normalmente utilizado em conjunto com o IPSec que pode prover a criptografia. O resultado é uma pilha pesada de camadas de protocolos, como afirma SCOTT, Charlie, WOLFE, Paul, ERVWIN Mike.

3.1.4.1 Características Para Um Filtro De Pacotes Do L2TP

Quando o L2TP está na camada de cima do IP utiliza o protocolo UDP na porta 1701. Entretanto, em muitas implementações, o L2TP é atualmente transmitido sobre IP via IPSec, usando encapsulamento do UDP.

A tabela 3 a seguir mostra o fluxo de uma negociação L2TP que utiliza o protocolo UDP sem criptografia. Um pacote requisitante de conexão do cliente chega ao servidor na porta 1701 que responde estabelecendo a conexão do túnel.

Tabela 3 – Mapeamento do fluxo de pacotes em uma conversação L2TP

DIREÇÃO	ENDEREÇO ORIGEM	ENDEREÇO DESTINO	PROTOCOLO	PORTA ORIGEM	PORTA DESTINO	NOTAS
IN	EXT	INT	UDP	>1023	1701	Cliente externo para servidor interno
OUT	INT	EXT	UDP	1701[1]	>1023	Resposta, servidor interno para cliente externo
OUT	INT	EXT	UDP	>1023	1701	Cliente interno para servidor externo
IN	EXT	INT	UDP	1701	>1023	Resposta, servidor externo para cliente interno

[1] O padrão não obriga que os servidores L2TP retornem pacotes da porta 1701; eles precisam receber pacotes na porta 1701, mas podem enviá-los por outra porta. Muitos servidores mandam pacotes pela porta 1701 para simplificar as interações com o NAT e o filtro dinâmico de pacotes.

3.1.4.2 Características De Proxying Do L2TP

É possível utilizar um sistema de proxy com o L2TP desde que esse sistema suporte o protocolo UDP. Se o L2TP não estiver criptografado não é seguro afirmar o que o proxy fará. Se estiver criptografado o proxy não terá como saber o que está acontecendo para aplicar uma segurança extra.

3.1.4.3 Características De Tradução De Endereços De Rede (NAT) Do L2TP

Em geral, o NAT não interfere no uso do L2TP. A tradução de endereço de redes não esconderá nenhuma informação quando usada com o L2TP. Também não poderá ser usada com L2TP entre duas redes que utilizam o mesmo espaço de endereço, porque o endereço original ficará visível uma vez que o encapsulamento L2TP for removido.

Se for usada uma implementação L2TP onde o ponto final envia resposta por portas randomicamente escolhidas, que não a 1701, poderá haver dificuldade para conseguir as respostas através do sistema de tradução dos endereços. O sistema de tradução não reconhecerá os pacotes recebidos porque a nova porta origem não é a mesma da anterior especificada na porta de destino.

4 IMPLEMENTAÇÕES DE VPN

Nesta seção será abordada a instalação de alguns softwares de VPN em sistemas operacionais e arquiteturas diferentes.

4.1 OPENSWAN

O Openswan é um projeto de código aberto de IPSec para o sistema operacional Linux (http://www.openswan.org). Foi um código continuado a partir do velho FreeS/WAN. É necessário um kernel igual ou superior ao 2.2 para a instalação. Neste exemplo é utilizado o *kernel 2.6* com *o Debian Etch*.

Com o utilitário *apt-get* foi instalada a versão pré-compilada dos pacotes com o comando:

```
# apt-get install openswan openswan-modules-source linux-patch-openswan

Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  ipsec-tools libcurl3 libgmp3c2 linux-patch-openswan openswan
  openswan-modules-source
Suggested packages:
  libcurl3-gssapi curl
Recommended packages:
  kernel-package linux-source
The following NEW packages will be installed:
  freeswan freeswan-modules-source ipsec-tools kernel-patch-freeswan libcurl3
  libgmp3c2 linux-patch-openswan openswan openswan-modules-source
0 upgraded, 9 newly installed, 0 to remove and 17 not upgraded.
Need to get 3494kB of archives.
After unpacking 10.5MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Continuando com a instalação:

As figuras 5 e 6 referem-se a encriptação oportunística que possibilita a um sistema, quando conectado a outro, tentar criptografar o canal da comunicação voltando a ser uma conexão não criptografada se não tiver sucesso.

Esse método não requer nenhuma pré-configuração entre os dois sistemas. Este modo não provê um forte nível de segurança na autenticação.

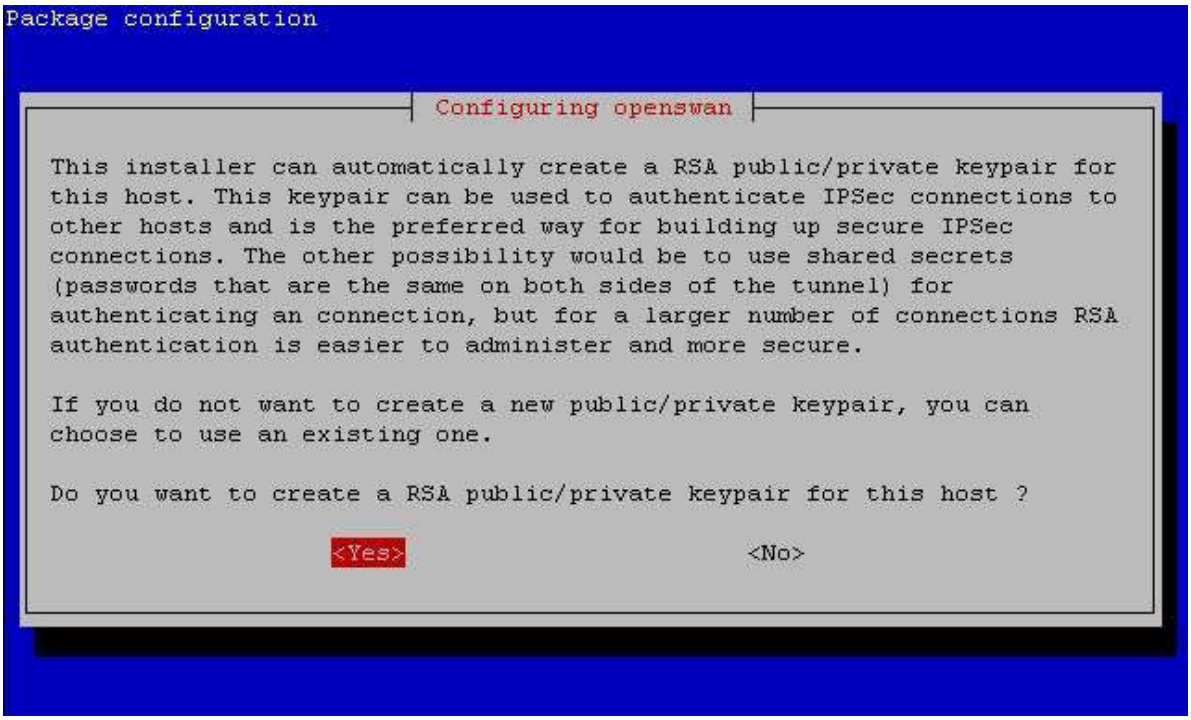


Figura 6 – Tela de configuração do Openswan sobre criação de chave RSA

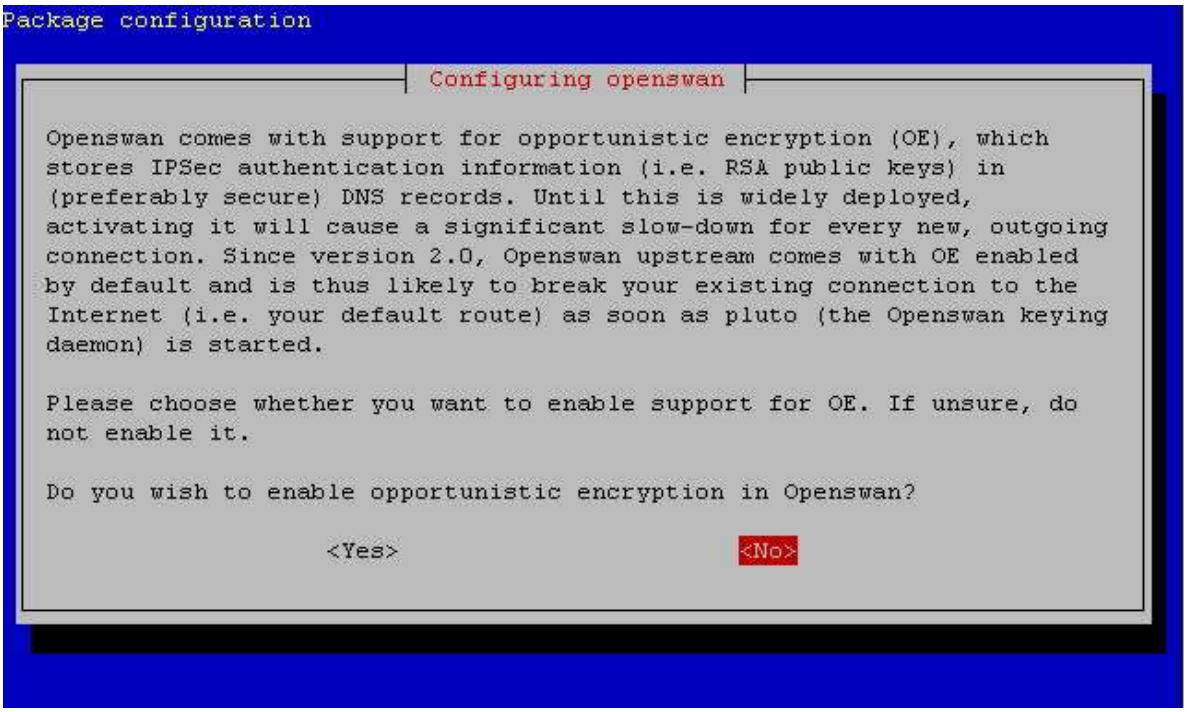


Figura 7 – Tela de configuração do Openswan sobre a encriptação oportunística

Setting up ipsec-tools (0.6.6-3.1etch1) ...

Setting up openswan (2.4.6+dfsg.2-1.1) ...
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/ipsec.d/private/suachave.pem'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:
Successfully created x509 certificate.

Disabling opportunistic encryption (OE) in config file ... already disabled

ipsec_setup: Starting Openswan IPsec 2.4.6...
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/net/key/af_key.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/net/ipv4/ah4.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/net/ipv4/esp4.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/net/ipv4/ipcomp.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/net/xfrm/xfrm_user.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/crypto/sha1.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/crypto/des.ko
ipsec_setup: insmod /lib/modules/2.6.8-3-686/kernel/arch/i386/crypto/aes-i586.ko

Setting up freeswan (2.04-14) ...
Setting up openswan-modules-source (2.4.6+dfsg.2-1.1) ...
Setting up freeswan-modules-source (2.04-14) ...
Setting up linux-patch-openswan (2.4.6+dfsg.2-1.1) ...
Setting up kernel-patch-freeswan (2.04-14) ...
server:/tmp#

Se não estiver utilizando um firewall, é recomendado desabilitar o redirecionamento de ICMP para evitar ataques de redirecionamento de rotas, com o comando:

echo ‘0’ > /proc/sys/net/ipv4/conf/all/send_redirects
echo ‘1’ > /proc/sys/net/ipv4/ip_forward

O Redirecionamento ICMP para rotas pode ocasionar falhas de roteamento nas VPNs criadas, podendo mesmo ser alvo de ataques do tipo man-in-middle

Para a criação de uma chave primária:

```
# ipsec newhostkey –output /etc/ipsec.secrets –hostname seuhostname

# chmod 600 /etc/ipsec.secrets
```

Geração de uma chave compatível com o Windows:

```
# openssl pkcs12 -export -in certs/suachave.pem -inkey private/suachave.pem -certfile
/home/ssl/chavedohostclient.pem -out certs/chavedohostclient.p12
```

4.2 STRONGSWAN

StrongSwan é um projeto OpenSource de uma implementação IPsec para o sistema Linux. É baseado no projeto descontinuado chamado FreeS/WAN e em seu patch do X.509 que foi desenvolvido em 2005.

De acordo com o site oficial, o foco do projeto está em três premissas:

a) Simplicidade da configuração
b) Criptografia forte e métodos de autenticação
c) Poderosas políticas do IPSec suportando grandes e complexa redes de VPN

Foi utilizado o Linux Ubuntu Server 8.02, e a instalação ocorreu com o comando:

```
$ sudo apt-get install strongswan
```

Após esse simples comando, o sistema instalará o software com os arquivos de configuração no /etc, para ser configurado de acordo com as necessidades do cenário que se deseja alcançar.

5 CONCLUSÃO

A importância de uma VPN nos dias de hoje e a escolha certa da tecnologia a ser utilizada é fundamental para o sucesso corporativo nos sentidos de comunicação, facilidade, economia e segurança.

A economia de quem utiliza uma VPN é uma das vantagens mais marcantes, pois sua implementação não requer uma linha dedicada usada para interligar os pontos desejados. Ela própria faz uma simulação de uma Rede Privada na Rede Pública que conhecemos como internet.

Com várias opções disponíveis, todas com suas vantagens e desvantagens é vital o estudo minucioso do cenário a ser utilizado para ser adotada uma medida de segurança condizente com o conteúdo a ser protegido.

Os detalhes de sua implementação como criptografia, firewall e políticas de segurança são cruciais para o sucesso de uma implementação correta de qualquer software escolhido e qualquer sistema operacional.

6 BIBLIOGRAFIA

OPENVPN.NET. **An Open Source SSL VPN Solution by James Yonan.** Disponível em http://openvpn.net. Acesso em 10 out. 2007

IETF.ORG. **Security Architecture for the Internet Protocol.** Disponível em http://www.ietf.org/rfc/rfc2401.txt. Acesso em 10 out. 2007

ZWICKY D., Elizabeth, COOPER, Simon, CHAPMAN. Brent D. **Building Internet Firewalls, Second Edition**. O'REILLY 2000

SCOTT, Charlie, WOLFE, Paul, ERVWIN Mike. **Virtual Private Networks, 2nd Edition**. O'REILLY 1998

TANENBAUM, A. **Redes de computadores**. Rio de Janeiro: Campus 2003

TKOTZ, Viktoria. **Criptografia – Segredos Embalados para Viagem.** Novatec Editora 2005

WIKIPEDIA.ORG. **RSA, Wikipedia**. Disponível em http://pt.wikipedia.org/wiki/RSA. Acesso em 10 out. 2007