Uma análise de soluções VPN em redes corporativas de alta capilaridade

Robledo de Andrade e Castro

Trabalho Final de Mestrado Profissional

Instituto de Computação
Universidade Estadual de Campinas

Uma análise de soluções VPN em redes corporativas de alta capilaridade

Robledo de Andrade e Castro[1]

Outubro de 2004

Banca Examinadora:

- Prof. Dr. Paulo Lício de Geus (Orientador)
- Prof. Dr. José Alfredo Covolan Ulson
  Departamento de Engenharia Elétrica, UNESP
- Prof. Dr. Célio Cardoso Guimarães
  Instituto de Computação, UNICAMP
- Prof. Dr. Edmundo R. M. Madeira (Suplente)
  Instituto de Computação, UNICAMP

[1]**Financiado pelo Grupo DPaschoal**

Substitua pela ficha catalográfica

Uma análise de soluções VPN em redes corporativas de alta capilaridade

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Robledo de Andrade e Castro e aprovada pela Banca Examinadora.

Campinas, 15 de Outubro de 2004.

Prof. Dr. Paulo Lício de Geus (Orientador)

Dissertação apresentada ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Substitua pela folha com a assinatura da banca

À minha esposa Rita.
Se cheguei até aqui, foi porque tive alguém ao meu lado incondicionalmente,
me ajudando a superar todas as dificuldades.
Essa vitória é nossa.

"Mesmo as noites totalmente sem estrelas podem
anunciar a aurora de uma grande realização."
(Martin Luther King)

"Aquilo que aprendemos, vale bem mais do que aquilo que nos ensinam."
(Alex Periscinoto)

Agradecimentos

Sobretudo a Deus e a Nossa Senhora Aparecida que sempre guiaram meus passos e ouviram minhas preces.

Aos meus pais e minha irmã, que torceram e sofreram junto comigo até o fim de mais este passo em minha vida. Amo vocês!

Ao meu orientador Prof. Dr. Paulo Lício de Geus, pela oportunidade e orientação.

A uma grande pessoa que tive oportunidade de conhecer nesse Mestrado, e foi o grande responsável pela conclusão deste trabalho. Edmar, não tenho palavras para expressar minha gratidão pela força e principalmente pela amizade (e claro à Dani por suportar sua "ausência"). Que Deus dê a todas as pessoas a mesma oportunidade que tive.

Ao Prof. Franzin do IC-Unicamp, pelas preciosas dicas, experiências e sugestões.

A Lino Sarlo, membro do IEEE, que mesmo durante a correria do lançamento de seu novo livro na área de segurança teve tempo de me disponibilizar material e dicas preciosas.

Ao Prof Juan da (PUC-Campinas), pela conversa e orientação e ao Prof Orosz (PUC-Campinas), pela força e acompanhamento.

To John Pecoraro (Netscaler VPN USA), for the papers and for being so kind and attentive.

To Paul Knight, member of IETF IPSec WG, for providing important drafts no longer available at the IETF IPSec charter and precious explanations about the IETF work in progress.

Aos meus amigos Piti / Joyce, Mari / Jô / Jú, Amauri / Kátia / Louise, Marcelo e Renata, sempre presentes.

Aos nossos grandes amigos Rogério Anzai e Rosana. Nossas conversas sempre me empurraram para frente, e me ajudaram a procurar o caminho certo.

Ao meu amigo Neto pela força, e ao Dib da Poli pela ajuda nos momentos decisivos.

To my eternal English teacher Eni Dell, for all the prayers and endless friendship. I hope to see you A.S.A.P. (that's a promise!).

Ao Dr. Hipólito, que conviveu comigo nesses momentos decisivos.

À Cláudia da secretaria pelo apoio e atenção.

À DPaschoal pelo apoio e crédito em meu trabalho.

Resumo

Com a crescente necessidade de se reduzir custos, as VPNs (Virtual Private Networks) surgem como alternativa para a comunicação corporativa. A princípio, encontram-se no mercado inúmeras soluções vendidas sob o termo VPN, baseadas em uma gama enorme de protocolos e abordagens. Na busca de uma solução viável e segura para um grande ambiente corporativo, cujo o número de filiais é fator impactante devido à alta capilaridade da rede, o conceito aparentemente simples de uma VPN pode se tornar uma fonte de preocupações no projeto de uma WAN. Esse trabalho analisa as principais abordagens e protocolos disponíveis, visando classificar de maneira clara os propósitos e limitações de cada abordagem, e foca na utilização do IPSec (IP Security) para prover uma VPN de baixo custo e principalmente segura.

O IPSec conforme apresentado na maioria dos livros parece extremamente simples de se implementar em uma WAN corporativa, mas é na verdade um protocolo complexo principalmente quando aplicado à uma rede de alta capilaridade, podendo comprometer a segurança da rede como um todo se seus conceitos não forem corretamente utilizados. O presente trabalho apresenta a justificativa da escolha do IPSec em uma abordagem CPE (Customer Premisse Equipment), e os principais problemas e soluções do protocolo em um grande ambiente corporativo.

Abstract

With the growing need for cost reduction, VPNs (Virtual Private Networks) appear as an alternative to corporate communications. There are many solutions sold in the market under the term "VPN", based on a wide range of protocols and approaches. In search of a feasible and secure solution for a large corporate environment, where the number of branches is important due to the high capillarity of the network, the apparently simple concept of a VPN can become a source of concern in a WAN project. This research analyzes the main available approaches and protocols, aiming to clarify the purposes and limits of each one and focusing on the usage of IPSec (IP Security) to provide a low cost and secure VPN.

As it is presented in most of the books, IPSec seems to be very simple to implement in a corporate WAN, but in fact it is a complex protocol, especially when implemented on a high capillarity network. It can even compromise network security if its concepts are not used in the correct way. This research also justifies the IPSec choice in a CPE (Customer Premise Equipment) approach and the main problems and solutions for this protocol in a large corporate environment.

Sumário

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

1.1 Motivação

Os profissionais da área de segurança estão enfrentando atualmente nas organizações um desafio que cresce a cada dia: fazer mais com menos. A competitividade entre as empresas e a globalização fez surgir um novo cenário de negócios, no qual a infra-estrutura de comunicação é fundamental.

Com o número de filiais crescendo cada vez mais, a necessidade de realizar negócios com diversos parceiros comerciais (fornecedores, clientes, parceiros logísticos etc.) e o crescente número de usuários móveis e trabalhadores remotos, a comunicação com a rede corporativa se torna um problema que precisa ser resolvido da melhor maneira possível, ou seja, provendo o acesso necessário à rede de qualquer ponto, de forma segura e com baixo custo.

Mas somente custo e segurança não são fatores decisivos em uma solução para comunicação corporativa. No cenário atual, com inúmeros pontos de acesso externos e a não existência de restrições geográficas, as organizações devem ter em mente que a escalabilidade da solução é muito importante, pois isto implica em redução de custos de administração e gerenciamento. Uma solução barata de comunicação entre matriz e duas ou três filiais pode se tornar extremamente cara ou ineficiente quando se eleva o número de filiais e/ou usuários para algumas centenas ou milhares.

Além disso, o alto número de parceiros de negócios faz com que facilmente se encontrem soluções variadas de comunicação, e manter infra-estruturas diferentes para cada parceiro a fim de satisfazer as necessidades de B2B com certeza não é interessante para as organizações. Aqui, pode-se identificar mais um ponto importante para uma solução ideal de comunicação corporativa: a interoperabilidade. Redução de custos em comunicações não se limita à redução de custos de aquisição e custos fixos de manutenção (como aluguéis, taxas etc.). Manter uma estrutura heterogênea com várias soluções e

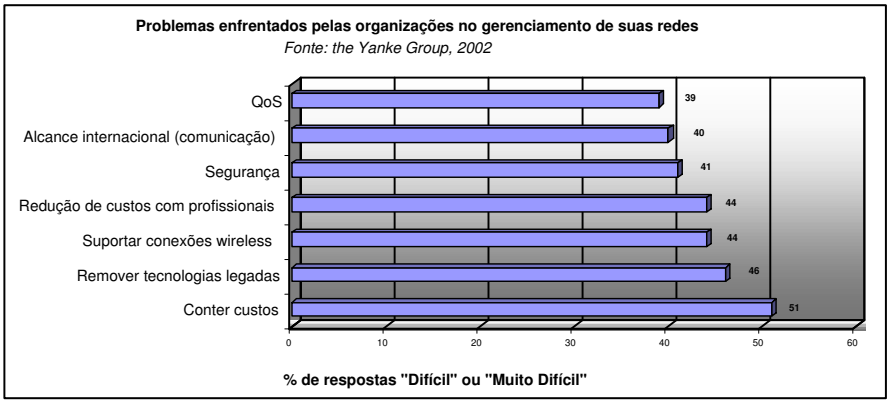

Figura 1.1: *Principais problemas relacionados à comunicação enfrentados pelas organizações.*

plataformas implica em custos adicionais de gerenciamento e administração.

Segundo uma pesquisa divulgada em outubro de 2002 [Gro02], conter os custos de comunicação referentes a redes de computadores é um dos problemas mais difíceis enfrentados pelas organizações, mais precisamente pelos executivos da área de Tecnologia da Informação, conforme mostra a Figura 1.1.

Soluções para se resolver os problemas de comunicação corporativa não faltam, como as linhas dedicadas ou *leased lines*, *frame-relay*, ATM e RAS (Remote Access Server). Essas tecnologias porém podem esbarrar em problemas de custo em um grande ambiente corporativo, ou simplesmente não vão além de necessidades específicas de comunicação, falhando por exemplo na disponibilidade de pontos de acesso em qualquer localização geográfica, dificuldades de expansão e até mesmo segurança.

Por outro lado, existe a Internet com seu uso universal, uma rede pública com presença em todo o planeta e custos de acesso bem reduzidos. Conectividade com a Internet é imperativa à quase totalidade das empresas, e não é difícil encontrar pessoas que tenham uma conexão com a rede pública em casa. Outros pontos de acesso à rede também não faltam: escolas, aeroportos, cafés, livrarias, quiosques, celulares e em uma outra infinidade de lugares, onde é possível conseguir uma conexão com a Internet a baixos custos.

Essa enorme capilaridade, aliada ao baixo custo de acesso e à utilização de um protocolo adotado pela grande maioria das empresas, o protocolo IP, faz com que a Internet seja considerada como uma alternativa do ponto de vista da comunicação corporativa, além de grande parte dos negócios feitos via Internet já serem uma realidade. O problema é que sendo uma rede pública, no sentido de prover acesso a todo e qualquer indivíduo, a Internet torna-se uma rede não confiável, sujeita a uma gama enorme de ataques, que geram por consequência grandes prejuízos às empresas. Portanto, o foco muda de "estar

conectado" para "estar conectado de forma segura", pois prover conectividade através da Internet sem uma forma efetiva de garantir a segurança faz com que a solução se torne extremamente limitada.

Vislumbrando a possibilidade de substituir as conexões dedicadas, redes privadas e *pool* de modems com linhas 0800 (RAS) para conexão remota pela comunicação via Internet, surgem as Redes Privadas Virtuais (*Virtual Private Networks*), ou simplesmente VPNs.

Na verdade, inúmeras definições podem ser encontradas para o termo VPN, como por exemplo conexões através de uma nuvem *frame-relay*. No contexto deste trabalho entretanto, o termo VPN será utilizado para designar as VPNs baseadas em IP (IP VPNs), utilizando a Internet para satisfazer as necessidades de comunicação das organizações de forma segura.

Durante a explosão do *e-commerce*, a segurança não tomou um lugar de destaque no estabelecimento das conexões com a Internet [Jas02], o que maximizou o acesso das empresas a Rede Mundial. Contudo, com o advento das VPNs, que visam prover a segurança que faltava na comunicação via Internet, as empresas podem obter uma grande economia utilizando a rede mundial para conectar filiais, parceiros e empregados de forma segura. As vendas de produtos relacionados a VPNs estão crescendo a cada dia, e as projeções são para que o número de unidades vendidas cresça ainda mais rápido que o lucro das empresas fornecedoras de soluções [Jas02], o que implica em soluções cada vez mais baratas. A utilização das VPNs ocupará uma fatia cada vez maior entre as soluções adotadas para a comunicação corporativa [Gro02].

1.2 Objetivos

Este trabalho foi inspirado na necessidade de comunicação de uma grande organização, o Grupo DPaschoal. O modelo desta empresa retrata a realidade de inúmeras organizações no mercado, com um grande número de pequenas filiais (lojas), parceiros comerciais, usuários móveis (vendedores, diretores etc) e remotos (*home-users*, analistas IT etc.), e a necessidade de prover comunicação segura e eficiente, reduzindo custos. Neste contexto, a alta capilaridade faz surgir problemas que nem sempre são de fácil solução.

Montar uma VPN entre dois pontos (matriz e uma filial) pode parecer extremamente simples, mas na verdade, o simples fato de adicionar um gateway VPN dentro da estrutura de segurança existente envolve uma série de implicações, podendo ocasionar por exemplo, violações na política de segurança definida pela empresa.

Quando se eleva o número de filiais para centenas ou milhares, o problema de integração da VPN com a arquitetura de segurança composta por Firewalls e outros dispositivos (como por exemplo o Intrusion Detection System ou IDS), toma proporções bem maiores, e começam a aparecer também problemas de desempenho, disponibilidade e ge-

renciamento. O leque de topologias também se torna grande, e cada um traz consigo uma série de implicações.

Isso faz com que qualquer organização que planeje implementar uma solução VPN em larga escala, necessite ter real noção das dificuldades e problemas que irão aparecer, os objetivos que poderá alcançar e quais os caminhos para realizar a integração da VPN com a arquitetura de segurança da organização.

A simples escolha do protocolo a ser utilizado portanto não implica em sucesso no projeto da VPN, pois um protocolo sozinho não garante a segurança do sistema [dG02a], e muito menos a aquisição de dispositivos VPN por alguns milhares de dólares irá garantir o sucesso da solução. O conceito das *Virtual Private Networks* em nada se assemelha com o conceito de *plug-and-play*.

Neste contexto, este trabalho introduz os principais conceitos de VPN, muitas vezes deixados de lado na implantação de um projeto de comunicação corporativa, e fundamental para resolver as várias situações encontradas no decorrer do desenvolvimento do projeto e da vida da WAN.

Além disso, dentre as diversas abordagens e protocolos, as principais vantagens e desvantagens são apresentadas de forma crítica, analisando-se o melhor protocolo para uma solução em um ambiente corporativo. Dentro deste cenário proposto, onde a capilaridade da rede é fator impactante, diversas soluções podem ser encontradas.

Porém, antes das soluções é necessário conhecer os potenciais problemas do cenário proposto, e fica evidente a necessidade de utilização de uma abordagem simples e eficiente para garantir um projeto de baixo custo e seguro. Este trabalho se propõe a encontrar uma solução viável para a comunicação corporativa por meio da reunião de inúmeros conceitos muitas vezes dispersos, e considerando problemas raramente abordados na literatura disponível atualmente.

1.3 Organização do trabalho

Este trabalho apresenta no Capítulo 1 qual a motivação por trás das VPNs, e introduz o objetivo do trabalho, fazendo com que o leitor buscando uma solução de comunicação segura para um ambiente corporativo, a custos reduzidos, compreenda o papel das VPNs neste cenário.

No Capítulo 2 são apresentados alguns conceitos básicos sobre VPNs mas importantes para o entendimento da tecnologia. Esses conceitos deixam margem para uma grande taxonomia de serviços que podem ser oferecidos sob o termo VPN.

Com base nestas classificações, o Capítulo 3 apresenta as diferentes abordagens para implementação de uma VPN. Esse "leque" de opções, passa pela análise de soluções oferecidas por provedores ou empresas terceirizadas, terminando por apontar o foco da abor-

dagem escolhida para este trabalho, o conceito de IP VPNs baseadas em CPE (gateway VPN dentro do site da organização).

Em seguida, no Capítulo 4 serão analisados os principais protocolos utilizados para o estabelecimento de canais seguros em IP VPNs utilizando a abordagem mencionada no Capítulo 3, que são de certa forma o coração de uma VPN, mostrando o funcionamento, vantagens e desvantagens de cada um, tentando apontar o melhor entre eles para uma solução voltada ao ambiente desejado.

No Capítulo 5, é feita uma descrição detalhada do IPSec, o protocolo que está se tornando o padrão *de facto* das VPNs e apontado no Capítulo 4 como a melhor solução existente atualmente, e incorporado de forma nativa no IPv6, de modo a familiarizar o leitor com conceitos importantes para análise dos cenários propostos.

Com base no ambiente corporativo (onde a capilaridade é muito alta, com centenas de filiais, além de parceiros e acesso remoto, resultando em um número muito grande de túneis), são apresentados no Capítulo 6 os principais problemas e considerações neste ambiente, além de uma análise das soluções adotadas atualmente, visando sempre manter a viabilidade do IPSec entre os protocolos disponíveis. O Capítulo 7 apresenta ainda algumas considerações importantes que não puderam ser abordadas de modo profundo neste trabalho.

No Capítulo 8 o trabalho se encerra com uma conclusão sobre projetos de VPN para ambientes que possuam alta capilaridade e requisitos de segurança a baixos custos, tendo as VPNs baseadas em IPSec como possível opção, além de fazer algumas sugestões para futuros trabalhos.

Estruturado desta forma, o leitor pode seguir uma sequência lógica que vai dos conceitos de VPN até os aspectos relevantes a uma solução corporativa envolvendo uma capilaridade muito alta, ou ir diretamente aos capítulos de seu interesse, caso já possua os conhecimentos apresentados nos demais.

Capítulo 2

VPN - Fundamento

2.1 Introdução

Em qualquer comunicação existente hoje, seja ela via rede de computadores ou entre seres humanos, um requisito é essencial: a privacidade. Se duas ou mais entidades estão interessadas e engajadas na comunicação, elas não vão querer que alguém "não autorizado", ou que não tenha interesse real na comunicação, participe de alguma forma. Isso exige que as entidades mantenham a comunicação privada, ou seja, é possível distinguir entre os interessados na comunicação e os demais, e manter os "demais" fora da comunicação.

Quando essa comunicação é feita em um lugar ou meio público, algum artifício deve ser usado para que somente as partes envolvidas participem, mantendo assim a comunicação de forma privada. E na Internet, uma rede pública, não é diferente. Para que se tenha uma comunicação segura entre dois ou mais pontos através de uma rede insegura, um conjunto de técnicas é utilizado de modo a tornar essa comunicação "privada", e a esse conjunto de técnicas dá-se o nome de *Virtual Private Networks* (Redes Privadas Virtuais), ou simplesmente VPNs.

Neste capítulo serão descritos os principais conceitos de uma VPN, suas vantagens, desvantagens e limitações, além de uma breve comparação com tecnologias existentes a fim de familiarizar o leitor com uma solução que vem crescendo a cada dia não só no mercado corporativo, mas no mercado de redes em geral, no que diz respeito às necessidades de comunicação segura.

2.2 O que é uma VPN?

Conforme descrito em [Tec00], o crescimento das VPNs vem esbarrando na falta de interoperabilidade das implementações, que derivam da confusão sobre o escopo e a definição das VPNs, e a confusão sobre a grande maioria de soluções que são descritas pelo termo VPN. As empresas por sua vez também ficam confusas com a variedade de soluções e tecnologias que são vendidas sob o termo VPN. Portanto, será apresentado a seguir qual o significado de VPN no contexto deste trabalho, que segue as definições descritas em [Tec00].

Como foi possível notar até aqui o principal motivador de uma VPN é o fator custo, que por sua vez é um dos alvos principais na grande maioria das empresas, não só no que diz respeito à TI. VPN é um conceito composto por duas partes: o conceito de uma rede "virtual" construída sobre uma rede ou meio compartilhado, aliada ao conceito de uma rede "privada", onde a confidencialidade dos dados e o uso exclusivo é garantido, a fim de atingir o objetivo principal descrito acima: reduzir os custos de comunicação, mantendo a segurança.

O termo *virtual network* pode ter vários significados. Um exemplo comum é encontrar-se em uma mesma LAN máquinas rodando o protocolo IP para acessar serviços TPC/IP (Telnet e SMTP por exemplo), e máquinas utilizando o protocolo IPX para acessarem servidores de arquivo Novell. Neste contexto existem duas redes lógicas (uma IP e outra IPX), mas utilizando os mesmos recursos físicos da LAN (*switches*, cabos, *routers* etc). É possível de certa forma dizer que existem duas "redes virtuais", separadas logicamente e unidas fisicamente.

No caso das VPNs, pode-se utilizar um exemplo de duas sub-redes geograficamente distantes, como a de uma matriz e uma filial, sem que haja nenhuma infra-estrutura física conectando as duas (como uma linha ou *link* dedicado). Se essas sub-redes estiverem conectadas a Internet, que é uma rede compartilhada por milhares de *Hosts*, formando outras redes e sub-redes, é possível conectar matriz e filial como uma única rede lógica através da Internet, conseguindo com isso uma rede virtual, mais rápida de implementar e a um custo bem menor que o conseguido através recursos físicos dedicados.

Surge portanto o objetivo de emular uma WAN, mas para que isso seja possível através de uma rede compartilhada o aspecto "privado" das Redes Privadas Virtuais (VPNs) é de fundamental importância. O propósito de uma rede privada é manter os dados (e o ato da comunicação) de forma confidencial, permitindo a participação somente das partes "interessadas". Isso faz com que o ganho em se usar uma rede compartilhada não seja perdido pela falta de segurança na comunicação.

Resumindo, uma VPN é uma emulação de uma WAN privada sobre uma rede compartilhada como a Internet ou mesmo *backbones* privados, que são compartilhados por

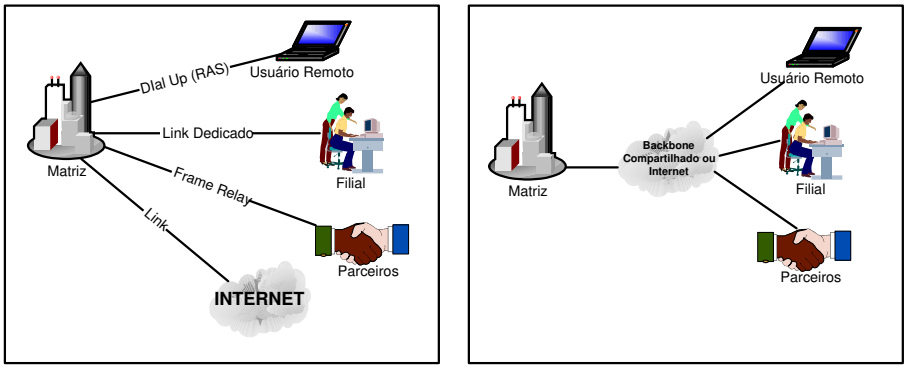

Figura 2.1: *Ambiente Corporativo e o Advento das VPNs*

vários clientes, mas a privacidade de cada "WAN virtual" é mantida.

No contexto deste trabalho, será dado enfoque ao termo VPN para VPNs baseadas em IP, que conforme definido em [Tec00], são aquelas implementadas sobre *backbones* IP, mesmo que o protocolo IP esteja rodando sobre outras tecnologias como ATM, sendo este *overlay* transparente aos serviços que rodam sobre o IP (no caso as VPNs).

2.3 A comunicação corporativa

Para atender às necessidades de negócio, as empresas investem pesado em suas redes locais. As LANs atendem às necessidades dos usuários localizados dentro do *site* da organização, mas o mercado exige cada vez mais que os empregados trabalhem remotamente, sejam eles vendedores, diretores em viagem, enfim, empregados que precisam de acesso à rede corporativa enquanto estão fora de seus locais de trabalho. Para suprir essa necessidade, bancos de modems são mantidos em um *site* (ou *sites*) da corporação, permitindo acesso via *dial-up* (RAS) aos usuários remotos.

Com o crescimento cada vez maior das corporações, no que diz respeito tanto à abrangência de mercado quanto expansão geográfica, as filiais remotas vão aumentando em um ritmo cada vez mais acelerado, e necessitam de comunicação com a matriz e/ou outras filiais. Uma das maneiras de se suprir tal necessidade é com linhas privadas ou *links* dedicados com *Frame-Relay* e ATM.

Além disso, os parceiros comerciais necessitam de comunicação e acesso restrito a dados e sistemas, alcançando o objetivo de soluções B2B (Business-to-Business), devendo ser acomodados de alguma forma nessa estrutura de comunicação. Isso sem esquecer a presença das organizações no *e-commerce* (B2C - Business-to-Consumer), fazendo a presença corporativa na Internet uma exigência.

A Figura 2.1 mostra o cenário de comunicação que existe hoje em um grande número

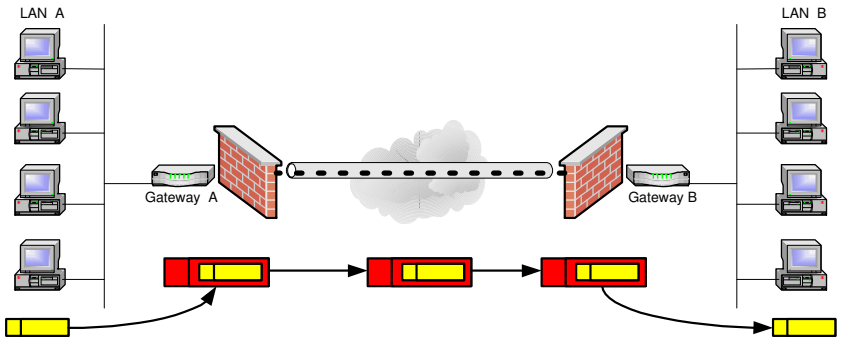

Figura 2.2: *Tunelamento de pacotes entre duas redes*

de empresas, e a proposta das VPNs para realizar as mesmas tarefas a um custo bem menor e garantindo a segurança oferecida pelos meios "antigos".

2.4 Conceitos Básicos

2.4.1 Tunelamento

Tunelamento é definido como o encapsulamento de um determinado pacote de dados (o pacote original ou *inner packet* dentro de outro pacote de dados (pacote de transporte ou *outer packet* conforme mostra a Figura 2.2, de modo que o pacote original seja invisível na rede em que o pacote de transporte será roteado.

A necessidade de tunelamento pode surgir quando não é apropriado que um determinado pacote cruze uma outra rede diretamente por inúmeros motivos, entre eles:

- O pacote original utiliza um protocolo não suportado pela rede a ser atravessada. O pacote é inserido em um pacote apto a cruzar a rede, sendo desencapsulado na outra extremidade, como ocorre por exemplo em IP sobre ATM.
- Não é seguro que o pacote original cruze a rede em claro, sendo encapsulado por outro pacote protegido por serviços de segurança, como a criptografia.

Dois componentes são necessários para se definir um túnel: os *end-points* do túnel e o protocolo utilizado para encapsular os dados que irão passar pelo túnel. Na maioria dos casos o túnel terá dois *end-points*, um que encapsula os pacotes (início do túnel) e outro que desencapsula os pacotes (fim do túnel), podendo o mesmo *end-point* ser início e fim de túneis ao mesmo tempo. No caso de *multicast*, existe um início e vários terminadores do mesmo túnel.

2.4.2 Segurança dos dados

A segurança dos dados toca em todos os pilares em que uma VPN é construída. A segurança da solução como um todo pode ser identificada pela segurança de seu elo mais fraco [Str01]. Se um elo dos componentes da solução não é seguro, a solução não pode ser considerada segura.

Confidencialidade

Levando em conta a utilização de um *backbone* não confiável (como a Internet) para a comunicação entre dois pontos, a tarefa de se interceptar uma sequência de dados torna-se relativamente simples [Edm04]. Por este motivo, os dados necessitam ser protegidos de forma a não ser possível seu entendimento por um possível "interceptador". Para esta finalidade utiliza-se a criptografia, que tem como objetivo embaralhar ou tornar os dados "não visíveis" de modo a permitir somente os pontos envolvidos na comunicação a decifrá-los.

Integridade

O fato dos dados estarem protegidos contra o entendimento do seu conteúdo através do recurso da confidencialidade, não garante que esses mesmos dados não possam ter sido alterados durante seu trajeto entre os pontos envolvidos na comunicação. Esse fato exige mecanismos que detectem qualquer alteração nos pacotes, garantindo que chegaram ao destino da mesma maneira que saíram da origem [Edm04]. É importante notar que o fato de garantir que o pacote não sofreu nenhuma alteração no trajeto entre origem e destino não implica que o mesmo esteja utilizando recursos para garantir a confidencialidade (dados não sigilosos).

Autenticidade

Além de proteger os pacotes de serem "lidos" ou alterados, é necessário que seja possível identificar que quem enviou os dados é realmente quem diz ser, e quem está recebendo também possa garantir a veracidade de sua identidade. Autenticando portanto os pontos envolvidos na comunicação, impede-se que algum usuário mal intencionado falsifique a origem do pacote ou faça se passar por um determinado destino, impedindo que um canal seguro seja estabelecido entre pontos não confiáveis [Edm04]. Além da garantia de identidade do emissor e do receptor, é importante que a solução se proteja de ataques do tipo *"replay"* [1].

[1] Ataque onde um atacante reenvia um pacote capturado a fim de afetar de alguma forma a segurança do sistema [Bel96]

2.4.3 Controle de acesso

Quando o processo de autenticação é completado, as entidades envolvidas na comunicação precisam decidir se é permitido ou não o acesso a um determinado recurso. Não basta apenas saber quem está engajado na comunicação, mas saber o que e como as entidades envolvidas podem acessar os recursos disponíveis. A esse processo dá-se o nome de controle de acesso.

O controle de acesso pode ser efetuado de duas maneiras, que serão analisadas com mais detalhes no Capítulo 6 no ambiente das VPNs:

- Nas pontas envolvidas na comunicação
- Realizado a parte por algum outro dispositivo, eximindo as entidades fim-a-fim de implementarem qualquer tipo de controle.

As decisões de controle de acesso são baseados em credenciais fornecidas de acordo com a necessidade e o tipo de aplicação. Certificados digitais por exemplo podem ser uma ótima fonte de dados a respeito de uma determinada entidade [Ste03], provendo informações a fim de enquadrar o perfil de acesso na política de segurança adotada na organização. Em resumo, a autenticação define quem está se comunicando, e o controle de acesso define a quais os recursos são permitidos o acesso das entidades envolvidas.

2.5 Modelos de Interconexão

Como foi dito, as VPNs permitem que redes sejam interligadas através de um *backbone* (rede) compartilhado, e no caso deste estudo, *backbones* IP, originando o que é chamado de IP VPNs. Na verdade, não necessariamente redes podem se conectar a redes. Um usuário com seu computador em algum ponto do planeta conectado a Internet[2] também pode ter acesso a sua rede corporativa, e essas várias maneiras de se estabelecer uma VPN são chamados modelos de interconexão.

Existem algumas maneiras de se estabelecer canais seguros para realizar tais conexões, o que será chamado aqui de tipos de túneis. A partir destes diferentes tipos de túneis, é possível definir diferentes tipos de conexão para a comunicação corporativa, em um conceito mais abstrato, como será visto a seguir.

[2]Conforme já foi dito, VPNs podem ser estabelecidas sobre qualquer *backbone* IP compartilhado. Neste trabalho, a Internet como *backbone* sobre o qual a VPN será estabelecida será amplamente utilizada como exemplo, e será alvo de estudos mais detalhados no decorrer do mesmo.

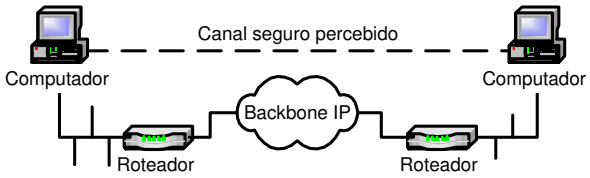

Figura 2.3: *Conexão Host-Host*

2.5.1 Tipos de túneis

Host-Host

Esta talvez seja a implementação mais simples de uma VPN, e significa o estabelecimento de um canal seguro para comunicação entre duas máquinas (*Hosts*). Um exemplo prático da utilização de uma "VPN" *Host-Host* é quando se utiliza o protocolo SSL (Security Sockets Layer) através de um *browser* como o Internet Explorer para acessar um servidor *web* dentro de uma DMZ (De-Militarized Zone) na corporação, para obter-se algum tipo de informação (ou mesmo correntistas acessando os *sites* de seus respectivos bancos). Existem dois *Hosts* (um no papel de *client* e outro no papel de *server*) fazendo uma comunicação "segura" (aqui entram outros aspectos sobre autenticação das duas pontas que não são importantes nesta exemplificação). Pode-se citar o exemplo de dois *Hosts* com suporte ao IPv6 [Hin95] estabelecendo um canal seguro entre si para troca de informações, tendo o IPSec [Atk98c] como suporte nativo em sua especificação [Cle03].

Outro exemplo seria dois servidores, um na matriz e outro na filial, que precisam sincronizar informações financeiras muito importantes. Pode-se então criar um canal seguro para este caso específico entre os servidores para que toda a comunicação seja protegida, mesmo passando através da Internet. Os dois *Hosts* podem estar inclusive na mesma LAN, mas os dados a serem trocados são extremamente confidenciais. Para evitar qualquer ataque vindo de *insiders* [dG02a], que ocupam uma parcela considerável dos ataques às redes das organizações, pode-se criar uma VPN (canal seguro) entre dois *Hosts* específicos (lembrar que uma rede é o conjunto de dois ou mais computadores que trocam informações entre si [And03]).

Host-Network

Este tipo de canal seguro parte de uma máquina e termina em um gateway VPN, que age como um *proxy* de segurança [Cle03]. Atrás deste gateway estão diversas máquinas que constituem uma ou mais LANs, que são chamadas de rede interna. A partir do túnel criado entre o *Host* e o gateway, é possível, de acordo com a política de segurança estabelecida, o *Host* remoto acessar as máquinas desta rede interna e vice-versa.

Os pacotes seguem pelo túnel até o gateway VPN onde são processados (autenticados, descriptografados, enfim, recebem o processamento necessário para saírem do túnel "desprotegidos"), e entregues ao destino final, como se o computador ou *Host* remoto estivesse fisicamente dentro da LAN, e tudo de modo transparente às aplicações.

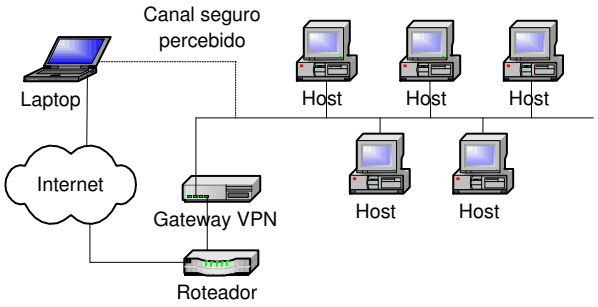

Figura 2.4: *Conexão Host-Network*

Network-Network

Neste terceiro tipo de tunelamento, duas (ou mais) LANs podem ser interconectadas através de canais seguros, formando uma WAN. Para os *Hosts* de cada rede, o tunelamento é totalmente transparente, pois é feito entre gateways nas bordas de cada LAN. Dessa forma, se um *Host* em uma rede A envia um pacote para um outro *Host* em uma rede B (ambas as redes conectadas por um canal seguro via Internet), o pacote sai totalmente desprotegido da origem até chegar no gateway da rede A, onde é processado para entrar no canal seguro.

Atravessando a Internet protegido, o pacote chega a outra extremidade do túnel (gateway da rede B), onde é processado (autenticado, descriptografado etc) e enviado dentro da rede B (novamente desprotegido) até o *Host* destino. Para ambos os *Hosts*, as operações realizadas para para que o pacote atravesse o canal seguro são totalmente transparentes, como se as duas subredes A e B fossem unidas apenas por um roteador. A Figura 2.5 mostra um modelo de tunelamento *network-network*.

2.5.2 Arquiteturas de Conexão

Conforme foi descrito acima, existem várias maneiras de se interconectar máquinas e redes através de canais seguros. É possível enxergar essa conectividade de um plano mais elevado, mais abstrato, quando se emprega esses diversos tipos de utilização de canais seguros dentro de um ambiente corporativo, que formam as arquiteturas descritas a seguir. Estas arquiteturas são nada mais que cenários encontrados no ambiente corporativo onde

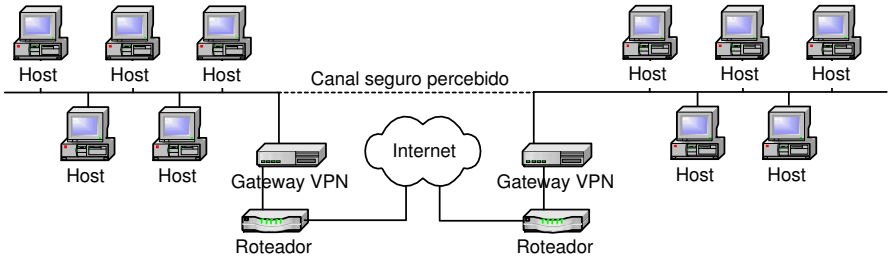

Figura 2.5: *Conexão Network-Network*

as VPNs poderão atuar na resolução dos problemas de conectividade e comunicação da organização.

Intranet Corporativa (*site-to-site Intranets*)

É possível descrever cada localização geográfica de uma empresa (escritórios, filiais, matriz etc) como um *site*. Todos esses *sites* pertencentes à mesma organização podem ter várias redes, e com o emprego das vlans (Virtual LANs) um número grande de sub-redes. Existe portanto em cada *site* uma *intranet*, que pode ser interconectada às demais por uma VPN formando uma única rede corporativa, ou mais comumente chamada de *intranet* corporativa.

Dentro de uma *intranet* corporativa é possível encontrar alguns tipos de topologias, que são as diferentes maneiras de se interconectar os diversos *sites* da organização. Basicamente a topologia de uma VPN está diretamente ligada ao fluxo de dados da corporação, ou seja, qual *site* fala diretamente com qual *site*, ou através de que *site* ou *sites* a comunicação entre duas filiais pode e/ou deve ocorrer, como será explicado na Seção 2.6.

A utilização de linhas dedicadas (que podem ser por exemplo do tipo *T-carriers*, *OC-lines*, *links* via satélite etc) é indicada para determinadas aplicações, tipicamente de missão-crítica e que exigem uma alta taxa de *throughput*, tendo em vista que uma linha dedicada possui garantia de banda passante. Com um *link* OC-3 por exemplo, uma consulta a um banco de dados entre *sites* geograficamente distantes pode parecer ao usuário como uma consulta a um banco de dados local, em relação ao desempenho.

O problema é que na maioria dos casos, a utilização de linhas dedicadas torna a infra-estrutura de comunicação extremamente cara. Com um alto número de filiais (imaginando centenas ou milhares de filiais) se torna praticamente inviável, além do custo de uma linha dedicada internacional ou mesmo nacional de longa distância ser ainda mais elevado.

É preciso analisar a necessidade de tamanha qualidade de serviço e disponibilidade, e as VPNs podem prover a conectividade que as empresas necessitam substituindo estas linhas dedicadas por conexões via Internet, além de abrir a opção para usuários remotos

acessarem a rede, o que não é possível com o uso de linhas dedicadas, resolvendo problemas de flexibilidade e escalabilidade, devido ao gerenciamento próprio das conexões e facilidade do estabelecimento de túneis, tirando-se vantagem da presença global da Internet [dG02a].

Com uma estrutura baseada em IP VPNs pode-se por exemplo criar um túnel dinamicamente para uma necessidade específica, como *backup* noturno ou uma videoconferência, e terminá-lo logo depois, flexibilizando e maximizando a utilização dos recursos, diferentemente de um PVC *Frame-Relay* por exemplo que fica com os recursos de comunicação alocados sendo eles utilizados ou não. Além disso, opções como *Frame-Relay* e mais recentemente o Multi-Protocol Label Switching, ou MPLS (que alguns autores apontam como possível e provável sucessor do *Frame-Relay* [Tec00] como será visto mais adiante), podem se tornar uma opção mais atraente no quesito custo-benefício para aplicações de missão-crítica que realmente precisam destas garantias.

Alguns aspectos sobre a utilização destas tecnologias no que diz respeito à segurança e QoS (*Quality of Service*) em soluções VPN serão detalhadas mais adiante, no Capítulo 3, quando serão analisadas as *Trusted*, *Secure*, baseadas em CPE e baseadas em rede.

Acesso Remoto (fixo e *road-warriors*)

O acesso remoto utiliza o tipo de conexão Host-*Network* para permitir que usuários que estejam fisicamente fora de seu local de trabalho (*site* da organização) possam ter acesso aos recursos da rede corporativa como se estivessem fisicamente dentro da rede, como se conectados à um *switch* dentro da LAN privada na matriz da empresa.

Tradicionalmente as empresas disponibilizam um *pool* de modems, geralmente com linhas 0800, que serão gerenciadas por um servidor RAS. Os usuários discam através de uma conexão *dial-up* utilizando a rede de telefonia alcançando o servidor RAS e consequentemente a rede da organização. Os usuários são geralmente autenticados através de *passwords*, um método de autenticação extremamente fraco e difícil de manter sob uma boa política [Sec02, Tue03], além desta disponibilidade de modems em estado de espera serem um prato cheio para ataques de *wardialing* [dG02a], que apesar de serem uma frente de batalha muitas vezes "esquecida" pelas empresas, ainda tem grande incidência, aliada ao grande número de ferramentas disponíveis que fazem o serviço sem grandes "habilidades" requeridas pelo *hacker* e o descaso ou despreparo das empresas em relação aos acessos disponibilizados via modem [Jon03].

Através do RAS os usuários pedem obter um IP da rede da organização, configuração DNS e WINS, fazer autenticação em redes específicas, entre outras características desejáveis ao acesso remoto [dRPLdG02]. Mas além do problema da segurança, existe o alto custo das chamadas, principalmente de longa distância, que devem ser feitas diretamente ao *site* da organização esteja o usuário onde estiver. Reembolsando o usuário pelas chamadas ou disponibilizando chamadas sem custo DDG, o valor para um número

elevado de acessos remotos aliado ao tempo de duração de cada chamada pode se tornar extremamente proibitivo, tendo em vista além do custo das ligações, a infra-estrutura necessária para disponibilizar um acesso via RAS, como linhas telefônicas e equipamentos para atender a essa demanda, elevada ao nível de uma grande corporação.

Pode-se dividir os usuários remotos em duas "classes distintas": O usuário fixo, que engloba os acessos de casa (*home-users*), uma única máquina em um escritório da empresa ou de um parceiro, que normalmente estarão utilizando sempre o mesmo meio e local de acesso (xDSL, *Cable Modem* etc) e os usuários móveis, também chamados de *Road-Warriors*, que são os usuários que não têm um ponto fixo de acesso, utilizam geralmente *laptops*, casos onde se enquadram vendedores, executivos em viagem, técnicos comerciais em visita etc.

Com as tecnologias disponíveis hoje para acesso a Internet, como xDSL e *Cable Modems* ou ISDN, é possível prover acesso aos usuários remotos "fixos" a custos bem baixos e com velocidade muito superior aos melhores modems com padrão v.90 e velocidade de 56 kbps. O esquema de modulação utilizado no país em conjunto com ruídos na linha podem fazer estes modems operar a velocidades de 19,6 kbps ou menos. Os usuários móveis poderão usufruir de acessos banda larga em aeroportos, cafés etc, mas tendo também disponível a opção de fazer uma ligação local (via modem) para um ISP (Internet Service Provider) qualquer e obter conectividade com a Internet. Outra vantagem seria o aproveitamento do enorme tempo que o funcionário leva no deslocamento casa-trabalho-casa, provendo a opção do mesmo trabalhar remotamente e satisfazendo interesses mútuos de empregado e empregador [Cal03].

Conectados a Internet é possível então estabelecer um canal seguro com a rede da organização e obter acesso aos recursos desejados, evitando custos com uma infra-estrutura RAS e chamadas telefônicas, além de melhoria na performance do acesso remoto. As chamadas ao *help desk* em termos de conectividade se transferem em parte ao ISP, tirando essa "carga" do *help desk* corporativo, que é responsável agora somente pelo estabelecimento do túnel até a rede da corporação [Sec02].

Aqui surge um grande desafio, que é a autenticação destes usuários, principalmente os *Road-Warriors*, pois não têm IP fixo e também não é possível utilizar métodos do tipo "*call-back*" [Sec02], além da segurança física ser difícil de implementar [dRPLdG02]. Uma série de implicações e necessidades de um acesso remoto VPN pode ser encontrados em [Edm04] e [dG02a]. Apesar do foco deste trabalho ser o modelo de VPNs "*site-to-site*", não há como deixar de abordar o acesso remoto, dando um panorama ao leitor de todos os pontos chaves para uma VPN corporativa, e sem dúvida nenhuma o acesso remoto fará parte da grande maioria das soluções e deve ser previsto na arquitetura adotada.

Extranets

Diferentes organizações têm cada vez mais a necessidade de trocar informações entre si. Um dos meios mais utilizados hoje em dia é a troca de arquivos EDI (Eletronic Data Interchange, sendo o ramo automotivo um grande exemplo de utilização), que evoluiu muito principalmente no que diz respeito à padronização, conforme encontrado nos padrões Anfavea[3] e Proceda[4]. Apesar disso, a customização de *software* e meios de proteger a troca segura dos arquivos EDI pode elevar os custos. Além disso, a evolução no processo de negócios faz com que algumas empresas necessitem de informações de uma forma mais dinâmica, e principalmente "*on-line*" de seus parceiros de negócio mais próximos (fornecedores e/ou clientes), a fim de alcançar maior competitividade no mercado. Esta competitividade exige maior agilidade na troca de informações, resultando evidentemente em maiores lucros.

Essa integração só é possível disponibilizando acesso entre redes de parceiros de negócios, o que é chamado de *extranet*, proporcionando uma verdadeira integração a fim de suprir as necessidades de B2B, como *supply chain*, vendas, suporte a clientes entre outras aplicações que são disponibilizadas em uma *extranet*.

A idéia aqui não é simplesmente disponibilizar uma aplicação *Web*, mesmo que protegida por SSL, onde qualquer um pode "bater a sua porta", tendo em vista que tal tipo de aplicação autentica somente o servidor por um meio forte de autenticação (certificados digitais), mas utiliza geralmente um método de autenticação do cliente extremamente fraco, como um *login* e uma senha [Sec02], além de geralmente ser restrito à aplicações específicas. Uma VPN para um cenário de *extranet* propiciará a comunicação de dados sensíveis somente entre os próprios parceiros, gerando ganhos em segurança com relação a um simples *site Web* e em agilidade na informação com relação ao processo de EDI, sendo possível uma verdadeira integração entre sistemas no caso de parceiros de negócio muito próximos (como Goodyear e DPaschoal, ou *Joint-Ventures* etc.), provendo por exemplo acesso a uma determinada base de dados a vários parceiros, deixando a interface da aplicação por conta de cada um, flexibilizando a integração e não forçando um determinado tipo de plataforma de desenvolvimento de *software* (ou mesmo a aplicação em si).

Além disso, a possibilidade de utilizar a Internet faz com que a integração destas organizações fique extremamente fácil e ágil, tendo em vista a conectividade com a Internet presente na maioria (senão totalidade) das empresas interessadas neste tipo de integração via *extranet*.

Neste cenário é possível prover um acesso VPN a um parceiro tanto via conexão *site-to-site* ou via Acesso Remoto, dependendo da necessidade de cada organização em especial.

[3]Disponível em www.anfavea.com.br
[4]Informações em www.proceda.com.br

Aqui fica evidente a redução de custos e o ganho em agilidade, estabelecendo e desconectando túneis conforme a necessidade da comunicação, acompanhando a rápida mudança das necessidades de negócios e trocas de parceiros comerciais, o que se torna muito mais difícil com linhas ou *links* dedicados. É importante frisar no entanto que a VPN deve prover um controle de acesso muito bem apurado, além de um bom método de autenticação, pois afinal, a rede de um parceiro deve ser considerada uma rede não confiável, e os acesso disponíveis a estes parceiros devem ter os destinos dos recursos estritamente controlados. Para um parceiro de uma extranet, pode-se (e deve-se) aplicar a regra de segurança "tudo é proibido, com exceção do que é estritamente permitido" [dG02a].

Além disso, a colocação de uma VPN na infra-estrutura de comunicação de uma organização pode impactar em reconfiguração de DMZs, *subnets*, disponibilização de recursos etc, principalmente quando o objetivo é prover um acesso em um cenário de *extranet*. Não se pode simplesmente através de uma VPN "abrir as portas" para toda a rede interna da organização. Uma VPN mal construída (ou configurada) pode por exemplo permitir que um parceiro veja os dados de uma cotação de outro parceiro, mesmo estando em bancos de dados diferentes, além de outros dados confidenciais que devem ser restritos a cada um. Isso deixa evidente que uma *extranet* não depende apenas de uma boa configuração de uma VPN. Uma boa arquitetura de banco de dados neste caso é importante para garantir a segregação dos dados de parceiros no *site* da corporação. A complexidade do controle de acesso e autenticação, além da estrutura da rede corporativa deve receber especial atenção quando acessos não confiáveis são integrados, caso típico das *extranets*.

Um ponto interessante a considerar é quem está se conectando a quem, ou seja, quem será o *initiator* e quem será o *responder* na comunicação VPN envolvendo uma *extranet*. Se um parceiro quer se conectar a rede da sua organização, a necessidade pode ditar a opção de acesso remoto ou *site-to-site*. Quando o inverso é verdadeiro, ou seja, a sua organização quer se conectar à rede de um parceiro, o acesso remoto deve receber atenção especial [Cle03]. Por iniciar o túnel dentro da rede interna, o Firewall será incapaz de inspecionar os pacotes a aplicar a política de segurança estabelecida para a organização, dado que os pacotes são criptografados no *Host* de origem. Isso pode ocasionar uma violação da política da organização, além de ser uma porta de entrada de vírus e cavalos de tróia, pois os mecanismos de defesa da organização podem ser facilmente "burlados".

Alguns autores consideram a comunicação *Host-Host* a mais segura [Str01], mas algumas análises de cenários onde o IPv6 está presente, com suporte nativo ao IPSec, mostra que podem ocorrer sérios impactos na arquitetura de segurança convencional [Cle03], com Firewalls e outros agentes de segurança (*proxy*, IDS etc) presentes no perímetro da rede. A possibilidade de túneis criptografados cruzando os Firewalls atuais leva à necessidade de fortificação de máquinas espalhadas pela rede interna, e alterando a barreira tradicional dos Firewalls, levando à uma estrutura denominada "Firewalls distribuídos" [Bel99],

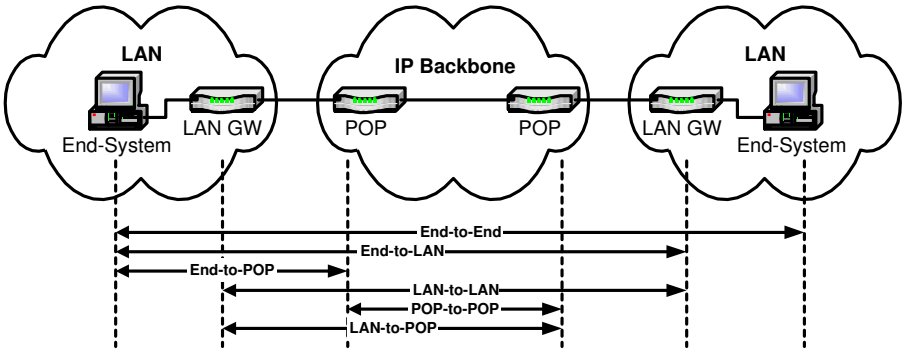

Figura 2.6: *Possíveis End-Points de uma VPN*

tecnologia ainda em estudo pela academia e não disponível em escala comercial. Por este motivo, a consideração sobre fortificação e colocação de uma máquina (numa DMZ por exemplo) que estabeleça um acesso remoto partindo de dentro de sua organização deve ser cuidadosamente estudado, caso a necessidade realmente exista para esta configuração. A posição dos gateways VPN na arquitetura do Firewall, além da utilização de protocolos como o SSH também podem colocar o Firewall em situação difícil pelo mesmo motivo, como será visto mais adiante neste trabalho.

2.5.3 Considerações sobre os *end-points* do canal seguro em uma VPN

Para as VPN, os terminadores dos túneis, também chamados de *end-points*, são onde são tomadas todas as decisões de autenticação e controle de acesso, bem como verificação de integridade. Por esse motivo, as escolhas dos *end-points* de uma VPN são extremamente críticas no *design* de uma solução [Str01].

Na prática é possível encontrar três tipos de *end-points*, que iniciam ou terminam um túnel VPN. Primeiro, o *end-point* pode ser um *Host* dentro da rede, ou seja, uma estação de trabalho. Quando se estabelece uma conexão SSH a um servidor qualquer, a máquina com o SSH *client* será um dos *end-points* na comunicação, e neste caso, um *Host*. Outro tipo de *end-point* é um gateway localizado no perímetro de uma LAN, provavelmente integrante de uma arquitetura de Firewall, e agindo com um *proxy* de segurança. Neste caso, o canal seguro é transparente aos *Hosts*, pois o gateway é responsável pelo início e/ou termino do túnel VPN. Por último, é possível ter o túnel iniciando ou terminado em um POP de um SP (Service Provider) de confiança da organização, iniciando a VPN portanto fora da rede corporativa. Esses modos de início e término de túneis podem dar origem a vários modelos de tunelamento, como mostra a Figura 2.6. A partir desses modelos, diversos tipos de VPN foram criados, e serão melhores detalhadas no Capítulo 3.

2.6 Topologias para VPNs

Quando se planeja uma solução de comunicação corporativa baseada em uma VPN, a topologia adotada é peça fundamental para o sucesso do projeto, além de nortear muitas das decisões com relação a roteamento, acesso remoto, protocolo utilizado etc.

Basicamente, quando se fala de topologia em uma VPN, existe uma referência quase que diretamente ao fluxo de dados, ou seja, quem se comunica com quem. É possível encontrar cenários onde uma filial fala (no sentido de ter comunicação) diretamente e somente com a matriz. Outro cenário poderia ser uma filial que fala diretamente com a matriz e diretamente com outra filial. Ou ainda uma filial que se comunica com a matriz diretamente, e com as outras filiais indiretamente através dessa ligação direta com a matriz.

Em um ambiente com poucas filiais, isso pode fazer pouca ou nenhuma diferença, mas novamente pode-se notar que em um grande ambiente corporativo, onde a capilaridade da rede é muito alta, o assunto "topologia" deve ser tratado com especial atenção.

A topologia adotada deve, em conjunto com a solução, prover escalabilidade, que implica em gerenciamento, custo, expansões futuras e outros fatores, não se esquecendo principalmente da eficiência. Para se tirar o maior proveito da solução, a topologia correta se torna portanto essencial [Sys03c].

A seguir, serão apresentados os principais modelos de topologias utilizados nas VPNs. Esses modelos podem ser combinados, conseguindo-se novos modelos híbridos juntamente com o emprego de novas tecnologias, a fim de atender a solução específica a ser adotada em cada organização. Antes de abordamos essas alternativas e derivações de modelo, com seus principais problemas e possíveis soluções, é necessário apresentar o conceito dos modelos básicos de topologia para uma VPN, conforme descrito a seguir. Cada modelo tem vantagens e desvantagens, problemas e possíveis soluções, que serão abordadas com maiores detalhes no Capítulo 6, após a escolha do protocolo no Capítulo 4.

2.6.1 Hub-and-Spoke

Este é o tipo mais simples de topologia que existe para uma solução VPN. Neste modelo, ilustrado na Figura 2.7, existe um nó central (*Hub*), que na grande maioria das vezes é a matriz da organização, e vários nós espalhados geograficamente que se conectam única e exclusivamente ao *hub*, podendo ser filiais, parceiros ou acessos remotos, chamados de *Spokes*. É possível fazer uma analogia a uma topologia tipo estrela. Apesar da simplicidade de gerenciamento, este modelo sofre de problemas de roteamento e performance, tendo em vista que no *hub* todo tráfego deve ser desencriptado e encriptado novamente caso haja comunicação entre *spokes*, além do *hub* se tornar um ponto único de falha. Além disso, *sites* geograficamente perto devem se comunicar via *Hub*.

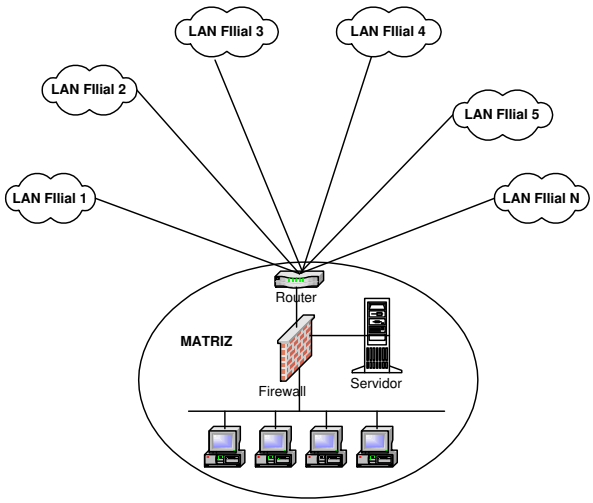

Figura 2.7: *Topologia Hub-and-Spoke*

2.6.2 *Full-Mesh*

Neste modelo de topologia, ilustrado na Figura 2.8, constata-se uma otimização do roteamento do tráfego, tendo em vista que cada nó possui uma conexão com cada outro nó da VPN. Com isso, o fluxo de dados segue diretamente para o destino, evitando *hops* (pertencentes a VPN) intermediários. Em compensação, a complexidade no gerenciamento e expansão deste modelo se tornam pontos críticos a serem analisados, pois o número de túneis se torna extremamente grande para múltiplos *sites*, sendo no mínimo n(n-1)/2 [Sys03b]. No caso de existirem por exemplo 300 filiais (sem contar parceiros e acessos remotos) pode-se chegar à quase 50.000 túneis, o que sem dúvida nenhuma não é tarefa fácil para gerenciamento.

2.6.3 *Partial-Mesh*

A utilização de um modelo *partial-mesh* engloba pontos dos dois modelos anteriores. É possível ter por exemplo algumas filiais falando com a matriz e somente com ela (*hub-and-spoke*) e outras que se comunicam diretamente (*mesh*), ou ainda filiais e matriz em *full-mesh* e demais acessos VPN (remotos e parceiros) em uma topologia *hub-and-spoke*. A Figura 2.9 mostra um exemplo.

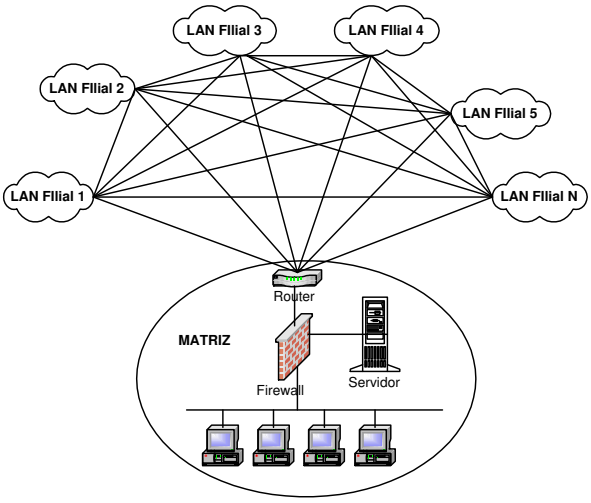

Figura 2.8: *Topologia Full Mesh*

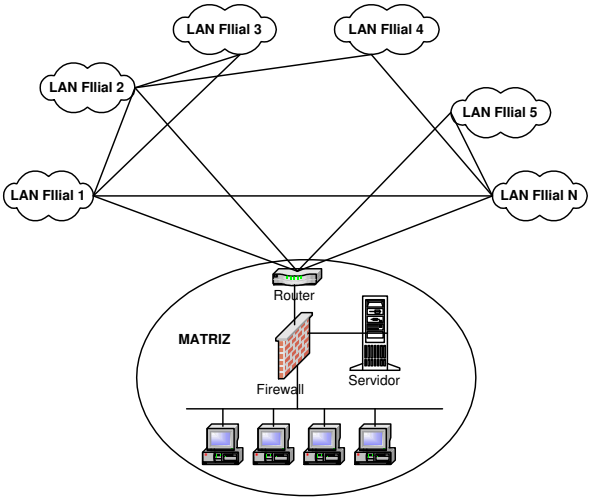

Figura 2.9: *Topologia Partial Mesh*

2.7 Conclusão

Este capítulo teve como objetivo introduzir o conceito das VPNs e situar a atuação desta tecnologia no cenário corporativo, principalmente em um ambiente de alta capilaridade (onde na maioria dos casos são pequenas filiais, no que diz respeito ao tamanho da rede a ser conectada). Analisando as considerações sobre os possíveis *end-points* de uma VPN, exemplificados no item 2.5.3, aliadas à topologia da rede desejada em função do fluxo da comunicação, chega-se a conclusão de que vários tipos de VPNs podem derivar destes aspectos, associados também ao protocolo, e por consequência o tipo de tunelamento e proteção oferecidos na comunicação (como por exemplo o uso da criptografia).

O próximo capítulo portanto, tem como objetivo analisar essas várias classificações dos serviços de segurança oferecidos pelas VPNs, mostrando ao leitor os tipos existentes, seus principais objetivos e o foco escolhido para objeto de estudo deste trabalho.

Capítulo 3

Uma taxonomia de redes virtuais

3.1 Introdução

Conforme foi analisado no capítulo anterior, é possível enumerar uma série de soluções e serviços de segurança sob o título de VPNs. Uma empresa com uma rede complexa, com alto número de pontos a serem conectados, além de acesso remoto de empregados e interligação de redes não totalmente confiáveis como parceiros e clientes, irá se deparar no mercado e na literatura com um grande número de abordagens para prover soluções que nem sempre têm o mesmo objetivo.

Isso quer dizer que uma determinada abordagem ou solução sob o termo VPN pode diferir completamente de outra no sentido do foco dos problemas a serem resolvidos e vantagens a serem oferecidas. Esta variedade de objetivos, que nem sempre são concorrentes, permitem que se crie uma classificação, uma taxonomia para os serviços oferecidos, que por falta de conhecimento das empresas podem gerar muita confusão. Este capítulo tem como objetivo enquadrar essas abordagens e soluções dentro de uma classificação que reúna os principais objetivos de cada uma, tendo em vista que uma rede complexa de alta capilaridade será alvo de ofertas de soluções pertencentes a diferentes grupos e consequentemente diferentes propósitos.

Visando a análise uma solução que atinja satisfatoriamente a equação segurança x custo, esta análise da taxonomia de serviços oferecidos é o ponto de partida para evidenciar o foco de atuação deste estudo, onde não se pretende travar uma batalha entre abordagens (principalmente por oferecem serviços diferentes), mas sim visualizar os problemas e possíveis soluções da mais apropriada para a equação citada. É deste ponto de partida que serão direcionados os esforços de estudos mais aprofundados, que vão desde a escolha do melhor protocolo até a sua implementação em uma rede complexa.

3.2 *Secure* vs *Trusted* VPNs

Até o momento, uma VPN para as empresas era, com exceção das linhas privadas contratadas das companhias telefônicas, um ou mais circuitos "alugados" de um determinado provedor, e cada circuito como se fossem um único cabo e gerenciado pelo cliente, podendo algumas vezes ser ajudado pelo provedor, mas a idéia principal era visualizar um cabo fisicamente presente, como os utilizados nas LANs do cliente.

A privacidade provida pelos provedores de dados era simplesmente que ninguém mais utilizaria ou teria acesso ao mesmo circuito, permitindo ao cliente ter seu próprio endereçamento IP (ou outro protocolo) e suas próprias políticas de segurança. Esses circuitos são implementados sobre vários roteadores e *switches*, agregando várias VPNs de diferentes clientes, e o comprometimento de qualquer um desses dispositivos pode permitir a análise de tráfego e outros tipos de ataques. O cliente passa então a confiar no provedor para manter a integridade dos circuitos alugados a fim de manter a privacidade obtida pelo cliente com linhas dedicadas. Por esse motivo, que o cliente passa a confiar plenamente no provedor para garantir a segurança, essas VPNs recebem o nome de *trusted* VPNs.

Com o advento da Internet se tornando uma infra-estrutura de comunicação viável para a comunicação corporativa, e a percepção que as *trusted* VPNs não ofereciam segurança real [VPN04], protocolos que empregam o uso da criptografia começaram a ser desenvolvidos, permitindo que um pacote ou dado seja criptografado na borda da rede origem (ou no próprio *Host* dentro desta rede), podendo cruzar a Internet como qualquer outro pacote, sendo descriptografado quando alcançar a rede destino (ou o *Host* dentro dela). Esse tipo de protocolo implementa segurança real comparada as *trusted* VPNs, pois mesmo um atacante conseguindo ter acesso a esses pacotes, eles não poderão ser lidos, e qualquer modificação fará com que o receptor os rejeite (providos por métodos de autenticação). VPNs que são construídas utilizando a criptografia e autenticação são chamadas de *secure* VPNs, pois o protocolo por si só garante a segurança.

Pode-se notar que a classificação aqui, entre *trusted* e secure VPNs está diretamente ligada ao protocolo utilizado. A princípio pode-se associar o termo "*trusted*" a VPNs oferecidas por provedores de dados, mas estes também podem oferecer VPNs protegidos por protocolos seguros, oferecendo portanto uma *secure* VPN. Claro que os protocolos associados às *trusted* VPNs são extremamente interessantes para os provedores pois promovem separação de tráfego e consequentemente permite agregação de várias VPNs em um mesmo *backbone*, requisito não necessário do ponto de vista de uma única empresa. Essa "segurança" gerada pelas tabelas de roteamento privadas que na verdade não são realmente seguras (estão fora do controle da empresa e qualquer um com acesso ao *backbone*, como administradores do provedor, pode ler e manipular o tráfego).

Derivada destas duas classificações surgem as VPNs híbridas, que geralmente utilizam uma *secure* VPN sobre uma *trusted* VPN, geralmente visando a segurança fornecida pela primeira e QoS oferecida pela segunda [VPN04], podendo inclusive ter parte como *secure* e parte como *trusted* VPNs, dependendo da necessidade. Em alguns países, a própria lei pode exigir que determinados tipos de dados, como transações médicas e financeiras utilizem uma tecnologia de *secure* VPN mesmo quando existe a infra-estutura de uma *trusted* VPN [Sys03b].

Em resumo, as corporações irão utilizar serviços providos pelas *secure* VPNs quando querem ter certeza que mesmo uma cópia dos dados seja capturada o atacante, quer seja ele um *insider* [dG02a] no provedor ou um atacante na Internet, que os os dados chegarão ao destino de forma privada e sem alterações. Já as empresas que procuram um certo nível de serviço irão procurar as *trusted* VPNs, pois querem ter certeza que seus dados irão se deslocar sobre um caminho específico controlado pelo ISP (ou uma série de ISPs, que também devem ser "confiáveis"). O importante é notar, que apesar dos SLAs (Service Level Agreement) oferecidos, garantindo uma série de serviços como QoS, largura de banda e privacidade (no sentido de conter os dados dentro do *core* do ISP) fica impossível ao cliente checar se a VPN dentro do provedor está realmente segura e qual o caminho percorrido pelos pacotes. Definir uma SLA inclusive pode ser uma tarefa árdua e nem sempre pode ser a tábua de salvação para uma eventual falha de serviço ou segurança, pois geralmente envolve restituição financeira, o que pode nem sempre recuperar a credibilidade de uma marca [Jim04]. A idéia das *trusted* VPNs portanto é que o cliente confie "cegamente" no ISP.

É claro portanto que as *secure* e *trusted* VPNs têm propósitos diferentes, mas não são exclusivas mutuamente, gerando as VPNs híbridas.

O "VPN Consortium"[1], conhecido com VPNC, define algumas propriedades para cada tipo de VPN, conforme abaixo [VPN04]:

Secure:

1. Todo tráfego na VPN deve ser encriptado e autenticado.
2. As propriedades de segurança da VPN devem ser de comum acordo entre todas as partes participantes da VPN.
3. Ninguém fora da VPN pode afetar as propriedades de segurança definidas.

[1] http://www.vpnc.org

Trusted:

1. Ninguém a não ser o ISP pode afetar a criação e modificação de um caminho na VPN.

2. Ninguém a não ser o ISP pode alterar, inserir ou deletar dados de um caminho/circuito estabelecido para uma determinada VPN.

3. O roteamento e endereçamento utilizados em uma *trusted* VPN devem ser estabelecidos antes da VPN ser criada.

O VPNC define também alguns protocolos para cada tipo de VPN, conforme descrito em [VPN04], tendo em vista as propriedades da organização, que é testar e avaliar a interoperabilidade entre fabricantes segundo uma série de níveis pré estabelecidos.

Para as *secure* o IPSec e o L2TP(Layer Two Tunneling Protocol)/IPSec são utilizados. Além destes protocolos é possível estabelecer uma *secure* VPN através do PPTP (Point-to-Point Tunneling Protocol), SSH e do SSL que vem trazendo uma nova abordagem para o acesso remoto.

Para as *trusted* VPNs existem os circuitos ATM[2] e *Frame-Relay* [For98], além de uma tecnologia mais nova e em evidência no mercado, o MPLS, que ainda está em definição pelo IETF apesar de já serem oferecidos serviços baseados em *drafts* liberados [Har03], inclusive no Brasil, com a promessa de substituir as redes FR e ATM [Alt02, Tec00].

3.3 IP VPNs vs WANs Tradicionais

É possível classificar as WANs existentes hoje em dois grandes grupos, as baseadas em IP, geralmente utilizando protocolo IPSec ou MPLS (além de L2TP, PPTP, SSL/TLS, entre outros) e as WANs tradicionais, baseadas em linhas dedicadas, circuitos *Frame-Relay* ou ATM. Com o advento das redes ATM e *Frame-Relay* como *backbone* dos provedores de dados, surgiram as primeiras VPNs, tornando as linhas privadas um investimento pouco interessante, tanto pelo tempo de implantação e falta de flexibilidade quanto pelo fator custo, sendo o fator distância um limitante na composição final de custos.

Na verdade o protocolo *Frame-Relay* veio como um grande substituto das redes X.25, ainda existentes, mas já consideradas uma tecnologia legada. As redes ATM se tornaram uma opção cara mesmo para os provedores, que acabaram por utilizá-la como *core* em seus *backbones* para conseguirem altas taxas de transferência, adotando o *Frame-Relay* como serviço padrão a ser oferecido às empresas como solução para a comunicação corporativa.

[2]Detalhes em www.atmforum.org

Os detalhes da utilização de *Frame-Relay* em conjunto com ATM foge ao escopo deste trabalho, sendo importante apenas o ponto de vista do cliente, que enxerga somente o serviço *Frame-Relay*. Maiores detalhes podem ser encontrados no *Frame Relay Guide* e ATM Forum[3].

Realmente o mercado adotou as redes *Frame-Relay* como solução corporativa, oferecendo uma série de vantagens em relação às linhas privadas, citando entre elas que sendo um protocolo de nível 2 do modelo OSI, pode suportar (transportar) qualquer protocolo através da rede (também chamada nuvem *Frame-Relay*), oferecer garantia mínima de *throughput* através do CIR, uma espécie de SLA em termos de garantia de banda, e custo reduzido comparado às linhas privadas, dependendo claro da topologia adotada (tipicamente *hub-and-spoke*).

Com o surgimento das IP VPNs, as redes ATM e *Frame Relay* começam a se tornar obsoletas no que toca ao oferecimento de serviço de dados pelos provedores. Tecnologias como o IPSec e principalmente o MPLS (que têm praticamente o mesmo foco de atuação das redes ATM e *Frame Relay*, como será visto adiante) estão sendo amplamente implementadas pelos provedores de dados. Apesar da área de computação nem sempre (ou quase nunca) permitir previsões certas do que prevalecerá no futuro (como já foram vistos diversos "*experts*" desmentindo suas próprias previsões publicamente) , a junção do *Frame Relay* Fórum com o MPLS Fórum, formando o "MPLS - *Frame Relay Alliance*", indica uma forte tendência das IP VPNs substituírem as tecnologias ATM e *Frame-Relay*. Já foram publicados diversos artigos de como integrar as tecnologias já denominadas "legadas" com o MPLS em uma fase de transição, além do uso de MPLS como nova solução para VPNs gerenciadas por provedores ser fortemente encorajado. Com isso, as redes FR tendem s se tornar mais caras, tendo em vista a necessidade dos provedores suportarem ambas as tecnologias (FR e MPLS) para os clientes que ainda utilizam o FR (as redes ATM serão deixadas de lado a partir deste ponto devido a grande parcela de usuários de FR para construção de WANs corporativas, além da semelhança de funcionalidades providas).

Do ponto de vista das empresas é importante analisar o investimento em uma WAN baseada FR sendo que as IP VPNs podem prover um retorno de investimento que justificaria a aquisição de equipamentos ou serviços de ISP [Dav03] (as linhas dedicadas já estão praticamente descartadas principalmente quando o fator distância é limitante). Além da questão custo, as IP VPNs proporcionam a facilidade de integração do acesso remoto, principalmente quando são construídas através da Internet, que apesar de se basearem em *best effort* neste caso ainda possuem taxa de perda de pacotes inferiores às redes FR, além de utilizarem uma única conexão WAN/Internet facilitando a expansão e a montagem de túneis sem nenhum custo adicional (*mesh*). No quesito segurança, alguns

[3]www.atmforum.com

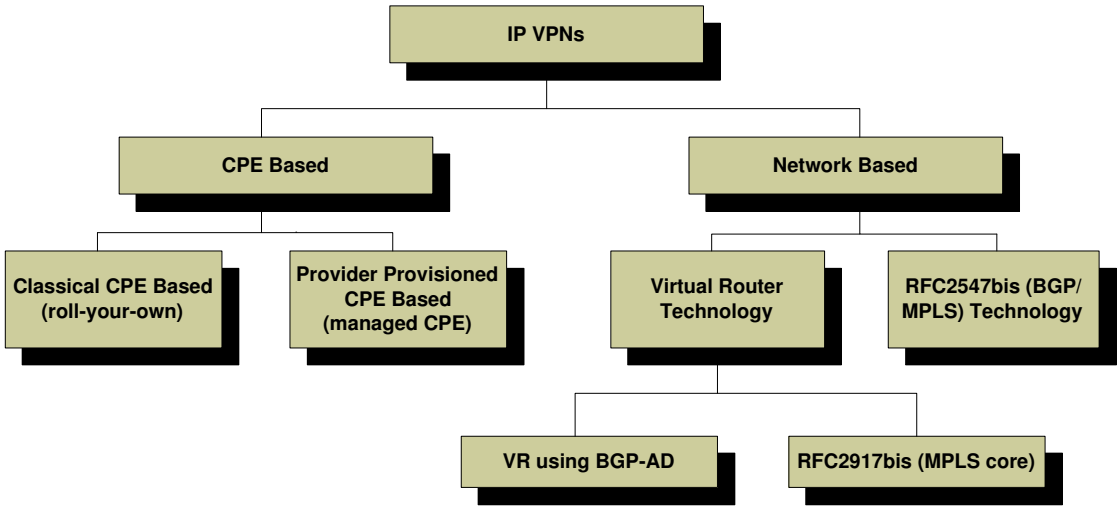

Figura 3.1: *IP VPNs - Classificação (Fonte: Nortel Networks)*

protocolos como o IPSec apresentam o recurso da criptografia, integridade e autenticação, o que não existe nas redes FR (Aliás, um ponto muito discutido por alguns autores é o emprego to termo "*Private*" do acrônimo VPN para uma rede *Frame-Relay*, pois na verdade os dados de cada cliente transitam em claro pelo *backbone* compartilhado de um determinado provedor de serviços).

3.4 IP VPNs - Direcionando o foco da solução

AS IP VPNs podem ser divididas em classificações que são apoiadas basicamente sob o posicionamento do gateway VPN e quem (empresa/provedor) é responsável pela construção e gerenciamento dos túneis. Essas abordagens, exemplificadas na figura 3.1, abrem um leque de protocolos e tipos de serviço, conforme será analisado adiante.

3.4.1 Baseadas em CPE

O tipo de VPN mais comum utilizado atualmente é a abordagem baseada em CPE. Como o próprio nome diz (*Customer Premises Equipment*), o gateway VPN, responsável por iniciar e/ou terminar o canal seguro se encontra dentro da organização. Soluções baseadas em CPE podem ser gerenciadas pela própria empresa ou ter sua gerência terceirizada a um ISP ou empresa de consultoria. O *backbone* pode ser qualquer *backbone* compartilhado, desde um único ISP, conjunto de ISPs ou até a Internet. Uma arquitetura baseada em CPE pode ser observada na Figura 3.2.

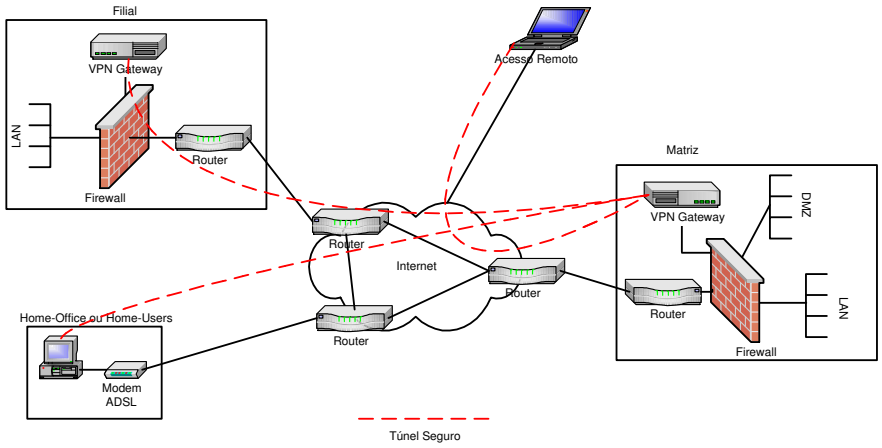

Figura 3.2: *VPNs baseadas em CPE*

De acordo com a gerência do equipamento, as VPNs baseadas em CPE podem ser divididas em:

Baseadas em CPE clássicas (*roll-your-own*)

Neste modelo a empresa gerencia seus gateways VPNs, que por sua vez se encontram dentro dos *sites* de domínio da empresa. Toda a política de segurança e arquitetura da VPN, incluindo sua interação com a rede e dispositivos já existentes fica a cargo da equipe de TI, o que requer de certa forma experiência e capacitação da equipe para não tornar a VPN o elo fraco da corrente e com isso comprometer a segurança.

Para os usuários remotos e/ou *home-users*, o gateway VPN é substituído por um *software client*, que na verdade exerce o papel de um gateway VPN em função da própria máquina, e na maioria das vezes ao se autenticar como membro legítimo de uma VPN ao gateway responsável por receber os acessos remotos, recebe toda a política de segurança definida pela empresa para que efetue uma comunicação segura e não comprometa a rede da organização.

O *client* VPN pode se conectar através da Internet diretamente ao gateway da organização ou utilizado como um segunda camada de proteção para um acesso RAS, utilizando o princípio de "*defense in death*". Isso diminui muito a chance de ataques de *wardialing*, pois um atacante conectado a um modem de um servidor RAS explorando alguma falha de autenticação deste serviço, ainda terá que se autenticar ao gateway VPN para obter acesso aos recursos da organização [Str03]. Essa solução pode ser interessante para pequenas empresas que ainda querem manter o acesso discado diretamente à empresa, mas incorporando um nível maior de segurança. Maiores detalhes do acesso remoto VPN podem ser encontrados em [Edm04]

Baseadas em CPE gerenciadas pelo provedor de serviços (*managed* CPE)

Em termos de estrutura, uma VPN baseadas em CPE com gerência terceirizada é idêntica ao modelo clássico citado anteriormente. A diferença está na administração do gateway, que pode ser feito por uma consultoria ou ISP. O equipamento CPE pode ser fornecido pela própria empresa terceirizada ou adquirido pela empresa interessada na VPN. Isto pode ser interessante para empresas que não possuem profissionais capacitados para montar e principalmente manter a VPN funcionando e crescendo de modo escalável, ou empresas que buscam um canal seguro fim-a-fim e ainda querem contar com algum tipo de QoS no *backbone* (e não fim-a-fim), neste último caso somente possível quando o ISP provê acesso através de seu próprio *backbone* ou *backbones* de parceiros sobre os quais tenha algum tipo de interação e controle. No caso de utilização da Internet, uma gerência terceirizada pouco tem a fazer em relação a QoS, podendo apenas trabalhar alguns pontos de qualidade de serviço fim-a-fim.

Por outro lado, uma gerência terceirizada inclui um elo de confiança na corrente, entre empresa e ISP (ou consultoria). O fato do canal ser seguro fim-a-fim do ponto de vista da empresa, não quer dizer que não seja possível a interceptação da comunicação no *backbone* utilizado ou mesmo acesso aos gateways, dado que o controle dos mesmos foge das mãos de profissionais de confiança dentro da organização. Neste ponto, é possível dizer que uma abordagem terceirizada implica em menor grau de segurança que o modelo controlado pela empresa, que mesmo visando aplicações que necessitam de QoS como voz sobre IP, videoconferência e B2B, está se falando de aplicações sensíveis à confidencialidade da informação.

A Toyota[4] por exemplo, utilizou o IPSec em uma abordagem baseada em CPE para uma rede de 1000 *sites*, e conforme descrito em [Max02], os principais fatores que motivaram essa escolha foram custo e flexibilidade. A responsável pelo projeto foi a WorldCom[5], por razões de custo e abrangência. O fator chave determinante para o que as empresas querem para uma solução VPN é o que esperam de QoS e segurança [Max02]. Alguns detalhes sobre a solução adotada pela Toyota em parceria com a WordCom serão discutidos na Seção 3.5, após alguns detalhes sobre abordagens baseadas em rede.

3.4.2 Baseadas em rede

A principal característica de uma VPN baseada em rede é que todos os dispositivos envolvidos na construção de uma VPN são sistemas compartilhados de propriedade do ISP, sendo todos localizados dentro de seu *backbone*, começando a VPN portanto na borda do *backbone* do ISP. Na empresa fica somente um roteador comum e através de

[4]www.toyota.com
[5]www.worldcom.com

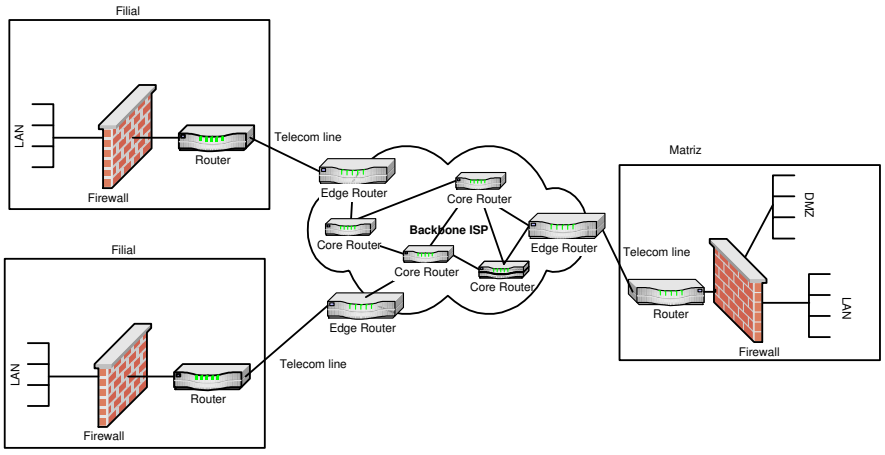

Figura 3.3: *VPNs baseadas em rede*

um *link* qualquer o *site* interessado em integrar a VPN deve se conectar ao POP mais próximo.Todo o gerenciamento, construção, manutenção e separação entre VPNs distintas cabe ao ISP, dados os equipamentos envolvidos estarem todos no *backbone*, conforme mostra a Figura 3.3.

Qualidade de serviço é um ponto forte, pois no caso de abordagens CPE o pacote chega criptografado e não há muito o que fazer em relação à classes de serviço, mesmo passando por um *backbone* privado de um ISP qualquer. Além disso, dentro do *backbone* do provedor é possível aplicar-se o conceito de engenharia de tráfego, e protocolos como MPLS vêm surgindo como importantes componentes para soluções baseadas em rede [Alt02].

A complexidade à primeira vista fica toda a cargo do ISP, visto que a empresa tem somente um roteador IP simples, ficando os serviços de VPN e inclusive Firewalls a cargo do ISP [Str03], além do ISP ser responsável pela disponibilidade da VPN, um ponto forte dado a disponibilidade de equipamentos e profissionais 24x7[6] disponíveis para manter os serviços contratados com um ótimo nível de confiabilidade.

Essa complexidade que a princípio está toda sob responsabilidade do ISP, pode mudar um pouco de figura quando se fala de segurança. Pela própria natureza da arquitetura, o nível de segurança é equivalente a uma VPN baseada em ATM ou *Frame-Relay*, dada ausência de criptografia e outros mecanismos de autenticação e integridade, principalmente quando se fala de MPLS, que surge como o protocolo que deve se estabelecer como padrão *de facto* das VPNs baseadas em rede [Har03].

Além disso, a segurança pode ser comprometida ainda por não existir um canal seguro da organização até a borda do ISP (o chamado *last mile*), além de limitações de distância entre *site* e POP e eventuais passagens por outros ISPs, na tentativa de solu-

[6]24 horas por dia, 7 dias por semana

cionar o problema de pontos restritos ao provedor escolhido. O acesso deve ser feito sob um *link* ponto-a-ponto de dados privado, sendo tecnologias compartilhadas como *cable-modem* totalmente não recomendáveis. Isso limita (e obriga) também a empresa a usar as tecnologias de comunicação impostas pelo provedor, suportada pelo seus equipamentos.

Dependendo do protocolo utilizado, o acesso remoto fica inviabilizado. Se os clientes remotos forem utilizar a Internet (*Cable Modem*, ADSL etc) para acessar a VPN, a rede privada do ISP deve estar conectada à Internet, e mesmo sem analisar como será feita a conexão Acesso Remoto x VPN corporativa, a empresa deve confiar plenamente na segurança garantida pelo provedor, tanto em relação a proteção de sua VPN em um *backbone* compartilhado quanto a brechas de conexão com a Internet que podem levar a uma possível invasão.

3.5 Baseadas em CPE vs baseadas em rede

Apesar de proverem serviços semelhantes, as abordagens baseadas em CPE e em rede são completamente diferentes em termos de estrutura e principal objetivo. Na primeira, a própria arquitetura e protocolos são voltados para se construir uma *Secure* VPN, visando principalmente a segurança fim-a-fim. Já a segunda, baseada no conceito de *Trusted* VPN, visa a qualidade de serviço e incorporação da complexidade de construção e gerenciamento da VPN das corporações.

Desse ponto de vista, é injusto comparar essas duas abordagens como concorrentes diretas, mas sim com a finalidade de escolher a melhor abordagem para o propósito deste trabalho: segurança e baixo custo. Via de regra as VPNs com enorme número de *sites* estão partindo para VPNs baseadas em rede pela simplicidade, quando muitas vezes deixam de lado a preocupação principal que é a segurança. Pior do que não ter segurança é ter uma falsa sensação de segurança, como a utilização de abordagens baseadas em rede ou mesmo protocolos de criptografia extremamente simples.

O fato de determinada tecnologia apresentar um bom nível de segurança, mas problemas de gerenciamento e escabilidade, não quer dizer que deve-se abandoná-la e procurar uma outra que não ofereça o mesmo nível (ou melhor) de segurança. Este trabalho visa justamente a análise de soluções que sejam eficientes no propósito de se construir uma VPN segura e tentar atacar os principais problemas desta tecnologia com o intuito de ajudar a resolvê-los e tornar a solução cada vez melhor para o propósito a que se dispõe.

Outro fator a ser analisado é a terceirização do gerenciamento da VPN, mesmo CPE, pois de certa forma é análogo a segurança da VPN baseada em rede. Tenho que confiar na parte terceirizada que gerenciará a VPN. Quantas pessoas têm acesso a visualizar o tráfego da VPN corporativa no ISP ou consultoria? Qual a garantia de que essas informações não podem ser "roubadas"? Qual a garantia que estão percorrendo um caminho realmente

seguro e têm a segregação de tráfego proposta? Existem meios da empresa medir todos esses pontos com segurança e confiabilidade?

A segurança do "*last mile*" ou "*local loop*", que é a ligação do roteador IP na empresa até o POP do *Service Provider* deve ter duas considerações: ausência de proteção e custo, que dependendo da distância pode desbalancear a equação custo x benefício. Além disso, é complicado fazer parceiros comerciais integrarem uma VPN restrita a um *Service Provider*, dados o custo do *link* e limitação de pontos de presença do ISP. O acesso à Internet deve ser provido por um outro *link* e consequentemente por um serviço adicional, compondo um custo a parte.

No caso da solução adotada pela Toyota [Max02], a autonomia de cada filial poder escolher seus parceiros comerciais foi facilitada e muito pela escolha de uma abordagem CPE, dada a conexão com a Internet e a presença do equipamento VPN em cada *site*. Vale lembrar entretanto, que o fato de descentralizar a aplicação de políticas de segurança (no caso em cada revenda) não implica em administração descentralizada. No caso da administração ser feita por pessoas (ou equipes) diferentes pode implicar em uma brecha a segurança, dada a possibilidade de um acesso de um parceiro comercial à toda rede corporativa via rede da filial. Neste caso, uma camada extra de proteção em cada *site* compondo um modelo de "*defense in death*" deve ser aplicado como uma série de "barreiras" a serem transpostas.

No caso de uma opção por terceirizar tarefas de segurança como uma VPN ou um Firewall, as empresas precisam analisar com cuidado os riscos e implicações destas decisão [Str03]. As corporações geralmente se enganam em achar que os responsáveis pela terceirização da VPN são também responsáveis por definirem sua política de segurança, sendo uma abordagem destas não muito sábia e perigosa.

Os "terceiros" não sabem as particularidades de cada rede e de cada cliente, a parte da organização que é crítica ou os dados que devem ser mantidos confidenciais. Apesar das empresas poderem exigir que a empresa terceirizada esteja em conformidade com a política de segurança da empresa, isto na prática não funciona muito bem. A empresa deve se preparar muito bem antes de definir seu SLA, tendo dados concretos que refletem sua política de segurança, como um *web-server* crítico "X" necessitar de 100% de disponibilidade juntamente com os bancos de dados "BD1" e "BD2". Um SLA não mensurável é inútil [Jim04]. Além de definir muito bem o SLA, a empresa deve validar que os procedimentos padrões da empresa terceirizada estão de acordo ou podem ser facilmente modificados para necessidades particulares da política de segurança (quem e como pode mudar regras de Firewall, que tipo de autorização é requerida, acesso remoto, integração de parceiros etc.). A complexidade de terceirizar o gerenciamento pode ser um fator importante, mas a lição de casa em definir bem o SLA pode ser uma tarefa extremamente complexa. Em caso de falha, como ressarcir a empresa? Financeiramente? Quanto custa

uma imagem ou logomarca perdida?

O fato de poder adicionar novos *sites*, mudar configurações e políticas podem ser muito mais demoradas quando o SP ou terceiro é envolvido, envolvendo mudanças em SLAs e tempo de reconfiguração da VPN controlada, o que pode gerar inclusive custos adicionais conforme contrato inicial. Já numa abordagem CPE a empresa tem total autonomia para executar tais tarefas, com muito mais agilidade e rapidez, desde que tenha ferramentas apropriadas, equipe com conhecimento técnico e principalmente um projeto de VPN bem montado, o que deve ser levado ainda mais a sério quando se fala em redes de larga escala, com uma capilaridade muito elevada.

Uma das principais desvantagens apontadas para uma solução baseada em CPE é o custo do equipamento. Calculando-se a economia no custo mensal, o custo do próprio equipamento pode ser fatorado nessa conta e rapidamente restituído, em comparação ao custo mensal das VPNs baseadas em rede [Max02].

3.6 Conclusão

Em uma comparação entre as abordagens "*Secure* x *Trusted*" e "baseadas em CPE x baseadas em rede", é possível constatar que na maioria dos casos os prós de uma são os contras da outra. O que foi idealizado para este projeto foi uma solução que substituísse as WANs tradicionais com mais segurança e a um baixo custo.

Do ponto de vista de segurança, as soluções CPE *based roll-your-own* são as mais seguras por oferecerem proteção fim-a-fim e não dependerem de confiança em nenhuma parte terceirizada. O fato é que esse tipo de implementação requer mecanismos que tornem a VPN gerenciável e escalável, para que a equipe de TI da própria corporação seja capaz de gerenciá-la sem deixar falhas e brechas na configuração e manutenção das políticas de segurança e da própria VPN, e sem gerar custos adicionais pela necessidade de pessoal qualificado para exercer tal tarefa.

As soluções baseadas em rede do ponto de vista de gerenciamento e escalabilidade são as melhores opções, mas em hipótese nenhuma podem ser consideradas a melhor solução no quesito segurança. Prova disso é o surgimento de várias soluções híbridas [Str03], onde existem soluções baseadas em CPE rodando sobre uma solução baseada em rede (geralmente IPSec sobre MPLS). Não se pode esquecer que a pergunta principal a ser feita não é "o que é melhor para o SP", mas sim "O que o cliente realmente precisa?".

Com base no propósito deste trabalho, fica evidente a opção por uma solução *Secure* VPN baseada em CPE, que abrange o ponto focal de uma solução ideal para qualquer corporação: a segurança [Net04b]. Com base nesta escolha, serão analisados os principais protocolos que proporcionam soluções *Secure* VPN baseada em CPE, na tentativa de escolher o melhor entre eles. Além disso, surge o desafio de tornar a solução viável,

gerenciável e escalável com base no protocolo escolhido, tópicos que serão abordados nos capítulos sub-sequentes.

Capítulo 4

Estabelecendo canais seguros

4.1 Introdução

Como foi visto anteriormente, a fim de prover uma comunicação segura sobre uma rede não confiável criando assim as VPNs, existe a necessidade de estabelecer canais seguros, que contam com a criptografia e o tunelamento para realizarem essa tarefa. Esses canais são conseguidos por meio da utilização de protocolos específicos, que tem por objetivo suprir a falta de segurança do atual protocolo IP.

Com isso, o protocolo a ser utilizado em uma VPN se torna o ponto chave, o coração da solução, pois dele depende uma série de decisões, características e limitações, e afetam diretamente os recursos e serviços que se desejam proteger. A questão não é simplesmente qual o melhor protocolo, mas sim o que melhor se adapta para uma determinada situação.

Este capítulo apresenta alguns dos principais protocolos disponíveis para soluções VPN no ambiente corporativo. Gigantes como a Microsoft apresentam o PPTP e o L2TP (sobre IPSec) como as soluções mais viáveis, incorporando estes protocolos no novo Windows 2003, enquanto o IETF apoiado por outros gigantes de mercado (como a Cisco) e comunidades *OpenSource* apostam no IPSec como o padrão *de facto* das VPNs [Atk98c, dG02a], [Sys00, Alt02], presente inclusive na próxima versão do IP, o IPv6. O VPNC aceita como padrão para as *Secure VPNs*, objeto de estudo deste trabalho, o IPSec e o L2TP/IPSec.

Apesar disso, soluções baseadas em SSL prometem revolucionar o mercado das VPNs, concorrendo com as soluções IPSec para acesso remoto, e embora não fazendo parte do escopo deste trabalho merecem atenção por ser um possível cenário de integração a VPN corporativa. O foco deste trabalho no entanto é a conexão entre LANs.

Neste capítulo serão analisados alguns dos protocolos utilizados para uma solução "secure VPN" através da Internet, com uma abordagem *CPE Based*, na tentativa de justificar a escolha do mais adequado para o cenário corporativo em questão.

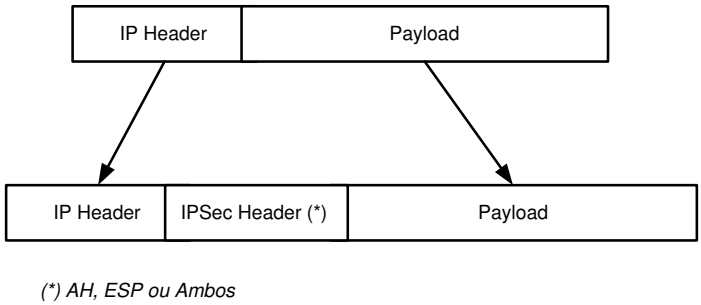

Figura 4.1: *Cabeçalho IPSec*

4.2 IPSec

4.2.1 Conceitos Básicos

O IPSec [Atk98c] é uma arquitetura que visa prover serviços de segurança, como autenticação, integridade, confidencialidade, proteção *anti-replay* e controle de acesso, tanto para o atual IPv4 quanto para próxima geração do IP, o IPv6 [Hin95], que já incorpora o IPSec de forma nativa em sua especificação. Na verdade o IPSec foi desenhado inicialmente para o IPv6, mas incorporado ao IPv4 como uma extensão a fim de atender as necessidades atuais, que não poderiam aguardar a chegada do IPv6 como padrão largamente utilizado na Internet [Sta98].

Além de estar se tornando o padrão *de facto* das VPNs (tornando-o uma solução muito interessante para as empresas, que esperam que a padronização resulte principalmente em interoperabilidade entre fabricantes), é reconhecidamente um protocolo seguro. Porém, a segurança de um protocolo não garante a segurança do sistema [dG02a]. O IPSec é composto por várias "peças", além de ser apenas mais um componente numa arquitetura segura, e portanto, a segurança do sistema depende da correta implementação do protocolo.

Os serviços oferecidos pelo IPSec são conseguidos por meio da utilização de dois protocolos de segurança, o *Authentication Header* (AH) [Atk98a] e o *Encapsulating Security Payload* (ESP) [Atk98b], inseridos após o cabeçalho IP, como mostra a figura 4.1

Além destes protocolos, o IPSec conta com um mecanismo de gerenciamento de chaves criptógraficas e negociação de serviços de segurança (protocolo, algoritmo etc.), chamado *Internet Key Exchange* (IKE) [Car98], que é baseado nos *frameworks* ISAKMP/Oakley. O IPSec provê o seguinte conjunto de serviços, conforme descrito em [Atk98c] e [Jan02]:

- *Autenticação:* evita que pacotes enviados por outra fonte com identidade da origem falsificada (IP *Spoofing* [Coo00]) sejam aceitos.

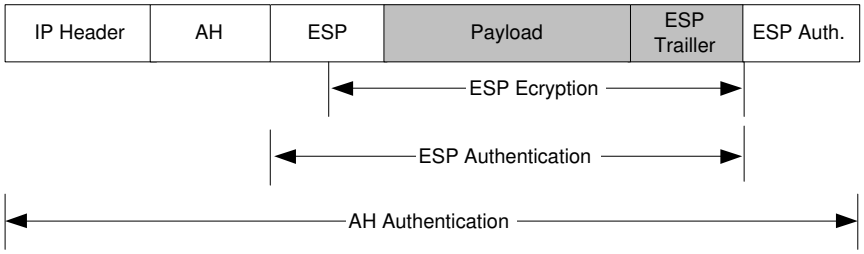

Figura 4.2: *Abrangência dos Protocolos AH e ESP*

- *Integridade:* Garante que os pacotes não sofreram nenhuma alteração no percurso entre origem e destino. Por ser um protocolo que trabalha na camada de rede, o serviço de integridade do IPSec é oferecido pacote a pacote, sem conexão.

- *Confidencialidade:* Através de mecanismos de cifragem dos dados impede que o conteúdo do pacote seja lido por terceiros não autorizados. Além disso, em modo túnel como será descrito a seguir, o IPSec provê confidencialidade do fluxo de dados, ocultando os reais extremos da conexão, uma forma de limitar a análise de tráfego.

- *Proteção contra* replay*:* Impede que pacotes capturados sejam reenviados posteriormente, o que é chamado de *replay-attack* [Coo00], a partir do qual alguns tipos de ataque podem ser realizados.

- *Controle de Acesso:* O estabelecimento de uma conexão IPSec deve seguir uma série de regras que compõem uma política de segurança envolvendo as duas pontas da conexão.

O IPSec DOI (*Domain of Interpretation*) descreve também a negociação de compressão do *payload* do protocolo IP, conforme descrito em [Tho98]. O IPComp, como é chamado, foi motivado pela ineficiência da compressão utilizada nas camadas de enlace e física, onde o ciframento já tinha sido realizado pela camada de rede (como o ESP, no IPSec). Com o IPComp, os dados são compactados, utilizando-se um algoritmo de compressão conhecido, antes de serem criptografados, sendo recomendado portanto que a compressão seja desabilitada nas camadas abaixo da camada de rede.

O protocolo AH é responsável por garantir a integridade dos dados e a autenticação da origem. Apesar de muitos autores utilizarem o termo "autenticação" para descrever os serviços citados, integridade e autenticação tem propósitos diferentes. Integridade é garantir que o conteúdo do pacote não foi alterado no trajeto. Já a autenticação garante que o emissor é realmente quem diz ser.

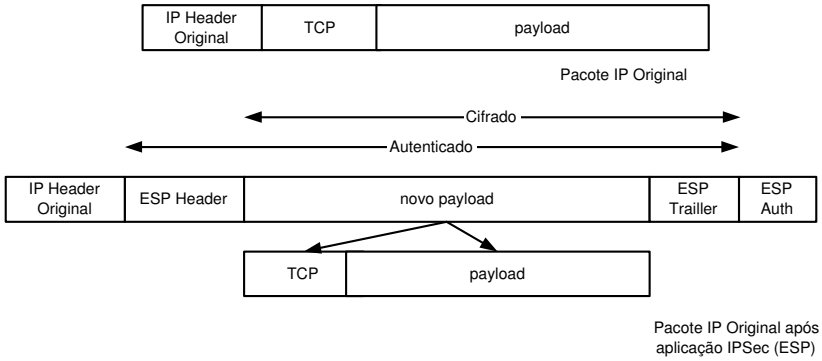

Figura 4.3: *IPSec em Modo Transporte*

O protocolo ESP provê além dos serviços oferecidos pelo AH, a confidencialidade, ou seja, garante por meio da criptografia que os pacotes não serão lidos por terceiros. Os serviços oferecidos pelo AH são também oferecidos pelo ESP para evitar ataques do tipo *cut-and-paste* [Bel96]. A diferença entre os serviços providos por ambos está na abrangência da proteção. Enquanto que no ESP a abrangência se estende somente ao próprio cabeçalho do ESP e à porção de dados do pacote, no AH a proteção se estende a todos os campos do pacote, excluindo-se aqueles que são alterados por roteadores durante o percurso.

O IPSec trabalha de duas maneiras, em modo transporte e em modo túnel, conforme descrito a seguir:

Modo Transporte:

No modo transporte os cabeçalhos dos protocolos de segurança (AH ou ESP) são inseridos após o cabeçalho IP original (No IPv4 após o cabeçalho IP e no IPv6 após o cabeçalho IP e extensões). Deste modo, o *payload* do novo pacote IP protegido pelo IPSec será o mesmo do pacote IP original, além das informações dos protocolos de segurança, conforme mostra a Figura 4.3.

O modo transporte é geralmente utilizado em comunicações entre *Hosts*, apresentando uma solução adequada para segurança de pacotes em redes locais [Jan02]. Apesar de ter a vantagem de se colocar apenas mais alguns bytes de *overhead* no pacote original IP, um dos problemas encontrados em se utilizar o modo transporte através da Internet é que os endereços IPs originais são mantidos, permitindo que um atacante observe quais *Hosts* realmente estão se comunicando (análise de tráfego). O modo transporte é geralmente utilizado em *Hosts* que possuem suporte ao IPSec em sua pilha TCP/IP (de forma nativa ou aplicada "sob" uma pilha IP já existente, entre o IP nativo e os *drivers* locais de

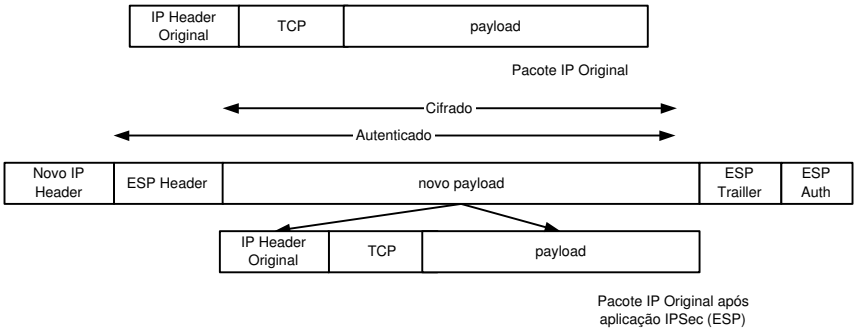

Figura 4.4: *IPSec em Modo Túnel*

rede). É importante não confundir IPSec em modo transporte com qualquer restrição à utilização exclusiva de protocolos de transporte (TCP ou UDP) com o IPSec, sendo suportados por exemplo ICMP, BGP, OSPF, entre outros protocolos que atuam sob a camada de rede (IP).

Modo Túnel:

Em modo túnel, todo o pacote IP original é encapsulado em um novo pacote IP. Desta forma, a proteção mesmo no ESP se estende a todo o pacote original. Na verdade, todo o pacote IP original, incluindo os campos mutáveis, são inseridos como *payload* de um novo pacote IP, conforme mostra a Figura 4.4.

O modo túnel é usado geralmente onde um dos extremos do túnel é um gateway IPSec (entre Host-*Gateway* ou entre *gateway-gateway*). Como todo o pacote original é protegido, caso o serviço de confidencialidade do ESP esteja sendo utilizado, a análise de tráfego se torna impraticável, pois os endereços origem e destino serão ocultados no *payload* no novo pacote IP. Conforme visto no modo transporte, evitar a análise de tráfego não é possível mesmo que a criptografia esteja sendo utilizada.

É possível que dois *Hosts* utilizem o modo túnel entre si, apesar de não ser recomendado, pois os cabeçalhos a serem encapsulados terão os mesmos endereços de origem e destino do novo pacote, apenas adicionando um *overhead* desnecessário para a comunicação, e consequentemente podendo causar problemas de fragmentação. Vale lembrar que computacionalmente a fragmentação gera um custo muito elevado, além dos custos já adicionados pelos serviços providos pelo IPSec (autenticação, criptografia etc).

Conforme descrito em [Atk98c], sempre que um dos extremos for um gateway (neste contexto um dispositivo IPSec agindo em prol de outros *Hosts*, como um *proxy* IPSec), o modo túnel deve ser utilizado. O modo transporte pode ser utilizado por gateways apenas quando estiverem exercendo o papel de *Hosts*, como por exemplo, no caso de

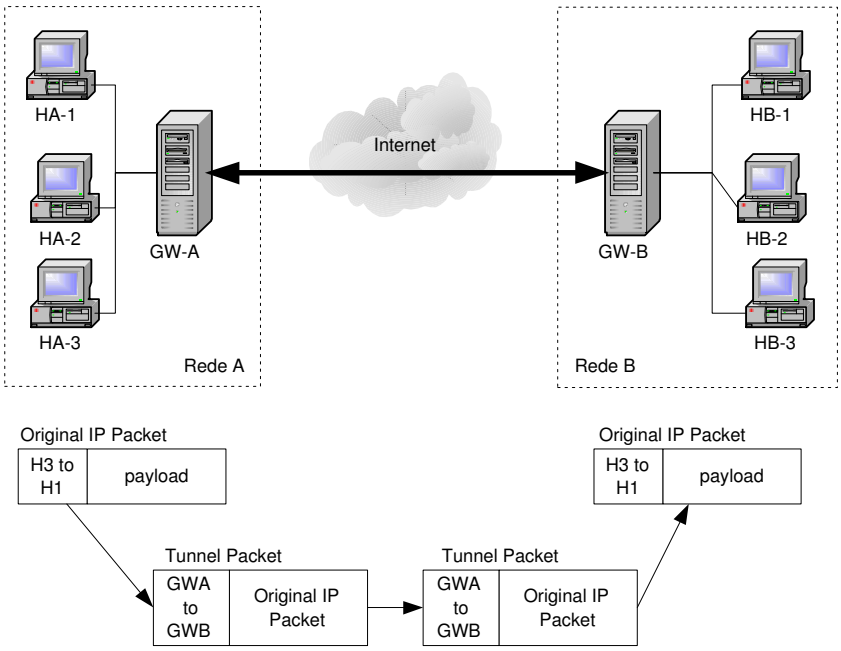

Figura 4.5: *Tunelamento de Pacotes*

pacotes SNMP destinados à administração do gateway.

Conforme mostrado na Figura 4.5, onde os gateways GW-A e GW-B implementam o modo túnel, nenhum dos *Hosts* nas redes A e B precisam de qualquer suporte ao IPSec, sendo o tunelamento feito de forma totalmente transparente.

Quando o pacote de HA1 para HB3 chega em GW-A, ele é encapsulado em um novo pacote, com origem GW-A e destino GW-B. Ao chegar em GW-B, o pacote é desencapsulado e entregue ao destino correto (HB3). Em consequência, todos os pacotes transitados entre a rede A e a rede B terão os mesmos endereços de origem e destino, não importando de qual *Host* tenha sido originado o pacote.

4.3 SSL/TLS

4.3.1 SSL

Funcionamento Básico

O SSL tem como objetivo adicionar segurança às mensagens de protocolos de transporte orientados à conexão, como é o caso do TCP [Jan02]. Os serviços oferecidos por ele são: autenticação do servidor e/ou do cliente (opcional), integridade, confidencialidade e

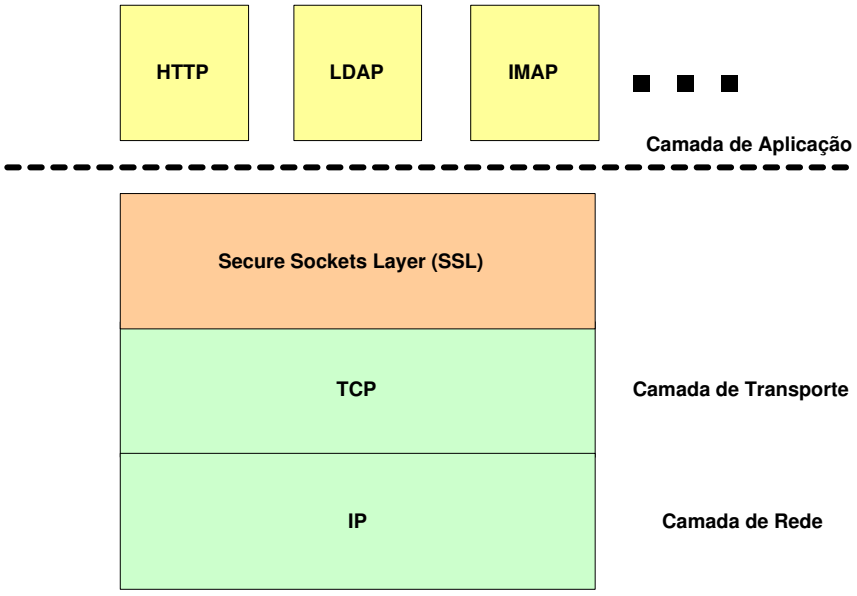

Figura 4.6: *Atuação do SSL*

proteção contra o reenvio de mensagens. O SSL roda acima do TCP/IP e abaixo dos protocolos de alto-nível como é o caso do HTTP ou IMAP, se integrando como uma camada adicional entre as camadas de transporte e aplicação, conforme Figura 4.6.

O SSL inclui dois sub-protocolos: o de registro e o de *handshake*. O primeiro é responsável pelas operações criptográficas de cifragem e decifragem, cálculo dos MACs (Message Authentication Codes, ou *hash's* assinados digitalmente) e verificação de integridade e autenticidade das mensagens. Os dados gerados são enviados à camada de registro para adição dos serviços de segurança e então repassados para as camadas inferiores. Depois da transmissão dos dados e do processamento pelas camadas de rede e transporte, a camada de registro valida o conteúdo e repassa a mensagem para a camada de aplicação. Caso a checagem de integridade falhe, a conexão é encerrada [Jan02].

Já o protocolo de *handshake* é utilizado antes do estabelecimento de uma comunicação segura dos dados. Ele acerta entre as duas partes envolvidas na comunicação quais os algoritmos e chaves criptográficas serão usados, qual a versão do SSL etc [Jan02].

O SSL usa uma combinação entre chave pública e criptografia de chave simétrica. A chave simétrica é muito mais rápida que a criptografia por chave pública, porém esta última fornece melhores técnicas de autenticação [Com98].

Uma sessão SSL sempre começa com uma troca de mensagens chamada SSL *handshake*. É o protocolo de *handshake* que autentica o cliente e o servidor, mas a autenticação de

ambos é opcional, dessa maneira é possível que um cliente se mantenha anônimo em uma comunicação. O problema é quando ambos os *Hosts* permanecem anônimos, abrindo caminho para um ataque do tipo *man-in-the-middle*. [Sch96, Bak00].

O protocolo SSL suporta o uso de vários algoritmos de criptografia, chamados *ciphersuites* para serem usados em operações de autenticação entre servidor e cliente, transmissão de certificados e estabelecimento de chaves de sessão [Com98].

A possibilidade de combinar ciphersuites pode permitir que as aplicações selecionem o grupo de algoritmos mais adequado a ser usado nos seus cenários.

Segurança do SSL 2.0

A versão 2.0 do SSL é considerada insegura [Jan02, Coo00] pelos seguintes motivos:

- Durante o processo de negociação do *handshake*, é possível que um atacante se posicione entre as duas partes de uma comunicação e altere os grupos de algoritmos propostos, escolhendo assim, os algoritmos menos seguros. Este procedimento é conhecido como *ciphersuite rollback attack.*

- Quando esta versão do protocolo é usada nos modos de exportação, as chaves dos algoritmos de autenticação são reduzidas a 40 *bits*, contendo somente os algoritmos permitidos pelo governo americano. Porém poderiam ser utilizadas chaves maiores sem desrespeitar as leis norte americanas, mas o protocolo reage dessa forma, reduzindo a segurança das informações [Jan02].

- O campo que armazena os bytes para o alinhamento das MACs geradas não é autenticado, possibilitando a alteração do mesmo por um atacante a fim de fazer o destino desconsiderar bytes válidos do fim da mensagem [Jan02].

Segurança do SSL 3.0

A versão 3.0 foi criada para resolver os problemas de fragilidade encontrados na versão 2.0 e também para acrescentar novos aspectos de segurança.

Nesta versão, as mensagens geradas pelo *handshake* são todas autenticadas, evitando desta forma o *ciphersuite rollback attack*. Também foi alterado o número de *bits* usados nas chaves dos algoritmos de autenticação, quando o SSL é utilizado no modo de exportação. Nesta versão, as chaves possuem pelo menos 128 *bits* no lugar dos 40 da versão 2.0.

O campo que contém o número de *bytes de padding* passou a ser protegido pelo serviço de autenticação, evitando assim, que um atacante altere o número de bytes validados pelo destino.

Porém, a versão 3.0 do SSL também possui algumas fragilidades:

- O tamanho da mensagem criptografada é o mesmo da mensagem original, desta forma, um atacante pode verificar o tamanho das mensagens do tipo *GET* enviadas para o servidor e mandar várias de mesmo tamanho. O atacante então, analisa as respostas do servidor que tenham mesmo tamanho da resposta recebida por ele, podendo assim descobrir a página *Web* acessada e as informações contidas nela, que podem ser sigilosas. Existe uma opção que é a inserção de um número aleatório de bytes na mensagem para evitar este ataque, mas ela é provida pelo SSL 3.0 apenas para os algoritmos de cifragem em cadeia [Jan02].

- A troca inicial de informações do protocolo *handshake* é feita sem criptografia. Após este primeiro "contato", os dois extremos da comunicação devem enviar uma mensagem que chama *change chipher spec* que serve para acertar os parâmetros que serão usados na proteção da comunicação. Caso os grupos de algoritmos escolhidos utilizem somente autenticação, um atacante pode capturar e deletar as mensagens *change cipher spec*, de modo que a comunicação continue sem qualquer tipo de proteção dos dados transmitidos.

- O servidor é responsável por avisar o cliente qual o algoritmo a ser usado para a troca de chaves e seus parâmetros públicos específicos. O campo que inclui os parâmetros tem integridade garantida, porém o campo que identifica o algoritmo não tem proteção. Desta forma, um atacante pode fazer o cliente processar parâmetros vindos do servidor para uso com o algoritmo Deffie-Hellman como sendo parâmetros do RSA. Para isto, o atacante captura a mensagem *Server Key Exchange*, altera a identificação do algoritmo no campo *Key Exchange Algorithm* e reenvia a mensagem ao cliente. Como conseqüência, é possível que o atacante consiga acesso ao *pre master secret* (utilizado para gerar chaves criptográficas usadas na comunicação segura), habilitando-o a decifrar e falsificar as informações entre cliente e servidor [Jan02].

- *Version rollback attack*: A versão 3.0 do SSL possui suporte à versão 2.0 por questões de compatibilidade. Com isto, usa-se a mensagem *hello* enviada pelo cliente ao servidor para dizer qual a versão do SSL a ser usada na comunicação. Porém, como o campo de controle da versão não é protegido pelo serviço de integridade, um atacante pode capturar a mensagem de *hello*, alterar a versão para estabelecer a comunicação com o SSL 2.0, fazendo com que a mesma esteja exposta a todas as vulnerabilidades desta versão do SSL.

4.3.2 Protocolo TLS (*Transport Layer Security*)

O TLS foi desenvolvido pelo IETF baseado no SSL 3.0, apenas com pequenas alterações sobre o mesmo. O TLS é um protocolo para proteção de conexões entre aplicações na

Internet que além de representar uma alternativa para o estabelecimento de conexões seguras tem a vantagem de ser um padrão não-proprietário, já que o SSL é patenteado pela Netscape [Uylio].

As principais diferenças entre o TLS e o SSL são de aspecto técnico, listadas a seguir:

- Diferenças nas funções de geração de números pseudo-aleatórios nos mecanismos de composição dos MAC's e
- Diferenças no processo de inserção de *bytes de padding*.

Apesar de bastante parecidos, o TLS 1.0 não é capaz de interagir diretamente com o SSL 3.0, mas a sua especificação descreve um mecanismo pelo qual é possível estabelecer uma comunicação segura com uma entidade que utiliza o SSL 3.0 [Jan02].

4.3.3 O SSL/TLS em um ambiente corporativo

Para prover conectividade entre duas LANs o protocolo SSL/TLS—que trabalha entre a camada de transporte e aplicação—pode se utilizar de dois artifícios: *port-fowarding* e tunelamento no nível de aplicação (chamadas de network-layer SSL). Caso contrário, a aplicação deve ser modificada para suportar o SSL, asim como acontece nos protocolos HTTPS (HTTP + SSL), POP3S (POP3 + SSL) etc. Só que prover conectividade a nível de aplicação para uma LAN corporativa não é uma solução viável.

Para o acesso remoto, as VPNs baseadas em SSL utilizam como prerrogativa o acesso simples através de um browser, o que quer dizer que não existe a necessidade de um software cliente e por consequência o acesso pode ser feito em qualquer máquina. A briga travada atualmente entre os procolos SSL e IPSec para acesso remoto VPN, deixa o SSL em desvantagem no quesito segurança. O cliente na maioria das vezes não é autenticado de forma segura, dado o acesso de qualquer máquina, e nada garante o que pode estar instalado nesta máquina ou o que pode ter sido "deixado para trás". Além disso aplicações legadas (como Citrix MetaFrame) necessitam de componentes baixados de forma transparente, o que faz a solução não ser tão "*clientless*" assim. Este trabalho não tem como objetivo analisar o acesso remoto VPN, ficando portanto restrito aos comentários apresentados nesta sessão. Uma pesquisa interessante sobre análise de soluções baseadas em SSL para o acesso remoto pode ser encontrada em [Gre].

A utilização de *port-forwarding* exige aplicações "bem comportadas" (aplicações que utilizam portas bem definidas). Do ponto de vista de uma solução corporativa, onde nem todas as aplicações utilizam portas bem definidas, essa abordagem soa como um "quebra-galho", restrita a algumas aplicações e não atendendo à conectividade desejada.

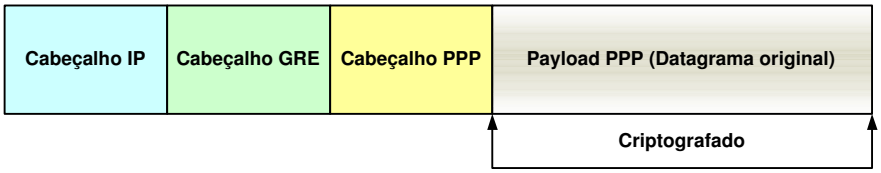

Figura 4.7: *Encapsulamento PPTP*

Uma solução proposta em [Hat02] é a utilização do PPP sobre SSL para estabelecer o canal seguro *LAN-to-LAN*. Além do overhead da pilha de protocolos, o gerenciamento desta solução é pouco escalável, sendo necessário configurar cada gateway tornando inviável a utilização de algum tipo de *mesh*. Conforme apresentado pelos próprios autores, a utilização de protocolos não orientados a conexão sobre o TCP pode trazer vários problemas [Hat02].

4.4 PPTP

O PPTP foi desenvolvido com base nos protocolos PPP (*Point-to-point protocol*) e no GRE (*Generic Routing Encapsulation*) e tem como objetivo prover um mecanismo para o tunelamento seguro de tráfego IP [Sim94].

Antes de enviar um pacote IP, o PPTP criptografa e encapsula o mesmo em um pacote PPP, o qual é encapsulado em um pacote GRE, conforme Figura 4.7.

Como acontece com outros protocolos, O PPTP também precisa que as duas partes envolvidas em uma comunicação negociem os parâmetros de proteção envolvidos na mesma. Porém, este processo de negociação não é protegido, permitindo que um atacante modifique os dados como o endereço IP dos extremos do túnel, nome e versão do *software*, nome do usuário e o *hash* criptográfico da senha do usuário [Coo00].

O PPTP apresenta também uma falha quanto a transmissão das mensagens do canal de controle que é feita sem nenhuma autenticação nem proteção de integridade, permitindo que aconteça um seqüestro da conexão neste canal de controle [E. 00].

Também existe a possibilidade de um atacante gerar falsas mensagens de controle ou alterar esse tipo de mensagem em trânsito sem possibilidade de detecção.

Outra falha de segurança do PPTP é que o cliente só precisa se autenticar depois de concluída a negociação dos parâmetros da comunicação. Isto permite que atacantes façam o servidor gerar vários processos de negociação a fim de que ele tenha que negar outros (possivelmente idôneos) ou até que o servidor seja paralisado por conta disso [E. 00].

A *Microsoft* possui uma implementação do PPTP com algumas extensões proprietárias incluídas na maioria das versões do *Windows*. Por este sistema operacional ser bastante

utilizado e sua implementação do PPTP ser viável e de baixo custo, é interessante se fazer uma análise de segurança da mesma.

Um dos pontos falhos no PPTP da Microsoft diz respeito a um dos formatos de armazenamento e transmissão de *hashes* de senhas conhecido como *LanMan*. O *LanMan* é *case-insensitive*, convertendo todos os caracteres da senha (que no *Windows NT* possui 14 caracteres de extensão) para *uppercase*, diminuindo desta forma o número de *hashes* possíveis e facilitando ataques de força bruta [dRPLdG02]. Mas o que é mais grave é que esta cadeia de 14 caracteres é dividida em duas de 7 no *LanMan*. Os *hashes* para cada uma das cadeias são gerados separadamente, o que reduz o esforço de um ataque de força bruta a descobrir 2 senhas curtas de 7 caracteres. Se não existisse essa quebra da cadeia, as senhas seriam bem mais seguras, já que os *hashes* de cadeias de 14 caracteres possuem aproximadamente 6 trilhões de possibilidades a mais em relação a um *hash* gerado a partir de uma cadeia de 7 caracteres [Jan02].

Dado que as informações do processo de negociação de parâmetros do PPTP são transmitidas sem nenhum tipo de proteção de confidencialidade, um atacante pode obter o *hash* da senha de um usuário armazenada no formato *LanMan* e com esta informação, descobrir a senha original. Deve-se considerar ainda o fato de que muitos usuários escolhem senhas previsíveis e sujeitas a ataques de dicionário [Kle90], o que facilita a violação de senhas representadas e transmitidas em *LanMan*.

Apesar do *Windows NT* possuir outro formato para a manipulação das senhas de usuário, caso a compatibilidade com o *LanMan* esteja ativa, a manipulação será feita usando este formato.

Outra fragilidade da implementação do PPTP no Windows diz respeito ao tamanho e ao processo de geração de chaves criptográficas para o serviço de cifragem. Dois modos de confidencialidade são oferecidos através do algoritmo RC4 [Sch96]:

- O primeiro utiliza de chaves de 40 *bits*, que são consideradas pequenas, muito suscetíveis a ataques de força bruta e além disso as chaves geradas são baseadas nas senhas dos usuários, ou seja, todas as sessões de um mesmo usuário irão utilizar a mesma chave, a não ser que o usuário altere sua senha. Isto se torna ainda mais grave caso o atacante consiga a senha do usuário através dapor meio da sua versão *LanMan* [dRPLdG02].

- O segundo utiliza de chaves de 128 *bits*, consideradas bastante seguras. Neste modo, as chaves também são geradas com base nas senhas dos usuários, porém combinadas com um número aleatório para cada sessão. Apesar de ser mais seguro que o anterior, o uso da senha do usuário diminui bastante o número de tentativas que podem compor um ataque [Jan02]. Todas essas vulnerabilidades do PPTP implementado em *Windows* fizeram com que a *Microsoft* recomendasse a desabilitação do formato

LanMan em cenários onde é possível o uso de outras opções [dRPLdG02].

4.5 L2TP e L2TP/IPSec

4.5.1 L2TP

O L2TP (*Layer 2 Tunneling Protocol*) foi desenvolvido com base no L2F (*Layer 2 Forwarding*) e no PPTP (*Point-to-point Tunneling Protocol*). Seu principal objetivo é o encapsulamento de pacotes PPP. O L2TP pode ser utilizado sobre redes IP, X.25, Frame Relay ou ATM enquanto que o PPTP deve ser usado sempre acima do IP.

Como o L2TP faz encapsulamento de pacotes PPP, ele pode usar os mecanismos de autenticação PPP, o protocolo de controle de cifragem (*Encryption Control Protocol* - ECP) [Mey96b] e o Protocolo de compressão (*Compression Control Protocol* = CCP) [Mey96a] que são usados pelo PPP para garantir a segurança da comunicação.

O L2TP provê suporte à autenticação, garantindo que os extremos do túnel sejam autenticados, porém não provê mecanismos de proteção do túnel L2TP, o que expõe tanto os pacotes de dados quanto os pacotes de controle a alguns tipos de ataque, tais como:

- Obtenção da identidade do usuário por meio da observação dos pacotes
- Alteração dos pacotes de dados de dados e controle
- Seqüestro do túnel L2TP ou da conexão PPP dentro do túnel
- Ataques de negação de serviço contra a conexão PPP ou o túnel L2TP
- Interrupção da negociação PPP ECP com o objetivo de remover a proteção de confidencialidade
- Interrupção ou enfraquecimento do processo de autenticação PPP, com a possibilidade inclusive de conseguir acesso à senha do usuário [Pat01].

Levando-se em consideração todos os problemas de segurança apresentados anteriormente, é recomendado o uso combinado do L2TP com outros protocolos que possam suprir sua falta de serviços de segurança, quando o L2TP for aplicado a um cenário onde existe uma rede não confiável (Internet, por exemplo) entre os extremos de um túnel [dRPLdG02].

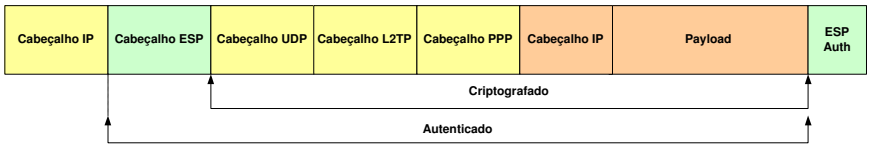

Figura 4.8: *L2TP + IPSec em modo transporte*

4.5.2 L2TP sobre IPSEC

Existem muitas propostas para se combinar o L2TP com outros protocolos a fim de solucionar os problemas de segurança do mesmo. Uma destas propostas, que apresenta grande vantagem para o acesso remoto VPN é a utilização do L2TP sobre o IPSEC [dRPLdG02]. Neste tipo de configuração é possível tirar proveito dos serviços de confidencialidade, autenticidade, integridade e proteção contra *replay*, providos pelo IPSEC e também da autenticação de usuários, configuração e atribuição de endereços IP nos extremos do túnel e suporte a múltiplos protocolos providos pelo L2TP.

Quando executado sobre o IP, o L2TP é transportado através do UDP. Desta maneira, a aplicação de proteção do IPSEC sobre o L2TP pode basear-se somente no uso de seletores que filtram o tráfego L2TP [Jan02]. No entanto, o IPSEC é usado em modo transporte neste caso, sem a criação do túnel IPSEC. A Figura N3 exibe o encapsulamento de um pacote IP feito pelo L2TP sendo utilizado sobre IPSEC, protegido somente pelo ESP:

No entanto, este procedimento impacta em um *overhead* considerável na pilha de protocolos, particularmente porque o IPSEC também é necessário por motivo de segurança, já que o *Host* pode estar conectado através de um link dial up de baixa largura de banda. A causa do *overhead* é a adição de vários cabeçalhos extras no envio de dados e protocolos de controle necessários ao controle da conexão, o que pode causar problemas como a fragmentação de pacotes IP.

Esta fragmentação pode ocasionar uma queda grande no desempenho, perda de pacotes e um aumento no consumo de memória no gateway VPN para realizar a remontagem dos pacotes fragmentados, podendo até inviabilizar a solução [dRPLdG02]. Além disso tudo, algumas formas de ataque se aproveitam da fragmentação de pacotes IP para burlar os Firewalls.

Usando o L2TP para tunelamento, protegido pelo IPSEC, teríamos uma aplicação *Web*, por exemplo, rodando sobre pilha de protocolos mostrada na Figura 4.9. Já utilizando somente o IPSec teríamos a pilha descrita na Figura 4.10.

Um outro ponto que pode apresentar problemas é no uso do PPP, porque as características de uma camada de enlace implementada através de um túnel L2TP sobre um *backbone* IP são completamente diferentes de uma que roda sobre uma linha serial [Tow99].

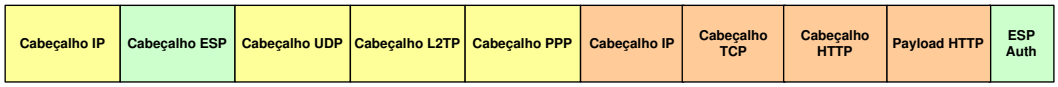

Figura 4.9: *Overhead da utilização do L2TP + IPSec*

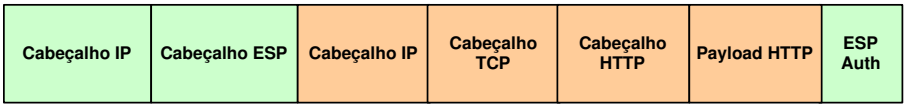

Figura 4.10: *Overhead da utilização do IPSec*

Parâmetros da conexão PPP mal escolhidos, por exemplo, podem resultar em freqüentes *resets* e *timeouts*, principalmente se a compressão estiver sendo usada. Isto acontece porque o túnel L2TP pode desordenar e até perder os pacotes, o que normalmente não ocorre em linhas seriais. A taxa de pacotes perdidos pode ser grande também devido ao congestionamento da rede [Tec00].

Outro problema no uso em conjunto do L2TP com IPSEC é que o IPSEC não consegue levar em consideração os valores dos campos de pacotes IP encapsulados pelo L2TP [dRPLdG02].

Apesar de ser a solução adotada pela *Microsoft*, é previsto a utilização do IPSec puro para o *Windows* 2003 / ISA *Server*, mas sem detalhes de como serão providos os requisitos desejáveis do L2TP, nem como serão os padrões e mecanismos de gerenciamento de chaves adotados até o momento de escrita deste trabalho.

4.6 SSH

O SSH é bastante utilizado para prover acesso seguro via *shell* e transferência de arquivos com outros servidores da rede, autenticação segura e privacidade dos dados.

Este protocolo foi desenvolvido para substituir os comandos de acesso remoto originais dos sistemas *Unix* BSD por versões seguras, prevenindo a captura de informações como senhas de usuários e o *hijacking* de conexões.

Desde que foi criado em 1995, o protocolo SSH teve várias versões, mas as principais e mais utilizadas são o SSS 1.5 (conhecido como SSH 1) e o SSH 2.0 (SSH 2) [Hat02]. As duas versões suportam o SSL e a versão 2.0 suporta também o TLS.

O estabelecimento de conexões é precedido pela negociação de algoritmos criptográficos. No SSH 2, a escolha dos métodos para a troca de chaves e geração dos MAC's fazem parte do processo de negociação de parâmetros. O primeiro passo sempre é a autenticação do servidor para tentar evitar que um cliente seja vítima de um servidor forjado por um atacante com o objetivo de capturar os dados de autenticação do cliente. Após a ocorrência

com sucesso da autenticação do servidor, é dado início à autenticação do cliente através de um dos vários mecanismos suportados pelo SSH. O mais comum é baseado no uso de senhas.

O SSH 2 suporta a consulta a autoridades certificadoras para a obtenção e validação de chaves públicas. Ele suporta também o mecanismo desenvolvido no SSH 1, no qual o próprio servidor envia sua chave pública, caso o cliente ainda não a tenha. É importante lembrar que este mecanismo expõe o cliente a servidores forjados por atacantes no momento do primeiro contato entre estes dois *Hosts*, onde as chaves públicas de ambos não são conhecidas. Por outro lado, caso a chave pública do servidor seja recebida com sucesso, as próximas conexões não estarão sujeitas a este tipo de ataque [dRPLdG02], sendo desta forma, mais seguro do que protocolos como *telnet*, no qual todo estabelecimento de conexão está sujeito a ataques como o anterior. Uma das formas de se evitar este problema no SSH é conseguir, de forma segura, as chaves públicas de servidores onde serão estabelecidas conexões SSH e guardá-las em base de dados local, evitando assim o risco de receber as chaves de maneira insegura e não confiável no primeiro contato.

Soluções utilizando o SSH em um ambiente de WAN corporativa seguem as mesmas considerações apresentadas na seção 4.3.3.

4.7 Conclusão

Por trabalhar na camada 3 do modelo OSI (*network layer*), o IPSec conta com a vantagem de oferecer transparência tanto ao usuário (principalmente se o IPSec for implementado em um gateway) quanto às aplicações. Rodando abaixo da camada de transporte (TCP , UDP), não existe a necessidade de qualquer alteração nas camadas superiores, bem como nos extremos da conexão, dando suporte a qualquer aplicação baseada em TCP ou UDP (entre outros), funcionar sem qualquer problema e de modo transparente. Além disso, os pacotes protegidos pelo IPSec são como pacotes IP comuns aos olhos dos roteadores ao longo do caminho, fazendo com que o roteamento também funcione de forma transparente e sem necessidade de modificação.

Protocolos como o SSL e o SSH são mais indicados para proteção de aplicações específicas. A utilização dos mesmos para tunelamento de tráfego entre redes remotas pode gerar um impacto na performance, no gerenciamento e na segurança, além de serem extremamente instáveis quando utilizados para tunelar protocolos como o UDP (não orientado à conexão) sobre TCP [Hat02].

O PPTP, apesar de ainda utilizado pela Microsoft, é considerado inseguro atualmente, sendo portanto não recomendado para uma grande WAN corporativa. Já o seu sucessor, o L2TP necessita do IPSec para prover todas as suas funcionalidades de forma segura. Essa dependência do IPSec implica em maior overhead, o que aponta o IPSec como a

melhor solução no momento para estabelecimento de uma comunicação segura sobre uma rede não confiável [Sch99].

Com base na análise e escolha do IPSec feita neste capítulo, o detalhamento de pontos importantes do protocolo é feito no Capítulo 5, de modo a facilitar o entendimento dos problemas e soluções apresentados no Capítulo 6.

Capítulo 5

IPSec em detalhes

5.1 Introdução

Quando o IPv4 [Pos81] foi especificado, não foi prevista a implementação de mecanismos nativos para garantir a segurança, devido ao meio em que era utilizado na época, como redes acadêmicas e militares. Como o "*boom*" da Internet, uma rede pública (no sentido de permitir acesso a qualquer pessoa) e consequentemente sujeita a todo tipo de ataques, a segurança da informação se tornou um ponto importante a ser alcançado, e por isso o IETF começou a trabalhar na especificação de extensões para o atual protocolo IP. O objetivo destas extensões era preencher as lacunas de segurança da especificação original, resultando hoje no que é chamado de *IP Security*, ou simplesmente IPSec.

A primeira vista, uma implementação de uma VPN utilizando o IPSec pode parecer simples, mas o protocolo é complexo e deve ser analisado sob vários aspectos em um grande ambiente corporativo. O objetivo deste capítulo é detalhar as particularidades do protocolo relevantes às análises das soluções propostas no Capítulo 6.

5.2 Associações de Segurança

5.2.1 Descrição

O conceito de associação de segurança, ou SA (*Security Association*) é o conceito central e talvez o mais importante na arquitetura IPSec. Uma SA é uma "conexão" *simplex* (unidirecional) que define os tipos de medidas de segurança que serão aplicadas aos pacotes, baseadas em quem está enviando o pacote, qual o destino e que tipo de *payload* ele carrega. Portanto, antes que dois *Hosts* comecem a trocar pacotes utilizando o suporte do IPSec, eles primeiro devem estabelecer uma SA.

Uma SA irá definir, com base em uma política de segurança pré estabelecida pelo

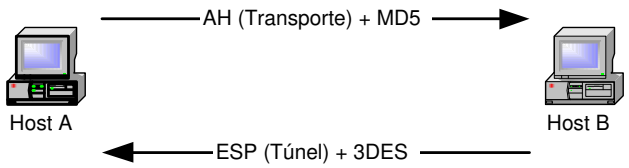

Figura 5.1: *AS com diferentes serviços de segurança*

administrador, qual o protocolo utilizado (ESP ou AH) e suas respectivas opções, qual o modo de operação (Transporte ou Túnel), algoritmos para criptografia e/ou autenticação, tamanho e valor de chaves, entre outros. Enfim, uma SA é um conjunto de informações que norteiam a comunicação segura baseada no IPSec entre dois *end-points*, e os serviços de segurança oferecidos dependem dos parâmetros definidos para cada SA.

Uma ou mais SAs podem ser criadas entre dois *Hosts*, de acordo com a granularidade definida pelo administrador. Pode-se por exemplo utilizar uma única SA para transportar todo tipo de tráfego entre os *Hosts* A e B, ou ter-se várias SAs com serviços de segurança diferentes conforme o tipo de tráfego.

Lembrando que uma SA é unidirecional, para uma comunicação nos dois sentidos é necessário o estabelecimento de duas SAs, uma para o fluxo do *Host* A para o *Host* B e outra para o sentido contrário. Isso permite também que a comunicação seja protegida por serviços de segurança diferentes em cada sentido, conforme mostra a Figura 5.1. Neste caso existe uma SA de A para B utilizando o protocolo AH em modo transporte e o algoritmo MD5 para autenticação. No sentido B para A é utilizado o ESP em modo túnel com o serviço de confidencialidade, utilizando 3DES para criptografia.

O exemplo citado serve para mostrar a importância da definição de uma boa política de segurança para o estabelecimento das SAs, além do que o simples fato da utilização do IPSec não garante a segurança do sistema. Um atacante pode explorar o sentido da comunicação que apresenta maior fragilidade, conforme apresentado em [Jan02], onde se recomenda a utilização da mesma proteção para ambos os sentidos como um cenário ideal.

As SAs são armazenadas em um repositório chamado *Security Association Database*, que será descrito adiante, e contendo informações confidenciais como chaves criptográficas e outras, deve ser armazenado em um local seguro, com acesso restrito [Hat02]. As SAs podem ser estabelecidas dinâmica ou estaticamente, embora este último caso seja mais raro por motivos de gerenciamento, escalabilidade e segurança. O serviço de proteção contra *replay* por exemplo necessita de estabelecimento dinâmico de SAs. Além disso, quanto maior for a intervenção humana, maior será a probabilidade de erros na inserção dos parâmetros e consequente falha no estabelecimento das SAs [Jan02]. Já o estabeleci-

mento de SAs de forma dinâmica se dá através do protocolo IKE (Internet Key Exchange), sem qualquer intervenção do administrador, conforme será descrito na Seção 5.4.

Uma SA é unicamente identificada por três parâmetros:

- *Endereço IP destino:* É o endereço IP do outro extremo da conexão, seja ele um *Host* ou um gateway IPSec.
- *Protocolo de segurança utilizado:* Identifica qual protocolo (AH ou ESP) está sendo utilizado. Os protocolos são identificados pelo mesmo parâmetro do campo *Next Header* do cabeçalho IP, ou seja, 51 para AH e 50 para ESP.
- *SPI (Security Parameter Index):* É um número de 32 bits geralmente escolhido pelo *Host* destino, e só tem significado dentro do mesmo. Funciona com um índice a fim de diferenciar a comunicação para um mesmo destino utilizando um mesmo protocolo de segurança.

Pode-se notar que o endereço origem não é utilizado para definir uma SA, devido ao fato de cada SA ser unidirecional, como já foi citado anteriormente (como o SPI tem significado apenas dentro do destino, é possível que o mesmo identifique a origem definida para a SA).

Com base nestes três parâmetros o *Host* destino ao receber um pacote consegue validar os serviços aplicados pela origem, com base nos parâmetros contidos na SA identificada, e dar continuidade ao seu processamento. Portanto, esta tripla deve estar sempre visível, e mesmo utilizando o serviço de confidencialidade do ESP o SPI não é incluído na porção criptografada.

5.2.2 Combinando SAs

Uma SA aplica um conjunto de serviços a um tráfego IP, e deve conter apenas um dos protocolos de segurança, nunca os dois juntos. Mas em alguns casos, é necessária a combinação de serviços que devem ser aplicados em sequência, como por exemplo a utilização do ESP para criptografia e do AH para abrangência da autenticação e integridade a todo o pacote, incluindo o cabeçalho IP mais externo ao qual o ESP não protege.

Neste caso, onde duas ou mais SAs devem ser combinadas, aplicadas uma após a outra, tem-se um mecanismo denominado de *SA bundle*[1], que nada mais é do que a combinação de duas ou mais SAs. O fato de agregar-se SAs em uma *SA bundle*, não quer dizer que devam terminar no mesmo ponto-[Atk98c], ou seja, pode-se por exemplo ter uma SA que termina em um determinado gateway, e outra aninhada que se estende até um

[1]Foi optado manter o termo em inglês por questões de linguagem técnica, a fim de não se criar novas expressões

determinado *Host*. SAs podem ser agregadas em uma *SA bundle* através de dois métodos: *transport adjacency* e *iterated tunneling*.

O modo *transport adjacency* implica na utilização dos dois protocolos de segurança (AH e ESP), sem a utilização do tunelamento. Utiliza-se o ESP, e em seguida o AH, ambos em modo trransporte. É fácil notar que a utilização de ESP sobre ESP, ou AH sobre AH não traz nenhum benefício adicional. Além disso, a utilização do AH após o ESP garante a extensão da integridade a todo o pacote, característica não alcançada pelo ESP. Apenas um nível de agrupamento é permitido, tendo em vista que sendo utilizado em modo transporte (cabeçalho IP original mantido) todo o processamento referente ao IPSec será feito no mesmo *Host* destino, sendo desnecessária a aplicação do mesmo protocolo de segurança mais de uma vez. A ordem dos protocolos (primeiro ESP, depois AH) também deve ser obedecida.

Já o modo *iterated tunneling* permite que os protocolos de segurança sejam aplicados tantas vezes quanto necessário. A diferença do método anterior é que os protocolos de segurança são aplicados em modo túnel, aninhando várias SAs umas dentro das outras, permitindo assim que cada SA termine (ou inicie) em um *Host* (ou gateway) diferente. Na verdade, três casos de *SA bundle* podem ser encontrados: a) origem e destino são os mesmos em todas as SAs agrupadas, b) somente a origem ou o destino são os mesmos para todas as SAs, ou c) as origens e destinos as SAs em uma *SA Bundle* são diferentes. Estes dois últimos casos são obrigatórios conforme especificado em [Atk98c].

5.2.3 Bancos de Dados de Segurança

Dois bancos de dados estão presentes em cada ponto com suporte ao IPSec: o *Security Policy Database* (SPD) e o *Security Association Database* (SAD). Estas estruturas servem respectivamente para armazenar as políticas de segurança definidas pelo administrador do sistema e as SAs já estabelecidas com base nestas políticas. A implementação destes bancos é interna e particular à cada implementação do IPSec, mas o comportamento dos mesmos pode ser mapeado para um nível de abstração mais genérico, importante para o entendimento do funcionamento do SAD e SPD, quais as informações presentes em cada um e como interagem entre si.

SAD

É possível definir o SAD como sendo um conjunto de parâmetros associados a cada SA ativa. Portanto, a cada SA criada, uma entrada no SAD é inserida (manualmente ou via IKE) contendo os parâmetros que a descreve. Uma SA é identificada no SAD através do SPI, do protocolo de segurança (AH ou ESP) e do endereço de IP destino. A tabela 5.1 mostra um exemplo simples de um SAD.

Tabela 5.1: Exemplo de SAD

SPI	Origem	Destino	Protocolo	Parâmetros (modo, *lifetime*, chaves etc)	Tipo	Entrada no SPD
420	192.168.18.1	172.134.19.23	ESP	(...)	Entrada	5
100	172.134.19.23	200.131.10.1	AH	(...)	Saída	3

Portanto, uma SA conterá todos os parâmetros necessários para processar um pacote pertencente a mesma. Entre os parâmetros, além da tripla que identifica a SA, pode-se encontrar:

- Modo (túnel ou transporte)
- Número de sequência dos pacotes
- *Anti-replay window*
- MTU (*Maximum Transmission Unit*)
- Algoritmo de autenticação, criptografia e chaves
- Tempo de vida das chaves
- Tempo de vida da SA

Pode-se notar na tabela 5.1 que uma SA é definida em uma única direção. Para um tráfego TCP por exemplo, irão existir duas SAs estabelecidas, uma para o tráfego de entrada e outra para o tráfego de saída.

Quando um pacote chega, com base na tripla "SPI (cabeçalho AH/ESP) + IP Destino (cabeçalho IP) + Protocolo (cabeçalho IP)" a entrada no SAD é encontrada. Se neste ponto não for encontrada nenhuma SA o pacote é descartado. Com base nos parâmetros armazenados no SAD para esta SA, o pacote é processado de acordo com o serviço de segurança especificado, retirando assim o IPSec. A partir daí, o pacote é submetido ao processamento do SPD, descrito adiante.

Quando um pacote vai deixar o *Host*, o SPD é consultado primeiro para verificar se atende à politica estabelecida e quais os serviços de segurança necessários. Com base nestas informações, uma SA que contenha os parâmetros que atenda ao serviço requisitado é procurada no SAD. Se existir, o pacote é enviado de acordo com a SA encontrada. Caso contrário, uma nova SA é negociada e inserida no SAD, permitindo então o processamento do pacote.

SPD

As SAs estabelecidas refletem a política de segurança definida pelo administrador. Esta política de segurança é composta por várias regras, nas quais os pacotes IP devem se encaixar para serem processados de acordo com o serviço desejado. Essas regras são armazenadas em uma estrutura denominada SPD, que deve ser consultada tanto para pacotes de entrada quanto de saída, garantindo assim que o fluxo de pacotes segue a política de segurança estabelecida.

É importante frisar a diferença entre SAD e SPD. O SAD contém os parâmetros que foram definidos para um determinado pacote (SA já estabelecida). Já o SPD é quem define quais e de que maneira os serviços serão aplicados. Por exemplo, o SPD diz quais algoritmos de criptografia devem ser utilizados em um determinado pacote, mas não guarda as chaves criptográficas. Estas chaves serão criadas no momento do estabelecimento da SA, sendo armazenadas portanto no SAD.

Pode-se dizer que cada entrada no SPD tem dois componentes: uma série de seletores e uma ação. Os seletores irão mapear um pacote IP para uma ação específica, que pode ser:

- *Descartar:* Não deixa que o pacote siga seu fluxo, impedindo o recebimento pelo seu destino. Este evento pode ser registrado para posterior análise de eventuais ataques ou tentativas de ataques [Jan02]
- *Executar bypass:* Deixa os pacotes seguirem sem proteção do IPSec, mantendo portanto o pacote original
- *Aplicar IPSec:* Realiza o processamento do pacote de modo que o mesmo siga com a proteção do IPSec.

Os seletores são constituídos de um parâmetro e um valor (ou faixa de valores). Os parâmetros podem ser divididos em duas categorias, conforme descrito em [Atk98c]:

- Parâmetros que podem ser identificados no pacote IP, como endereços IP, *protocol number*, portas dos protocolos de camadas superiores (TCP por exemplo) etc.
- Parâmetros derivados da autenticação, como endereços de *email*, *distinguished names* de certificados digitais etc.

A fim de tornar a política de segurança mais flexível e aumentar sua granularidade, os seletores podem ser combinados com operadores lógicos *AND*, *OR* e *NOT*. Coringas (*wildcards*) e valores do tipo "*don't care*" (ignorar) também podem ser utilizados, ajudando a reduzir o número de entradas no SPD. Em alguns casos, a política pode ser

flexível ao ponto de deixar dois pontos negociarem entre alguns algoritmos de criptografia disponíveis (por exemplo, 3DES x AES). A Tabela 5.2 mostra um exemplo de SPD com alguns seletores.

Tabela 5.2: Exemplo de SPD

Regra	IP Orig	IP Dest	Porta Orig	Porta Dest	Protocolo	Ação	SA *Index*
1	A	B	*any*	23	TCP	(Modo Túnel, ESP, AH, 3DES, MD5)	250
2	A	C	*any*	23	TCP	*bypass*	—
3	*any*	D	*any*	22	TCP	(Modo Transp, AH, SHA1)	135
4	A	B	*any*	80	TCP	(Modo Transp, ESP, 3DES, MD5)	241

É possível que mais de uma entrada no SPD seja aplicável ao pacote analisado. Como o SPD é uma lista de regras ordenada, a primeira regra que se aplicar ao pacote será selecionada. Além disso, é importante definir uma política *default* para quando nenhuma das regras se aplicar ao pacote. Geralmente por questões de segurança, o descarte do pacote é a política default [Str01].

No caso dos pacotes que chegam, após o processamento segundo as regras da SA encontrada no SAD, o SPD verifica se o pacote chegou de acordo com as políticas definidas para esta SA. Supondo-se no caso da Tabela 5.2 acima, que um pacote HTTP (porta 80) tenha chegado pela SA gerada a partir da regra 1 (lembrar que a SA é identificada pelo SPI, *End* Destino e Protocolo IPSec). Após o correto processamento do IPSec, o SPD irá verificar que estes serviços de segurança não são adequados ao protocolo HTTP, descartando o pacote.

Interação entre SAD e SPD

Como foi mostrado, o SAD e o SPD estão extremamente inter-relacionados, e o correto funcionamento do IPSec depende da interação entre estes dois bancos. Os pacotes que chegam a um determinado ponto IPSec recebe tratamento diferenciado dos pacotes que saem deste mesmo ponto, e por isso os tráfegos de entrada e saída podem ter políticas de segurança diferentes (como um SPD para tráfego de saída e um SPD para tráfego de entrada), como mostra a Figura 5.2

O fato do SPD ser consultado tanto na entrada quanto na saída pode causar um impacto significante na performance de um ponto IPSec. A complexidade das entradas de um SPD torna difícil a indexação para uma busca rápida. No caso do uso de informações

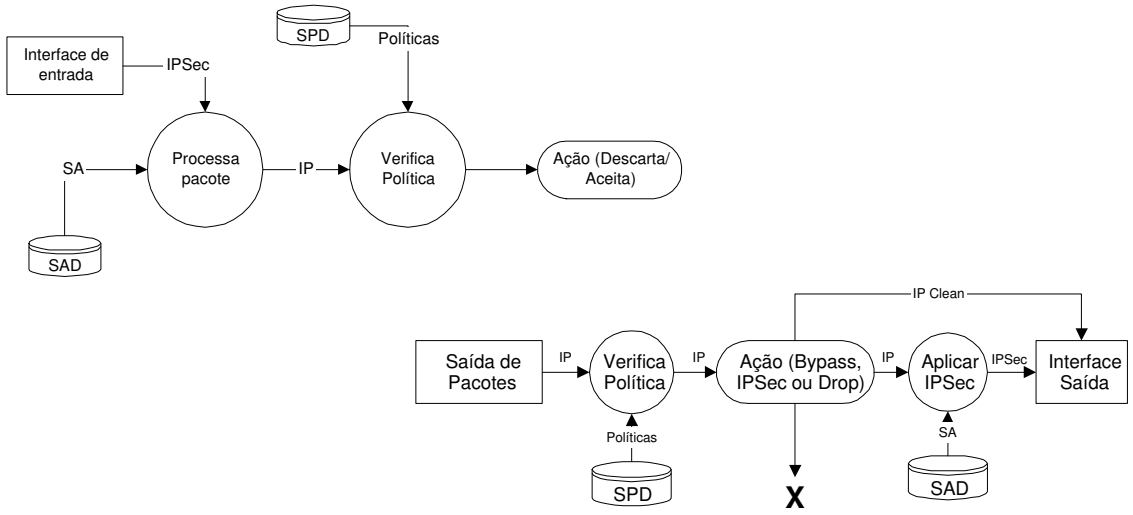

Figura 5.2: *Interação entre SAD e SPD*

relativas à autenticação para os seletores, como por exemplo o campo *distinguished name* de um certificado x509, não é possível associar informações do pacote IP diretamente ao seletor. Isso faz com que o SPD resolva estes nomes para que o pacote IP possa ser mapeado a uma determinada ação pelos seletores utilizados. Esta resolução é feita durante a fase de negociação da AS pelo IKE, descrito adiante. O SPD traduz nomes de "alto nível" como um campo *distinguished name* para uma entrada contendo endereços IP. Esse processo claro, tem um custo que também pode fazer que o SPD seja um fator impactante na performance de um ponto IPSec.

5.3 Protocolos do IPSec

Como já foi citado anteriormente o IPSec, que na verdade é uma arquitetura e não um protocolo [dS03], se baseia em dois protocolos de segurança para alcançar as funções a que se propõe. Esses protocolos que visam oferecer a proteção que faltava ao pacote IP em sua especificação original são o AH e o ESP. Nas próximas sessões será mostrado cada um deles de forma um pouco mais detalhada.

5.3.1 *Authentication Header* (AH)

O IPSec *Authentication Header* é utilizado para prover serviços de autenticação, integridade e *anti-replay* por pacote. O *checksum* do pacote original IP que detecta manipulação incorreta do pacote é facilmente recalculado, sendo necessário um serviço de

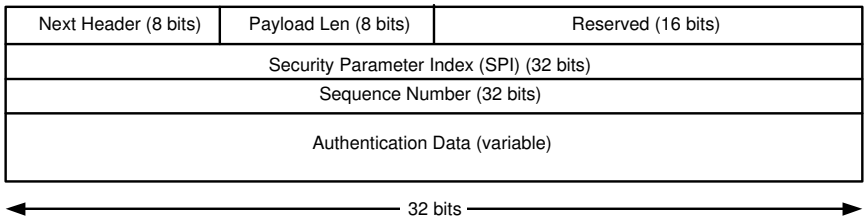

Figura 5.3: *Formato do cabeçalho do AH*

autenticação e integridade mais eficiente [Coo00]. A proteção do AH conforme mostra a Figura 5.3 se estende a todo o *payload* do pacote original e ao máximo do cabeçalho IP final possível (exceto campos mutáveis). O protocolo AH não provê confidencialidade (criptografia).

Quando o cabeçalho AH é inserido após o cabeçalho IP, o campo *next header* do cabeçalho IP passa a conter o valor 51, indicando que após o cabeçalho IP será encontrado um cabeçalho IPSec AH. O valor original da campo *next header* do cabeçalho IP será incluído no cabeçalho AH, indicando qual era realmente o tipo do *payload* do pacote IP original (TCP, UDP, ICMP etc).

O cabeçalho do AH consiste em seis campos:

- *Next Header:* Identifica o tipo do protocolo imediatamente após o cabeçalho do AH. Na verdade este campo terá o valor que continha o campo *Next Header* do cabeçalho IP original

- *Payload Len:* Ao contrário do que o nome indica, este campo indica o tamanho do cabeçalho AH, e não o tamanho do *payload* do pacote. O tamanho é expressado em palavras de 4 bytes menos 2 (a fim de manter consistência com o IPv6 [Str01])

- *Reserved:* Reservado para uso futuro, sendo preenchido com zeros. Usado atualmente para fins de alinhamento, fazendo com que o SPI se alinhe dentro de palavras de 32 *bits*.

- *Security Parameter Index (SPI):* Índice utilizado para indexar as SAs. Contém um valor arbitrário que em conjunto com o IP destino e o protocolo utilizado identificará unicamente uma SA para um *Host* destino.

- *Sequence Number:* Este campo é incrementado a cada pacote pelo emissor com o intuito de evitar ataques *replay*. Isso permite que o receptor cheque o número de sequência de um pacote contra uma janela de recepção, constituindo um mecanismo

anti-replay. Independente do receptor estar analisando estes valores, o emissor sempre honrará com sua atualização, sendo inclusive mais um fator limitante para o tempo de vida de uma SA (tamanho máximo de 232 - 1) [Dun01]

- *Authentication Data:* É um campo de tamanho variável, que contém o *Integrity Check Value* (ICV) deste pacote. O ICV é calculado pelo algoritmo escolhido no estabelecimento da SA, e é utilizado para verificar a integridade e autenticidade do pacote. Consistem em um MAC e *bytes de padding*, preenchidos conforme o algoritmo utilizado a fim de manter o tamanho nas fronteiras de palavras de 32 *bits*. Para cálculo do ICV são excluídos os campos TOS, *Fragment offset*, *Fragmentation flags*, TTL e *Header checksum*, passíveis de alteração durante o trajeto do percurso. Estes campos são considerados com valor zero para o cálculo do ICV. Vale lembrar que para processar corretamente os pacotes protegidos pelo AH em caso de fragmentação, o pacote deve ser remontado primeiro, para depois ser submetido a o processamento do IPSec.

5.3.2 *Encapsulating Security Payload* (ESP)

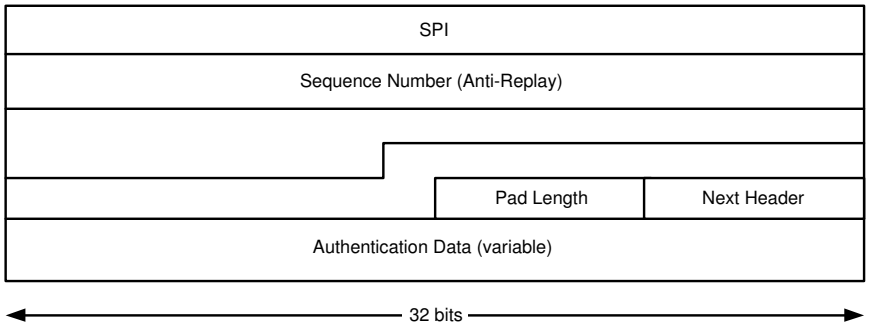

Figura 5.4: *Formato do cabeçalho do ESP*

O protocolo ESP provê autenticação, confidencialidade dos dados por meio da cifragem, e serviço opcional *anti-replay* para os pacotes IP. Autenticação e cifragem são serviços opcionais, mas sempre um dos dois deve ser selecionado, ou o protocolo não traria nenhum benefício em sua utilização. Na verdade, se a cifragem é utilizada, a autenticação é fortemente recomendada para que se evitem certos tipos de ataques [Str01].

O algoritmo criptográfico utilizado na cifragem dos pacotes é ditado pela SA pela qual o pacote será enviado (e essa SA só será estabelecida se refletir a política do SPD). Quando a cifragem não é desejada se utilizando ESP, o algoritmo *NULL* [Ken98] é utilizado, fazendo com que o ESP atue somente na autenticação do tráfego.

Assim como no AH, alguns campos adicionais são adicionados ao pacote para prover os serviços desejados, e na maioria das vezes possuem o mesmo significado que no AH (SPI, *Sequence Number*, *Next Header* e *Authentication Data*). Uma diferença é que os campos estão separados e distribuídos pelo pacote IP, criando-se assim um cabeçalho no início do pacote, um *trailer* posicionado ao final do pacote IP original seguido por um segmento de autenticação (adicionado somente quando o serviço é utilizado). O campo *Next Header* do pacote IP assume valor 50 identificando a presença do ESP.

O campo *padding* é utilizado para inserção de bytes para ajustar os blocos dos algoritmos de cifragem e autenticação, ou para procedimentos de proteção contra análise de tráfego (visando ocultar o tamanho real do pacote). O campo *Pad Length* indica o tamanho do *padding* utilizado, a fim de ser retirado corretamente após o processamento do pacote. Os campos SPI, *Sequence Number* e *Authentication Data* são autenticados, enquanto que os campos *Payload Data*, *Padding*, *Pad Length* e *Next Header* são autenticados e cifrados.

É importante lembrar que esse aumento adicional de cabeçalho, *padding* etc. resultará em um pacote maior que poderá ultrapassar o MTU e consequentemente ser fragmentado. Assim como no AH, o pacote deve ser remontado antes do processamento pelo mecanismo do IPSec.

5.3.3 AH x ESP

O AH comparado ao ESP provê um nível de proteção maior no quesito autenticação, dada a extensão da proteção aplicada ao pacote que atravessará a rede não confiável. Por outro lado, sua utilização é incompatível com um mecanismo muito utilizado pelas empresas por razões de falta de endereços IP válidos e segurança, chamado NAT. Como o NAT altera o pacote na saída para a rede externa, a utilização do AH fará com que o pacote seja descartado em seu destino. Por esse motivo o ESP vem sendo utilizado na grande maioria das VPNs baseadas em IPSec construídas até o momento, e é recomendada em [Bel04].

Além disso, a característica do IPSec prover uma gama tão grande de opções é criticada por tornar o protocolo complexo, e por consequência inseguro. A retirada do AH da especificação original do IPSec é sugerida em [Sch99]. Essa recomendação foi incorporada em uma das últimas versões do FreesWan [Tea04] antes de ser divido em duas linhas de implementação, o OpenSWan e o StrongSWan.

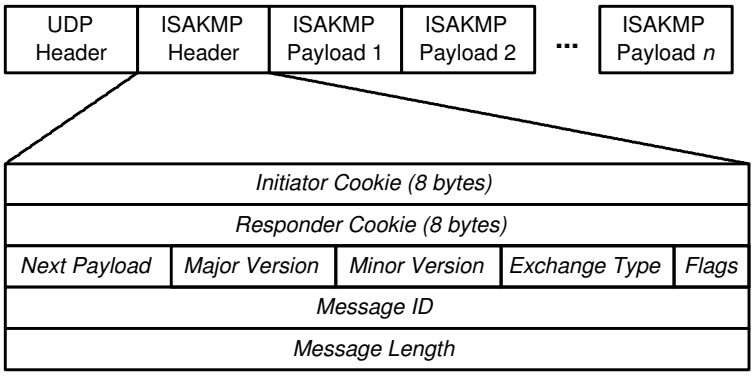

Figura 5.5: *Mensagem ISAKMP*

5.4 *Internet Key Exchange* (IKE)

5.4.1 Descrição

Apesar dos protocolos ESP e AH especificarem quais os serviços de segurança serão aplicados a um determinado fluxo de pacotes, representados por cada SA, eles não especificam como essas SAs são negociadas e estabelecidas. A fim de que essas SAs sejam negociadas dinamicamente sempre que houver necessidade, foi especificado o protocolo *Internet Key Exchange* (IKE) definido em [Car98].

Essa negociação dinâmica das SAs permite que os recursos sejam poupados devido a criação de túneis sob demanda, além de melhorar a segurança, evitando que o tempo de vida de uma SA seja configurado de modo a evitar a exposição do material criptografado a tentativas de ataques e análise.

O IKE é baseado no *framework* definido pelo protocolo ISAKMP (*Internet Security Association and Key Management Protocol*) [Tur98], implementando parte dos mecanismos de negociação de chaves OAKLEY [Tur98] e SKEME [Kra96], além de dois outros métodos [Str01].

ISAKMP define como os gateways irão negociar os serviços e chaves criptográficas, provendo também meios para autenticação. No entanto, a definição de como a autenticação é feita ou como as chaves são geradas não é responsabilidade do protocolo ISAKMP.

Uma mensagem ISAKMP consiste de um cabeçalho e vários *payloads* enfileirados em um pacote UDP (porta 500), conforme mostra a Figura 5.5. Os campos de *cookie* são utilizados para dificultar ataques de DoS[2].

ISAKMP define duas fases, descritas a seguir, onde na primeira é estabelecida uma associação de segurança ISAKMP (bi-direcional e diferente de uma IPSec SA), para que as trocas da fase 2 ocorram de forma mais rápida neste canal seguro formando assim

[2]Desde que o atacante não possa analisar o tráfego ou redirecionar as mensagens iniciais do IKE [Str01]

uma IPSec SA. Uma ISAKMP SA pode ser utilizada para negociar várias IPSec SAs, reduzindo o *overhead* de negociação para estabelecimento dos túneis.

5.4.2 Fase 1

O objetivo da fase 1 é estabelecer uma ISAKMP SA, apresentando três modos de realizar essa negociação: o *main mode*, o *aggressive mode* e o *base mode*, sendo este último pouco implementado e portanto não abordado neste trabalho.

No *main mode*, considerado mais seguro, são trocados seis pacotes formando uma sequência de 3 passos: são enviadas várias propostas para estabelecimento de uma ISAKMP SA (algoritmos criptográficos, algoritmos de autenticação, grupos Diffie-Hellman[3]), sendo escolhidas uma delas pelo *responder*; os gateways trocam material para geração das chaves criptográficas e *nonces* para evitar *replay-attacks*; os gateways trocam informações para autenticação mútua através dos mecanismos de segredo compartilhado, assinatura digital ou PKI, descritos mais adiante.

No *aggressive mode* são trocados apenas três pacotes,sendo que as propostas de SA, parâmetros de troca de chaves, *nonce* e informação de identificação são enviadas numa única mensagem. A informação de autenticação trocada entre os gateways não é cifrada. A retirada deste modo da especificação do IPSec é fortemente recomendada [Sch99].

5.4.3 Fase 2

Estando estabelecido o canal seguro formado pela ISAKMP SA na fase 1, ocorre uma troca de três pacotes estabelecendo por fim uma IPSec SA a ser armazenada no respectivo SAD. Este modo utilizado na fase 2 é chamado de *Quick Mode*.

No *Quick Mode* são escolhidos os algoritmos criptográficos e de autenticação para a IPSec SA, além do tempo de vida da SA (em segundos ou bytes), grupo Diffie-Hellman, modo transporte ou túnel e informações de chaves.

Como uma única ISAKMP pode ser utilizada para várias negociações de IPSec SAs, pode surgir a preocupação da ISAKMP SA ser comprometida e vir a comprometer todas as IPSec SAs negociadas em sequência. Um recurso chamado *Perfect Foward Secrecy* (PFS) pode ser utilizado fazendo com que uma nova negociação Diffie-Hellman seja realizada para cada nova SA. Isso pode gerar um grande impacto na performance da VPN devido ao algoritmo Diffie-Hellman ser muito oneroso [Hat02]. A Cisco por exemplo não recomenda a utilização de PFS ou trabalhar com tempo de vida das SAs muito curto, a menos que a

[3] A diferença entre os vários grupos Diffie-Hellman é o tamanho números primos utilizados nos cálculos. Os grupos 1, 2 e 5 utilizam números de 768, 1024 e 1536 *bits* respectivamente, enquanto os grupos 3 e 4 são baseados em curvas elípticas

informação seja extremamente sensível [Sys], por impactar a performance e o tráfego na rede.

5.4.4 Geração de chaves

A geração de chaves criptográficas simétricas é feita através do algoritmo Diffie-Hellman [Hel76], que permite que duas partes derivem uma chave criptográfica a partir de trocas de parâmetros publicamente conhecidos. Esses parâmetros são dois números primos muito grandes que satisfazem certas propriedades matemáticas e torna praticamente impossível derivar o segredo compartilhado a partir do tráfego capturado. Detalhes do algoritmo Diffie-Hellman estão além do escopo deste trabalho.

Como o algoritmo Diffie-Hellman é suscetível a ataques *man-in-the-middle*, os dois gateways devem estar previamente autenticados [And03], evitando o seqüestro da negociação de uma SA.

5.4.5 Métodos de Autenticação

A autenticação via IKE pode ser realizada de três maneiras: segredo compartilhado, assinaturas digitais e Infraestrutura de Chaves Públicas (PKI).

No primeiro método, o administrador deve colocar um segredo compartilhado em cada par de gateways (através de um mecanismo seguro) para que os mesmos se autentiquem mutuamente. Isso gera um problema de escalabilidade quando o número de gateways cresce muito, e principalmente quando há presença de algum tipo de *mesh*. Fica impraticável ao administrador manter uma política de renovação dos segredos compartilhados periodicamente, bem como a adição de novos *sites* implica na reconfiguração dos demais gateways. Para contornar esse problema, é comum a utilização de *wildcards*, ou seja, vários gateways compartilhando um único segredo. Esse modo é ainda mais perigoso, pois o comprometimento de um gateway pode levar o atacante à possibilidade de estabelecer um canal seguro com qualquer outro gateway que compartilhe o mesmo segredo. O uso deste método portanto não é recomendado para ambientes com alto número de gateways ou *Hosts* utilizando IPSec [Sch99, Bel04, Ste03].

No segundo método, utilizando assinaturas digitais (DSA ou RSA) cada gateway a ser autenticado assina um conteúdo com sua chave privada. Se a assinatura for validada pelo outro gateway por meio da chave pública do gateway que assinou a mensagem (utilizando portanto os princípios da criptografia assimétrica [Sch96]), a identidade pode então ser validada. Um problema encontrado neste método é a distribuição das chaves públicas, para que os gateways possam validar as assinaturas digitais.

Para resolver o problema de distribuição de chaves, além de prover uma série de informações sobre o dispositivo a ser autenticado, pode-se utilizar certificados digitais. O uso

de certificados X.509 normalmente requer a existência de uma Infra-estrutura de Chave Pública (ICP ou PKI) baseada em uma Autoridade Certificadora (*Certificate Authority* - CA) que emite e eventualmente revoga certificados de usuários e máquinas. A CA pode ser mantida dentro da empresa ou opcionalmente ser utilizado um centro de confiança oficial (como Entrust, Verisign etc.). Esta sobrecarga adicional impõe um fardo considerável no desenvolvimento inicial de uma solução VPN. Contudo, esse investimento é rapidamente compensado [Ste03]. Se um *hacker* se apoderar de uma chave privada basta revogar o certificado e publicar em uma CRL (*certificate revocation list*), disponíveis aos gateways via HTTP ou LDAP, ou mesmo de forma *on-line* via OCSP (*On-Line Certificate Status Protocol*). Além disso, um certificado tem validade determinada e expira automaticamente, sendo necessário a emissão de um novo.

Para que este processo de autenticação seja seguro, é crucial que exista uma confiança total no certificado da outra ponta. Isto pode ser feito por meio da inclusão do certificado da raiz da CA que emitiu os certificados de usuário e máquina em cada extremo da VPN. A confiança é então transferida para o certificado da CA. Se autoridades certificadoras multi-nível são usadas, então toda a cadeia de confiança deve estar disponível para cada dispositivo VPN [Edm04]. Uma implementação completa de uma PKI provê todos os meios para que os gateways se registrem junto a CA, que emitirá seus certificados e manterá todo o processo de autenticação de forma escalável e segura.

Apesar da literatura atual ressaltar as várias vantagens de uma PKI, é importante frisar que existem várias considerações a respeito da sua real segurança. Schneier descreve algumas considerações a respeito da utilização de uma infra-estrutura de chaves públicas em [Sch00], entre elas a segurança do armazenamento da chave privada e a tendência de utilização de métodos mais fáceis em detrimento da segurança, como SSO.

5.5 Conclusão

Os documentos (RFCs) apresentados pelo IETF a fim de definir o protocolo IPSec consistem de vários textos, muitos deles complexos ou extensos, o que tem ocasionado até o momento uma série de interpretações e consequentemente diferentes implementações [Dun01]. Um exemplo disso é o *client* IPSec Cisco que apresenta problemas de interoperabilidade com o novo StrongSWan, onde o campo *Vendor ID* foge da definição proposta pelo IETF.

Schneier comenta a complexidade do protocolo como um dos pontos mais críticos da especificação do IPSec [Sch99], além da flexibilidade e redundância de funcionalidades, como apresentada pelos protocolos AH e ESP. Um sistema deve ser projetado de modo que todos os mecanismos de segurança trabalhem em conjunto [Sch96]. A complexidade é uma das maiores ameaças à segurança, e a dificuldade de se realizar uma avaliação da

eficiência do protocolo não garante que ele seja cem por cento seguro. Apesar das críticas, os melhores profissionais de segurança, entre eles Bruce Schneier, apontam o IPSec como a melhor solução até o momento para o tráfego sobre um a rede não confiável.

Este trabalho tem como objetivo apresentar o protocolo de uma forma clara seguindo as definições e *drafts* propostos até o momento, e apresentar soluções simples e eficientes para uma rede complexa com vários pontos remotos. Dessa maneira é possível manter o IPSec como uma opção segura e viável. Do modo em que é apresentado nas RFCs, além de difícil entendimento é praticamente inviável aplicar o IPSec em uma VPN corporativa para o cenário proposto. O capítulo seguinte tem como missão viabilizar o IPSec neste ambiente provendo as principais características desejadas a uma grande rede.

Capítulo 6

O IPSec e o Ambiente Corporativo

6.1 Introdução

Conforme mostrado nos capítulos anteriores, o IPSec é o protocolo mais indicado para uma VPN utilizando a Internet como *backbone*, e apesar de duras críticas é indicado em [Sch99] como a solução mais segura até o momento. No entanto, deve-se ter em mente que dentre as premissas básicas de qualquer VPN, a nova tecnologia deve suprir no mínimo os requisitos das antigas já existentes no mercado (ou na organização), enfatizando o fato que uma VPN não vem para introduzir novos paradigmas na área de redes, e muito menos para resolver todos os problemas de segurança que já existiam com as WANs tradicionais, mas sim prover conectividade de forma segura e barata [Tec00].

Do ponto de vista de uma pequena corporação, contendo 2 ou 3 filiais/escritórios remotos, cujas necessidades em relação aos tipos de serviços oferecidos venham ao encontro do apresentado no Capítulo 3 para uma abordagem CPE, é fácil visualizar que o IPSec pode substituir as WANs tradicionais ou serviços de SPs, provendo comunicação eficiente e segura, pois todos os problemas de roteamento, *mesh*, configuração e gerenciamento podem ser facilmente resolvidos até mesmo de forma manual.

Voltando o foco para um grande ambiente corporativo, a alta capilaridade mostra que o IPSec ainda carece de mecanismos para prover uma solução viável e econômica. Este capítulo tem como objetivo apresentar as principais dificuldades de se implantar uma VPN baseada em IPSec, cujo o risco do custo de manutenção e gerenciamento pode acabar com qualquer chance de se conseguir o retorno do investimento. São apresentadas também soluções capazes de manter o IPSec entre as soluções viáveis a serem adotadas, mesmo pelas grandes corporações.

6.2 O problema do alto número de túneis

O cenário proposto neste trabalho é baseado no cenário existente hoje no Grupo DPaschoal, onde existem centenas de filiais (hoje em torno de 300 pontos e aumentando), que constituem pequenas redes, e uma matriz, onde se localiza a administração e principais recursos da organização. Generalizando para redes de organizações assemelhadas, pode-se visualizar duas possibilidades de análise: a da VPN provendo toda funcionalidade já existente de uma infra-estrutura legada ou a não existência atual de comunicação entre matriz-filiais (no conceito de uma WAN) e as possibilidades de uma VPN IPSec baseada em CPE neste cenário.

Partindo do segundo foco, serão apresentados vários cenários apontando suas vantagens e problemas, que implicarão em investimento versus funcionalidades desejadas, ficando a cargo do leitor a solução mais apropriada para o nível de conectividade, segurança e escalabilidade desejados. Nesta concepção, a rede do Grupo DPaschoal pode ser expandida muito além dos seus pontos de venda, o que foge do escopo deste trabalho, mas deixa o caminho aberto para sua continuação.

A definição original do IPSec, baseada na especificação do IPv6 [Hin95] previa inicialmente a capacidade de dois *Hosts* se comunicarem de forma segura (proteção *end-to-end*). A partir da adaptação do IPSec ao IPv4, e dada a possibilidade da utilização do conceito das VPNs para comunicação segura, foi concebida a utilização de uma espécie de *proxy*[1] VPN (chamado de gateway VPN) para agir em função dos *Hosts* que não possuíam suporte nativo ao IPSec, criando assim a possibilidade de utilização do protocolo como base para uma WAN [Net].

O problema é que em sua definição, o IPSec é conflitante com alguns pontos necessários a uma grande rede, conforme descrito em [Sys03b, Net, JTLE04] e citados abaixo, dificultando inclusive a utilização de alguns dos principais atrativos da substituição das WANs tradicionais por uma VPN baseada em IPSec. Entre as necessidades de uma rede com um alto número de túneis, e consequente dificuldades do IPSec, estão:

1. Roteamento dinâmico sobre o IPSec, que em sua implementação pura não permite que isso aconteça devido a decisão de roteamento estar dentro do SPD/SAD, além dos gateways VPN não possuírem endereços da mesma sub-rede, apesar de considerarem os demais gateways como vizinhos (um único *hop*), o que impede os algoritmos de roteamento de executarem sua função. Isso dificulta manter rotas de forma

[1] A idéia da palavra "*proxy*" aqui é um dispositivo provendo suporte IPSec para outros dispositivos que não o possuem. Um *proxy web* diferentemente, recebe requisições HTTP de um *Host* (há uma conexão Host-*Proxy*), e faz as requisições HTTP para a Internet em nome do *Host* que não tem permissão para isto (conexão *proxy-Internet*). A questão aqui não é falta de suporte ao protocolo, apesar do *proxy* agir em prol de outros dispositivos, mas falta de permissão para um *Host* sair diretamente à Internet via HTTP.

estática e permitir a conectividade entre *spokes* ou novas sub-redes. Fica difícil também a utilização de rotas alternativas em caso de falhas, além da dificuldade de gerenciamento e adição de novas filiais.

2. O IPSec em uma implementação pura necessita de um par de túneis (2 SA's) conforme descrito em [Atk98c], o que pode levar o número de túneis a um número inconcebível para configuração manual. No caso de uma implementação *hub-and-spoke*, o número de túneis é da ordem de O(n). Já no caso de uma topologia *mesh*, essa complexidade é da ordem de $O(n^2)$. Isso torna uma das vantagens do IPSec, a de prover conectividade de forma direta sem custos adicionais, uma dificuldade a ser vencida, dada a inviabilidade de se configurar manualmente cada gateway. Aqui surge a necessidade de túneis dinâmicos e consequentemente mecanismos de descobrimento dos gateways VPN dado um determinado endereço IP.

3. A política de segurança da rede, principalmente o controle de acesso, deve ter considerações específicas, a fim de evitar qualquer violação da política estabelecida. A topologia e a solução adotada impactam diretamente nestes quesitos, sendo o controle de acesso via Firewall, IPSec ou rede interna (i.e. *Windows Active Directory*) muito importante do ponto de vista de integração VPN - Rede da organização.

4. O dimensionamento do gateway VPN se torna um assunto de vital importância, pois pode não suportar o número de túneis iniciados/terminados pelo mesmo. Surgem questões de *clustering*, empilhamento, paralelismo etc.

5. O *link* Internet passa a receber um novo tipo de tráfego em quantidade significativa (dado o número de *sites*), devendo ser dimensionado corretamente, seja pela sua própria expansão ou pela topologia adotada, como por exemplo a utilização de mais de uma conexão com a rede pública, evitando gargalos no *link* das filiais e principalmente da matriz, o mais propenso a sofrer os efeitos deste gargalo.

Os problemas relacionados põem em risco o sucesso da solução, pois afetam de forma direta o gerenciamento e a escalabilidade. As dificuldades de se adicionar um novo *site* na rede ou realizar qualquer alteração na configuração existente podem gerar brechas na segurança e até mesmo tomar tempo e gerar eventuais falhas na VPN, deixando de lado a vantagem de rápida adição de novos *links* em relação às WANs tradicionais, bem como gerar custos adicionais diminuindo as chances de alcançar o retorno do investimento. Uma das alternativas de se colocar uma VPN em uma organização é descrita na Seção 6.5.1, e complementa os problemas relacionados nesta seção, utilizando uma implementação pura do IPSec conforme apresentado nas RFCs e na quase totalidade de livros sobre o assunto, que analisam basicamente o acesso remoto em relação à matriz ou redes com poucas sub-redes ou filiais remotas.

Foram analisados diversos tópicos e soluções com o intuito de prover alternativas para a solução dos problemas descritos, que serão detalhados nas seções seguintes. O principal foco das soluções adotadas, enumerados os problemas acima, será sustentado por 4 pilares: conectividade, disponibilidade, escalabilidade e segurança da VPN. Na verdade as soluções/cenários aqui propostos trabalham a idéia do IPSec ser utilizado como uma conexão segura ponto-a-ponto, deixando o controle de acesso fora do IPSec, seguindo o modelo de segurança em camadas [Net04a] para se prover uma solução VPN passível de suportar uma grande WAN. É importante frisar a tentativa de sempre que possível, utilizar a definição proposta atualmente pelo IETF juntamente com mecanismos já amplamente discutidos e utilizados (como os algoritmos de roteamento), o que não impede que tais soluções sirvam de possíveis sugestões para melhoria do protocolo neste cenário corporativo.

6.2.1 Considerações sobre redundância e tolerância a falhas

Quando se fala em redundância e tolerância a falhas, é importante deixar claro o objetivo deste trabalho. No caso de uma VPN, é possível enumerar os seguintes itens que podem garantir a comunicação da WAN (via VPN) em caso de falha:

- Redundância de conexões físicas com a Internet
- Redundância de gateways VPN (dispositivos físicos)
- Redundância de caminhos lógicos (túneis) em uma VPN

Existem soluções proprietárias para gateways VPN que permitem uma solução *clusterizada*, ou seja, vários equipamentos físicos provendo um único gateway logicamente. Esses dispositivos possuem mecanismos de balanceamento de carga (*load-balancing*) e em caso de falha de um dos dispositivos o gateway "lógico" permanece em funcionamento de forma transparente, apenas distribuindo maior carga entre os dispositivos ainda operantes.

Em outras soluções é possível que mais de um gateway VPN compartilhe informações de estado das conexões (SAs) e em caso de falha de um dispositivo um outro gateway assume automaticamente o gerenciamento dos túneis. Além disso podem realizar o gerenciamento de *links* físicos redundantes atingindo alto grau de confiabilidade.

Protocolos como VRRP [Lin98] e o HSRP [Li98] foram desenvolvidos para facilitar a *clusterização* e o *hot-swap* [Str01], descritos acima. Este trabalho não considera tais opções de redundância e tolerância a falhas por alguns motivos:

- As soluções são proprietárias, ocasionando na grande maioria das vezes falta de interoperabilidade, uma característica desejável em uma implementação do *framework* IPSec.

- Por consequência, na maioria das vezes a empresa fica amarrada a um determinado fabricante
- O custo destes equipamentos se torna elevado

O objetivo deste trabalho é analisar soluções padronizadas ou em discussão pelo IETF, a fim de se conseguir os objetivos desejados de segurança, baixo custo e interoperabilidade. Portanto, o roteamento dinâmico em conjunto com *mesh* dinâmico utilizando protocolos já existentes e diferentes abordagens para implementação do IPSec pode prover um bom grau de confiabilidade na VPN e por consequência na comunicação corporativa.

Claro que existem grandes diferenças entre o tempo de recuperação de uma falha com uma solução baseada em roteamento e túneis dinâmicos contra uma solução *clusterizada*. Apesar do *cluster* ser sem dúvida mais eficiente do ponto de vista da resposta a um incidente ou falha na rede, a necessidade do ponto de vista custo x benefício além das vantagens trazidas por uma solução padronizada deve ser cuidadosamente analisada.

É importante lembrar também que apesar de estar fora do escopo deste trabalho, um bom desenho das aplicações e serviços que rodarão sobre a WAN, na camada de aplicação descrita no modelo proposto na seção seguinte, prevendo eventuais períodos de falha pode ser uma alternativa para evitar gastos desnecessários com tolerância a falhas que exigem um ótimo nível de resposta. Um exemplo é o faturamento de uma filial poder ser feito mesmo na falta do *link* com a matriz, deixando informações gerenciais e atualizações em lote para serem feitas via WAN. Centralizar tudo na matriz com certeza pesa na infra-estrutura de comunicação, pois no exemplo citado a falta de comunicação com a matriz pode parar o faturamento de uma ou várias lojas.

A pergunta passa de "quanto tempo leva para a VPN se recuperar de uma falha" para "quanto tempo posso ficar sem comunicação", direcionando a empresa para a melhor solução custo x benefício.

6.3 Uma proposta de solução baseada na análise de camadas

Decididos a abordagem a ser utilizada pela VPN juntamente com o protocolo e o *backbone* escolhidos (IPSec baseada em CPE sobre Internet), a topologia será um tópico de grande importância na solução a ser adotada, pois a partir dela será possível mostrar as possibilidades e limitações da comunicação corporativa. Antes de se detalhar cada topologia, é possível analisar a rede da organização em várias camadas. Estas camadas, que compõem a rede da organização e a solução VPN como um todo, visam prover um nível de entendimento bem definido do escopo de cada uma, bem como a transparência

entre elas. As camadas superiores irão ditar as necessidades para as camadas inferiores, que devem prover os serviços necessários para a abstração requerida pela camada imediatamente superior. Com isso, ao substituir-se uma solução *Frame-Relay* por exemplo, é possível conseguir além de uma nova solução mais segura e mais barata, uma solução transparente à rede da organização.

Na grande parte da literatura existente, a integração do IPSec em uma VPN se funde com a rede da organização já existente, sendo inviável esse tipo de abordagem para uma rede maior e mais complexa, conforme será evidenciado no decorrer deste capítulo.

A rede corporativa foi dividida em 4 camadas[2], conforme listado abaixo:

1. Camada de aplicação (sistemas e recursos de rede), mostrada na Figura 6.1, que indica o fluxo de dados e as necessidades de segurança e conectividade. Apesar de na grande maioria das vezes uma solução de comunicação visar a necessidade ditada pelos sistemas e recursos disponibilizados na rede, um bom desenho de sistemas (distribuídos ou centralizados) e disponibilização de recursos (servidores de arquivo, correio etc) podem facilitar e muito a solução de rede adotada. Não adianta prover uma estrutura tipo *mesh* complexa para uma WAN se todos os sistemas e recursos estão localizados na matriz, tornando a solução baseada em *mesh* com custos e esforços elevados sub-utilizada, resultando na verdade em um simples *hub-and-spoke*.

2. Camada de rede lógica da organização, mostrada na Figura 6.2, que indica as sub-redes existentes, domínios de roteamento e zonas protegidas por Firewalls. Pode-se pensar nesta camada como o nível IP da rede da organização, como se os roteadores de borda de cada rede remota estivessem conectados diretamente, abstraindo a WAN e desconsiderando localização geográfica ou física das sub-redes e equipamentos. Os gateways VPN seriam aos olhos da rede lógica um gateway comum para se atravessar a uma outra rede/sub-rede.

3. Camada VPN, mostrada na Figura 6.3, responsável pela criação da WAN propriamente dita. Seria como uma "nuvem", provendo o mesmo nível de abstração de uma WAN tradicional. Fazendo uma analogia a Internet, a VPN seria o *backbone* da rede da corporação. No caso de existirem domínios de roteamento, onde os gateways VPN divulgam rotas que internamente são sub-divididas em sub-redes menores, pode-se dizer que os roteadores (gateways) separando essas sub-redes fazem parte da VPN, e do ponto de vista dos gateways consistem em uma faixa mais abrangente de endereços formando uma única sub-rede. Como exemplo, um GW

[2]As camadas propostas aqui são níveis de abstração de uma solução de comunicação completa utilizando uma VPN, em nada se comparando ao modelo OSI

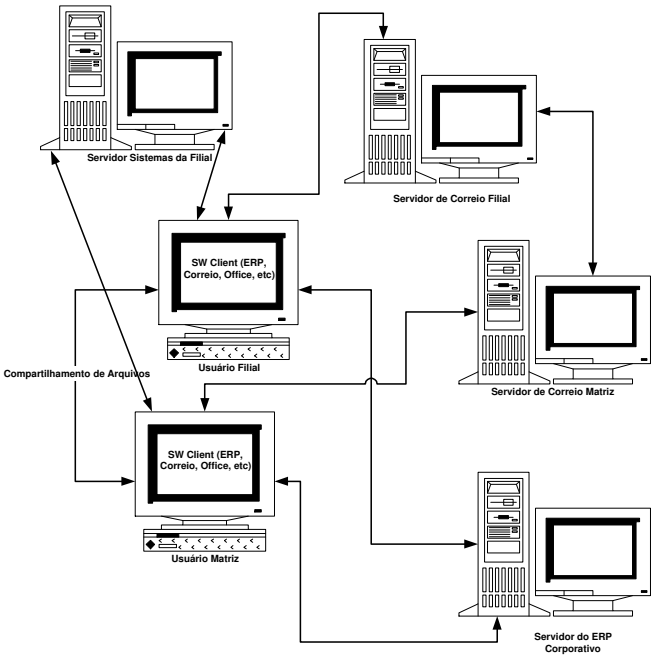

Figura 6.1: *Camada 1 - Aplicações e Serviços*

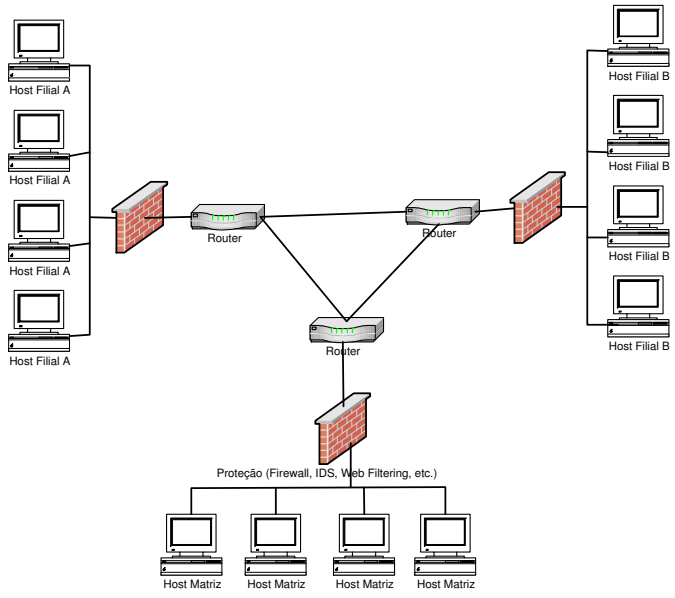

Figura 6.2: *Camada 2 - Rede Lógica da Organização*

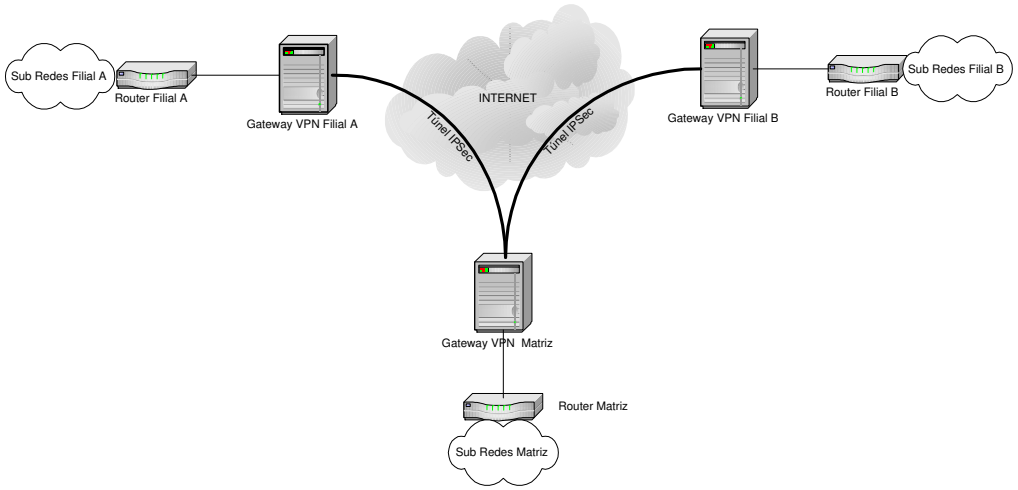

Figura 6.3: *Camada 3 - VPN*

pode divulgar que é responsável pela faixa "10.10.1.0/24", quando na verdade existem 2 sub-redes "10.10.1.0/25 e 10.10.1.126/25", pertencentes à camada de rede lógica da organização, atrás dele.

4. Camada de rede física por baixo da VPN. Nesta última camada se encontram os roteadores e endereçamentos da Internet que farão os pacotes chegarem de um gateway VPN a outro, incluindo as interfaces físicas externas dos gateways. Apesar de um gateway VPN enxergar outro gateway VPN como o próximo *hop*, o pacote passará por inúmeros roteadores existentes na Internet, atravessando portanto a rede física.

Com base nesta visão em camadas proposta aqui, serão analisados os comportamentos de cada topologia adotada e as decisões tomadas dentro das possibilidades e limitações de cada uma. A camada de aplicação por si só não é objeto de estudo deste trabalho, mas a separação em camadas direciona a solução para a utilização do IPSec provendo *links* ponto-a-ponto sem utilização do controle de acesso (IPSec). A VPN assume o papel de WAN simplesmente deixando funções de roteamento e filtragem para dispositivos externos ao IPSec, conforme detalhado adiante. É fácil visualizar que é possível encontrar algoritmos de roteamento rodando em cada camada (com exceção da primeira) de forma independente: um para a rede lógica, outro entre os gateways e um outro (ou outros) nos roteadores distribuídos pela Internet.

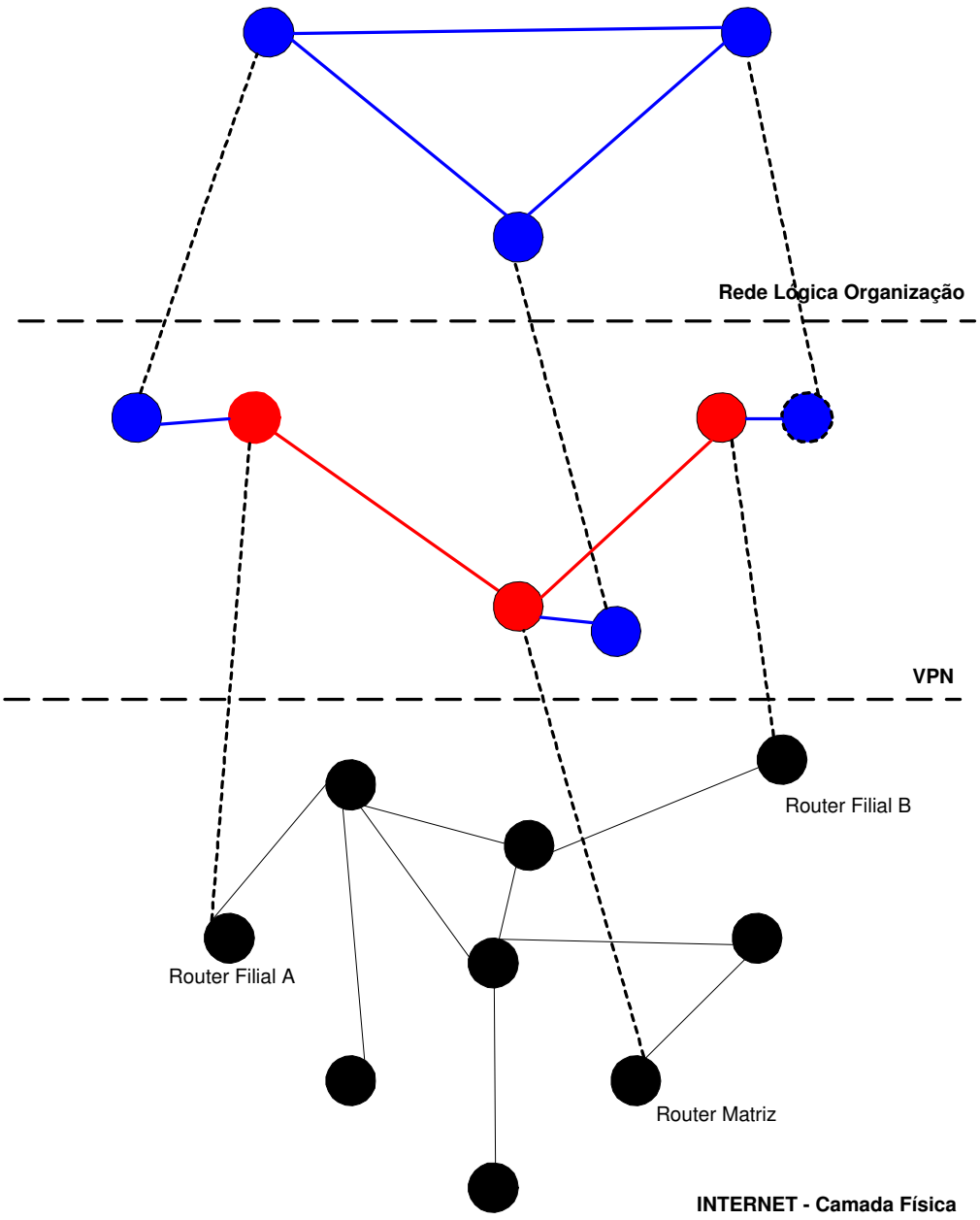

Figura 6.4: *Divisão em Camadas - Pontos de Abstração*

6.4 Considerações sobre roteamento e conectividade

6.4.1 Roteamento e Conectividade vs IPSec, o problema e as necessidades

Ao mencionar uma visão da rede corporativa em 4 camadas, e fazendo uma analogia ao modelo OSI, onde uma camada presta serviço a outra imediatamente superior mas uma mudança na camada superior não deve afetar a camada inferior, pode-se ter um ganho muito grande quando existe a possibilidade de independência das camadas "rede lógica", "VPN" e "rede física".

Do ponto de vista da rede lógica da organização, deve existir uma conectividade *any-to-any* entre as várias sub-redes, seja via roteamento estático ou dinâmico, ficando o controle de acesso a cargo dos mecanismos e políticas adotadas.

Em uma rede IP comum, onde os *sites* são conectados através de WANs tradicionais, a camada VPN e rede física acabam se fundindo, sendo que o roteador de borda consegue determinar o outro roteador de borda e ao mesmo tempo verificar o próximo *hop* (um roteador da Internet ou do *backbone* do SP) a fim de que o pacote chegue à outra sub-rede. Além disso, a única função executada é encaminhar o pacote ao destino final baseado em tabelas de roteamento. Já em uma VPN baseada em IPSec, um gateway enxerga o outro como um único *hop*, deixando as decisões de roteamento para outros dispositivos (separados ou não) e incorporando funções de filtragem.

Atuando na camada da VPN, o IPSec pode apresentar problemas ao tentar prover essa conectividade. O SPD, explicado em detalhes no Capítulo 5, é verificado para todo pacote que pretende atravessar o túnel entre os gateways. Cada entrada no SAD apresenta restrições ao (IP/rede) destino, (IP/rede) origem, protocolo, porta de origem e porta destino. Qualquer pacote com destino a uma sub-rede da organização que esteja situada em outro *site*, é enviado ao gateway VPN para que baseado no SPD encaminhe o pacote via uma SA existente no SAD ou dispare o IKE para popular o SAD com uma nova SA. Consequentemente pacotes do tipo *broadcast* e *multicast* não passam nos túneis.

Como mostra a Figura 6.5, um túnel que permita pacotes da rede B chegar a rede A deve existir no SPD/SAD. No exemplo da figura o gateway A protege a rede 192.36.4.0/24 (rede A), o gateway C protege a rede 192.36.5.0/24 (rede C) e o gateway B protege a rede 192.36.6.0/24 (rede B). Configurados os gateways manualmente (SPD) para que a rede A acesse as redes B e C, a rede B acesse a rede A e a rede C acesse a rede A, existirão 4 túneis (lembrando que uma SA é unidirecional).

Aparentemente a conectividade está estabelecida, mas fazendo os testes de transmissão conforme a Tabela 6.1, utilizando-se o comando *ping* para gerar um pacote entre dois *Hosts*, pode-se constatar o seguinte:

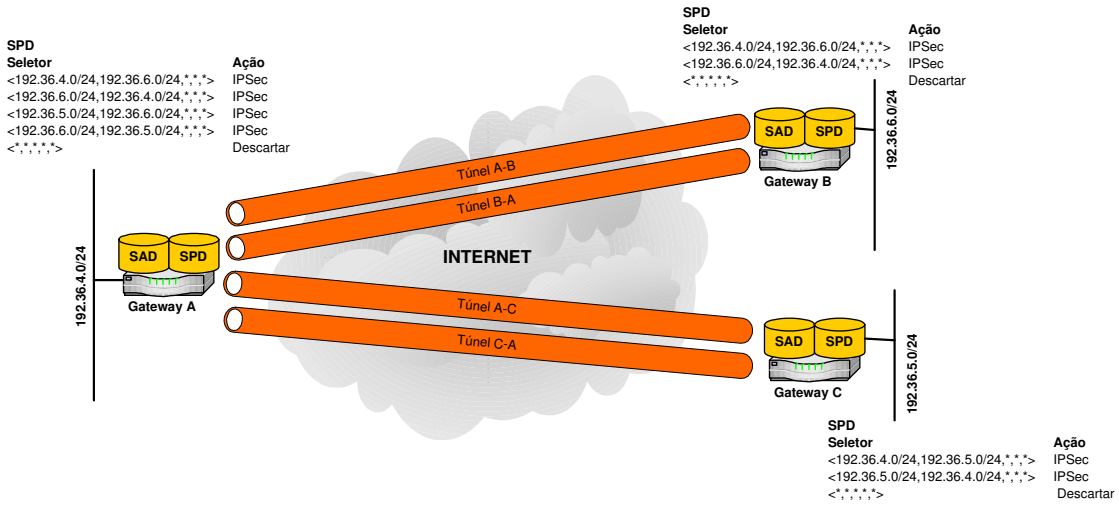

Figura 6.5: *IPSec - Túneis e Conectividade*

Tabela 6.1: Conectividade através de túneis IPSec

Origem	Destino	Resultado
192.36.4.15	192.36.5.25	*OK*
192.36.4.15	192.36.6.35	*OK*
192.36.5.25	192.36.4.15	*OK*
192.36.6.35	192.36.4.15	*OK*
192.36.5.25	192.36.6.35	FALHA
192.36.6.35	192.36.5.25	FALHA

No caso acima, as redes B e C não podem se comunicar mesmo que existam rotas no gateway A (ou outro dispositivo antes dele) pois não existe um túnel B-C. Da mesma forma, se for colocada atrás de C uma sub-rede 128.20.30.0/24 por exemplo, e populando-se as tabelas de rotas, nem mesmo A poderá se comunicar com essa nova sub-rede de C, dada a ausência de um túnel que permita este tráfego. Soluções utilizando *wildcards* (0.0.0.0) no gateway A constituem uma abordagem perigosa, pois aceitaria pacotes com qualquer destino, além de criar problemas com a criação de uma rota *default* (nem todos os pacotes necessitam ou devem ir para a rede A) e mesmo assim a sub rede em C ficaria isolada, sendo necessário um novo túnel entre B e C para comunicação direta ou um novo túnel de B para A que permita acesso à rede C, outro de A para C permitindo acesso proveniente da rede B, além de dois túneis adicionais para realizar o caminho de volta C-A-B, sendo que A deve gerenciar estes túneis de modo que pacotes com destino B ou C passando por A não sejam encaminhados para a rede interna de A.

Considerando as duas sub-redes em C, dois túneis precisam ser criados para cada par

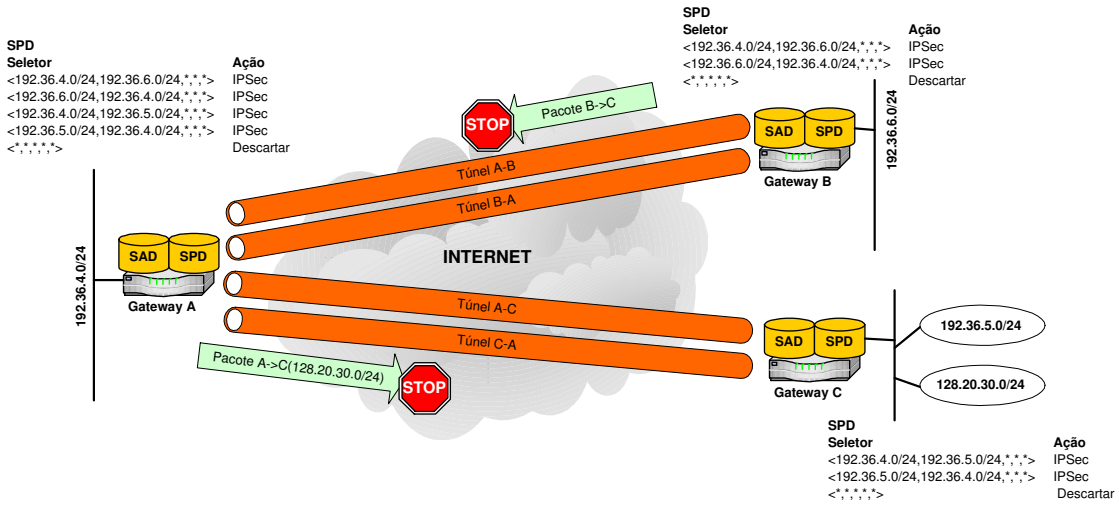

Figura 6.6: *IPSec - Conectividade vs SAD/SPD*

interessado em manter uma conectividade. Quando se aumenta o número de *sites*, a dificuldade de manter e gerenciar esse grande número de túneis e ainda atualizar corretamente a tabela de roteamento torna a tarefa do administrador um tanto quanto complicada. A Figura 6.6 mostra que se nada for alterado em relação ao SAD e ao SPD, a comunicação com a nova sub-rede ou entre C e B não será possível, conforme descrito acima.

A vantagem de se ter um controle de acesso dentro do IPSec, que pode suprir as necessidades de uma pequena rede, se torna limitante quando a complexidade e a natureza dinâmica da rede entram em cena. Sem alguns mecanismos auxiliares, o administrador de uma grande rede enfrentará constantemente dois problemas que serão tratados aqui, a conectividade e o roteamento dinâmico.

Pelos problemas do IPSec descritos acima, é possível dividir a utilização do protocolo sob duas perspectivas: uma baseada em regras(*rule-based*), que segue a implementação pura do IPSec e outra baseada no roteamento(*route-based*), seja ele estático ou dinâmico , que é parte da proposta deste trabalho para se conseguir a escalabilidade, conectividade e transparência desejadas em uma rede de alta capilaridade.

Uma montagem de VPN orientada por regras

Quando se analisa uma implementação pura do IPSec, considerando uma túnel (originado a partir de uma SA) e seus respectivos SAD e SPD, pode-se dizer que a VPN é montada orientada a regras (*rule-based* [Tec03]), visando refletir a política de segurança. Deve-se definir a topologia da VPN em primeiro lugar e então ditar, baseado na topologia escolhida, quem pode se comunicar com quem de uma maneira segura. Este tipo

de abordagem funcionou bem para os Firewalls, mas encontra suas limitações aplicadas a uma VPN [Tec03]. O principal problema é que a camada VPN está totalmente ligada à camada de rede lógica, criando-se assim rotas estáticas definidas pelo SAD/SPD.

Além de gerar problemas de redundância e tolerância a falhas devido as rotas e políticas estáticas impostas pelos gateways IPSec, problemas de gerenciamento também surgem como complicadores para o IPSec em uma grande VPN.

Existem duas maneiras de se estabelecer uma VPN baseada em regras.

A primeira é definir a topologia e então a política de segurança:

1. A empresa define a VPN e então todos os endereços IP (ou sub redes) pelos quais a VPN é responsável (na verdade, por quais domínios cada gateway é responsável).

2. A política é definida para dizer quem fala com quem (os túneis são estabelecidos)

Se a organização tem controle completo sobre sua topologia, não é difícil criar um *setup* como este, mas à medida que a VPN cresce, e a rede impõe sua natureza dinâmica, esse conceito apresenta sérias limitações. Qualquer mudança na topologia irá gerar uma alteração na VPN toda, e como cada gateway tem que enxergar a mesma topologia, algumas configurações complexas não podem ser feitas. Além disso, o número de túneis que serão criados para cada *Host* ou sub-rede pode crescer até um ponto cujo o gerenciamento fica inviável.

É o que acontece na Figura 6.5 onde B não pode se comunicar com C através de A pois não enxerga a mesma topologia de A e consequentemente a política definida para os túneis não reflete essa possibilidade de comunicação. Vale lembrar que apenas definir um túnel extra de B até A que permita falar com C, exigirá mudanças no roteamento que devem estar presentes no gateway A, para que o mesmo encaminhe o pacote de A até C.

O mesmo acontece em uma tentativa de implementar *full-mesh* em *sites* centrais (como regionais ou lojas de maior porte) e *hub-and-spoke* em alguns *sites* satélites (pequenas lojas), a fim de se aproveitar a vantagem de controle regionalizado e melhor exploração de SLAs específicos. Esta abordagem não pode suportar tais funcionalidades porque cada gateway deve enxergar exatamente a mesma topologia dos demais gateways. Assim, uma rede D adicionada atrás de C que queira se comunicar com B e A, vai enxergar todos os outros gateways como responsáveis pelos respectivos domínios de criptografia [3], e os demais gateways irão enxergar D como responsável pelo seu próprio domínio, quando D deveria enxergar C como responsável pelo resto da rede e os demais enxergar C como responsável pelo domínio de D. Isso implica em novos túneis, diretos formando um *mesh*. Pode-se estabelecer túneis entre C-A,B-A,D-C e assim por diante evitando *mesh*,

[3]Termo usado por alguns autores para definir por quais endereços ou faixas de endereços o gateway VPN é responsável

definindo políticas que façam C aceitar qualquer tráfego de D, e assim construindo túneis que permitam o tráfego passar entre os gateways, não esquecendo o roteamento, pois A ao receber um pacote de C não deve enviar o mesmo para rede interna, mas sim para outro túnel VPN.

Esse estabelecimento de túneis que faz o gateway C ser responsável por toda a rede aos olhos de D, e assim por diante, é uma segunda abordagem onde se define a topologia dentro da política de segurança. Na verdade, abstraindo-se os túneis criados, pode-se dizer que a organização define dentro da política de segurança quem fala com quem e para qual gateway deve-se enviar o tráfego. Apesar de ganhar alguma flexibilidade, mas gerar um número desordenado de túneis, ambas implementações requerem que a organização amarre a topologia da rede lógica com a VPN, e qualquer mudança na rede reflete em mudanças na política. Muitas vezes as pessoas responsáveis pela segurança não são as mesmas responsáveis pela rede, e o simples fato de se adicionar um novo servidor ou recurso pode fazer com que uma falha na conectividade passe despercebida até que alguém tente utilizá-lo (o mesmo vale para qualquer gateway que fique indisponível), sendo necessário descobrir onde está o problema e alterar toda a política da VPN (e o roteamento) para manter a conectividade. E a tendência é que com o aumento da rede, a complexidade de gerenciamento da VPN cresça exponencialmente [Tec03].

Uma montagem de VPN orientada pelo roteamento

A abordagem orientada à regras (*rule-based*) que foi apresentada na seção anterior, funde as camadas VPN e rede lógica. Uma outra abordagem para o IPSec, é a utilização do roteamento para determinar o que deve ou não passar pelos túneis ao invés das políticas contidas no SPD. Com isso, é possível separar totalmente a camada de rede lógica da camada VPN conforme proposto no modelo de camadas. Esta abordagem orientada ao roteamento (*route-based*) cria os túneis entre os pontos que desejam se comunicar, como *links* dedicados, e o roteamento determina como o tráfego chegará até o gateway VPN. Assim, a organização não necessita definir a topologia da rede para conseguir a conectividade desejada, basta definir o túnel e a rota.

Para estabelecer uma WAN utilizando uma VPN *Route-Based*, a organização precisa olhar para a topologia de sua rede (e não mais definir conforme a VPN), determinar quem deve falar com quem diretamente e montar a configuração da VPN do modo desejado (*hub-and-spoke*, *mesh* nas pontas e *hub-and-spoke* nos *sites* centrais etc.). Definida a camada VPN, a organização deve então estabelecer as rotas através dos gateways, podendo se utilizar de rotas alternativas, criando-se caminhos redundantes e adicionando confiabilidade à solução, devido à flexibilidade e redundância de uma configuração *route-based*.

Para permitir que os túneis IPSec funcionem como *links* dedicados, é necessário definir uma interface virtual para cada extremo do túnel, o que não faz parte da especificação

do IPSec pelo IETF [Atk98c]. Essas interfaces virtuais são associadas à interface física do gateway, podendo compartilhar o mesmo endereço ou utilizar qualquer endereço IP oferecendo grande flexibilidade.

O pacote ao chegar nessa interface virtual, é encapsulado em um pacote que tem como origem o gateway VPN origem e destino o gateway VPN posicionado no outro extremo do túnel, podendo-se assim utilizar os seletores de tráfego do IPSec, garantindo que somente os verdadeiros gateways se comuniquem. As maneiras de se implementar tais funcionalidades e *interfaces* serão apresentadas adiante.

É importante frisar que apesar de algumas soluções como o FreeSwan[4] apresentarem em sua implementação uma interface virtual, que tem como objetivo único capturar os pacotes e encaminhar o mesmo para o processamento do IPSec, não é possível aplicar os algoritmos de roteamento nestas *interfaces*. A idéia de uma *interface* virtual é que seja uma *interface* roteável, onde após uma decisão de roteamento o pacote possa ser encaminhado pelo túnel sem ser barrado (inverte-se a sequência filtragem-tunelamento, para tunelamento-filtragem, explicada com detalhes mais adiante).

Esta abordagem simplifica muito a implementação de uma VPN IPSec, além de aumentar e muito o potencial das funcionalidades oferecidas, mas ainda pode ter um impacto em redes de larga escala no quesito roteamento, sendo feito de forma manual, o que leva a um gasto excessivo de tempo e dificuldade de gerenciamento, apesar de maior grau de segurança. Surge portanto a necessidade de se utilizar o roteamento dinâmico sobre o IPSec, conseguindo-se algumas funcionalidades como:

- Balanceamento de carga
- Tolerância a falhas
- Gerenciamento de mudanças
- Facilidade de se adicionar novos *sites*

A implementação de uma *interface* virtual nas condições citadas acima, é capaz de prover endereços para as *interfaces* dos gateways formando uma mesma sub-rede, característica necessária para os algoritmos de roteamento que requerem o estabelecimento de algum tipo de vizinhança ou adjacência [And03]. Desta forma, é possível realizar uma ligação entre um algoritmo de roteamento e cada interface virtual, habilitando assim o roteamento dinâmico sobre o IPSec. Os túneis funcionam de modo análogo à *links* dedicados, proporcionando às organizações as mesmas facilidades de uso que as soluções

[4]Agora sucedido por duas ramificações, o OpenSwan (www.openswan.org) e o StrongSwan (www.strongswan.org).

tradicionais proporcionavam até então, com os benefícios de proporcionar um grau de segurança muito mais elevado e um custo bem inferior.

Para se realizar uma mudança no caminho dos pacotes com uma implementação pura do IPSec em modo túnel, seria necessário a recriação de SAs, o que em ordem de magnitude de tempo é muito maior que qualquer decisão de roteamento.

A configuração inicial a princípio se assemelha muito à configuração utilizando o roteamento fixo, mas a partir deste ponto as facilidades de gerenciamento e escalabilidade de uma VPN utilizando IPSec e roteamento dinâmico mostram sua superioridade. A intervenção humana é reduzida drasticamente, e a VPN é então capaz de "aprender" a topologia da rede e absorver qualquer mudança ou adição de recursos ou *sites*. Se um túnel fica indisponível por algum motivo, o algoritmo de roteamento se encarrega de achar uma rota alternativa, provendo assim um certo grau de redundância e tolerância a falhas. Assim, com pouca intervenção humana, os gastos com equipe técnica são reduzidos, tornando a solução interessante para as organizações, sendo que a partir de então a equipe responsável por definir as políticas de segurança é a única responsável por definir explicitamente os desejos da empresa, sem se preocupar com a camada VPN.

Os Firewalls voltam a ganhar em grau de importância, evitando duplicidade de políticas de segurança (muitas regras de filtragem tinham que ser replicadas no SPD), passando agora a seguir o modelo de camadas, atuando na rede lógica da organização, e seguindo o modelo "*Layered Security Model*" mostrado na Figura 7.1, definindo claramente os papéis de cada equipamento/componente na rede.

6.4.2 Soluções para prover conectividade e roteamento dinâmico sobre IPSec

Conforme já foi mencionado anteriormente, o IPSec por si só pode transportar através dos túneis os algoritmos de roteamento (assim como qualquer protocolo que rode sobre IP), mas não é possível utilizar-se destes protocolos para realizar o roteamento, pois estes algoritmos necessitam ser ligados a uma determinada interface, estabelecer relações de vizinhança, utilizar-se de mecanismos de *broadcast* e *multicast* entre outras características.

Para que seja possível trabalhar com o roteamento sobre IPSec, foram analisadas duas abordagens que visam a conformidade do *Framework IP Security* com sua especificação original (justamente para evitar questões de interoperabilidade e adoção pelo mercado), sem alterações no protocolo, além de prover a funcionalidade desejada, que é o roteamento passando sobre os túneis IPSec. Nenhuma delas foi padronizada, estando atualmente na forma de *drafts* e sendo utilizada ainda de forma "proprietária" por alguns fabricantes que apostam nas direções a serem tomadas pelo IETF e não podem fazer o mercado esperar. Um dos maiores obstáculos que o IPSec vem enfrentando é justamente a falta de

definição do padrão para troca de informação de roteamento (e o próprio encaminhamento de pacotes, feito via roteamento manual) [Gle04].

É interessante citar, embora fora do escopo deste trabalho, que com estes métodos é possível inclusive aos SPs oferecerem o IPSec como solução terceirizada para constituir o *backbone* de uma WAN corporativa, oferecendo o protocolo mais seguro atualmente para proteção fim-a-fim [Sch99], dada a possibilidade de se realizar o roteamento dinâmico entre *sites* e mantendo as tabelas de roteamento da camada VPN privadas, de modo semelhante a uma rede *Frame-Relay*.

A utilização de *wildcards* (permitir tudo) nos túneis IPSec se torna uma abordagem perigosa [Kni], sendo que nos modos apresentados a seguir é possível aplicar os seletores de origem e destino (envolvendo os gateways). Pode-se citar ainda a menor chance de erro no encaminhamento dos pacotes, devido à habilidade intrínseca do roteamento dinâmico.

Um outro problema a ser considerado quando se trata de roteamento dinâmico sobre IPSec, é a seleção do endereço de origem por parte do gateway [JTLE04]. Muitos terão várias *interfaces*, algumas virtuais, e algumas implementações podem deixar que o gateway decida qual endereço origem utilizará. Caso o mesmo não utilize como origem o extremo do túnel (na camada VPN) e pegue um endereço do GW na camada de rede física, problemas que vão de falhas na camada de aplicação até o comprometimento da segurança, como respostas em claro, podem surgir. Portanto, é necessário que o gateway utilize endereços no contexto da camada VPN, tanto para origem quanto para o destino (extremos do túnel).

IPIP sobre IPSec

Esta solução utiliza uma combinação de IP sobre IP (IPIP) seguida pelo modo transporte do IPSec. O pacote é encaminhado a uma *interface* IPIP que encapsula o pacote com os endereços de origem e destino dos gateways envolvidos na comunicação, passando em seguida para o IPSec para aplicar o modo transporte, conforme mostra a Figura 6.7. Por utilizar o protocolo IPIP definido em [Per96], as características de *interface* do túnel e seleção do endereço de origem são bem definidas.

Apesar de resultarem em pacotes aparentemente iguais no cabo, a semântica de cada um não é a mesma, ou seja, no primeiro caso, o pacote sofreu análise da política de segurança do IPSec para poder ou não ser encaminhado através de uma SA, que não constitui uma *interface*. No segundo caso, o pacote original passa pela decisão de roteamento (sofrendo análise da política de segurança antes de ser submetido ao IPSec) e é encapsulado por meio da interface virtual IPIP com endereços dos gateways (e protocolo = 4 no cabeçalho IP) e encaminhado pelo túnel que transporta o tráfego entre o gateway origem e destino.

A idéia de usar o IPIP + IPSec *Transport Mode* parece violar as regras do IPSec que

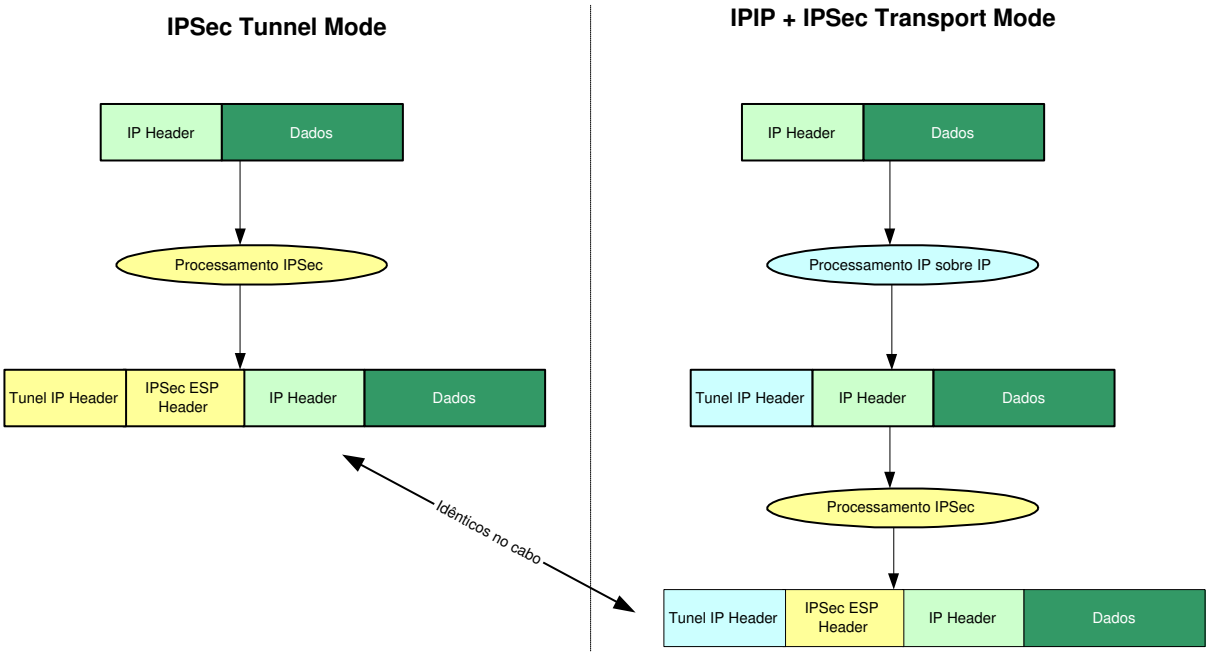

Figura 6.7: *IPSec Modo Túnel e IPIP + IPSec Modo Transporte*

diz que somente tráfego *Host-Host* deve usar *Transport Mode*, e a princípio é utilizado para comunicação *network-network*. Na verdade, este trabalho propõe que os gateways VPN atuem como roteadores de borda, e neste caso, estão enviando pacotes de um para o outro, cujo roteamento e encapsulamento foi feito anteriormente (no mesmo *Host* ou em outro), e nesse caso, descritos inclusive pelos seletores de origem destino da SA estabelecida, realizam uma comunicação *Host-Host* (cada gateway está agindo como um *Host*, ou roteadores que agora encaminham pacotes de forma segura um para o outro), estando em conformidade com a especificação original do IPSec [Atk98c]. Bellovin recomenda o uso do modo transporte para comunicações ponto-a-ponto [Bel04].

No exemplo da Figura 6.8, existem duas *interfaces* físicas (10.10.1.1 e 1.1.1.1) e uma *interface* virtual criada pelo IPIP, com endereço 10.1.1.1/30. Do mesmo modo, o gateway B apresenta 3 *interfaces* sendo que os endereços do túnel IPIP pertencem a uma mesma sub-rede, a fim de facilitar a troca de informações dos algoritmos de roteamento. A *interface* conectada na LAN faz parte da camada de rede lógica da empresa. A *interface* virtual atua na camada VPN e a *interface* externa na camada física. A habilidade de lidar com roteamento, no exemplo citado, é uma característica importante para o gateway VPN, que caso contrário deve confiar esta tarefa a um outro dispositivo e cuidar dos detalhes de interação roteador –> gateway VPN, como *reverse-path* [Coo00].

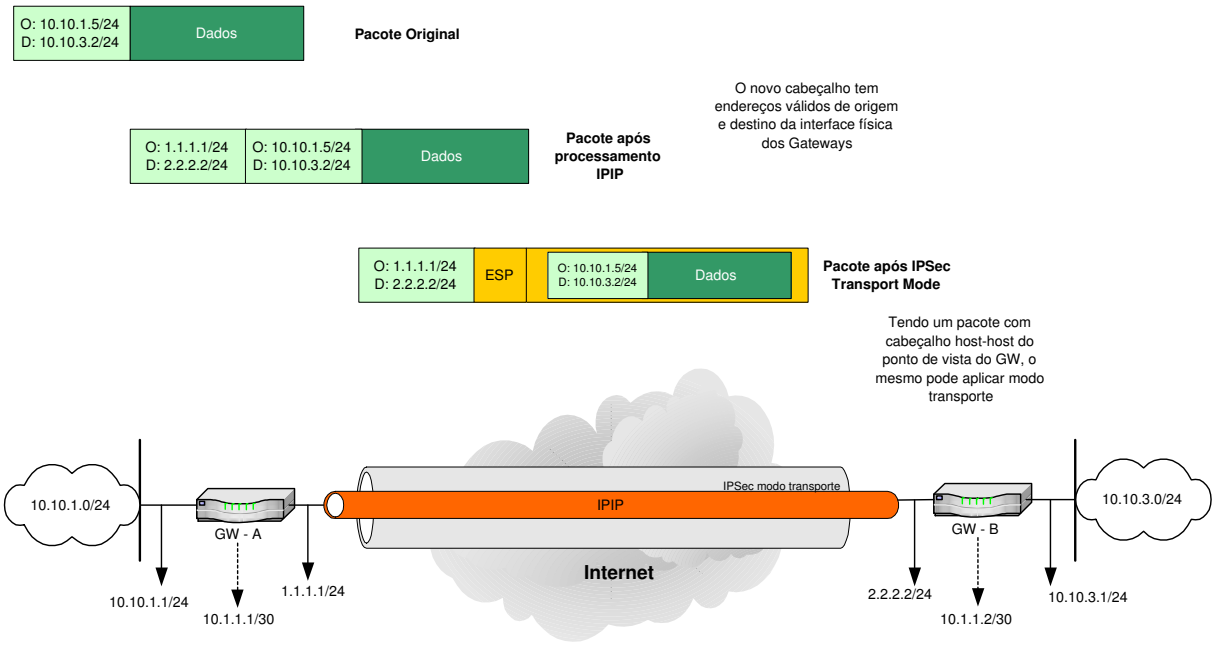

Figura 6.8: *IPIP + IPSec Transport Mode - Funcionamento*

É importante notar que ao receber o pacote original, mesmo sendo uma *interface* virtual o encapsulamento IPIP deve utilizar os endereços de origem e destino dos extremos do túnel IPSec, ou seja, os endereços das *interfaces* físicas externas de saída/entrada para cada gateway. Isso resolve também o problema de seleção da origem para o encapsulamento de pacotes de maneira modular, simplificando a utilização do IPSec, que agora só deve permitir pacotes com origem e destino dos extremos do túnel IPSec, encapsulados pelo IPIP.

No caso da *interface* externa do gateway considerada pelo IPSec utilizar um endereço inválido passando por NAT no trajeto até o gateway destino, o modo túnel com encapsulamento UDP deverá ser utilizado.

Uma característica do modo túnel do IPSec é a utilização de seletores, descritos no Capítulo 5, para verificar a existência de uma SA que se enquadre nos cabeçalhos IP ou da camada de transporte. Essa característica não é suportada pelo método descrito (IPIP + *Transport Mode* IPSec), devido à checagem da SA ocorrer ANTES do pacote original ser desencapsulado. Para isto, uma extensão na especificação do IPSec teria de ser feita [JTLE04], fazendo com que seja procurado dentro do pacote se existe algum cabeçalho de transporte aninhado dentro de outro pacote (a própria RFC 2401 reconhece essa possibilidade [Atk98c]). O fato de se utilizar o IP como uma camada de transporte válida sobre IP permite ao encapsulamento IPIP verificar o conteúdo do pacote encapsu-

lado, expressando as mesmas políticas que seriam aplicadas no IPSec. O fato é que em ambas as soluções a definição das camadas para o protocolo IP é violada, por considerar informações além do protocolo imediatamente superior. De qualquer forma, a utilização de checagem de cabeçalhos IP dificilmente será utilizada em um ambiente onde o roteamento (dinâmico principalmente onde novas redes podem ser aprendidas a qualquer instante) está presente, pois um gateway intermediário deve permitir o trânsito de pacotes através dele, além de ser mais interessante a concentração dessas políticas no Firewall, dada a separação do controle de acesso do IPSec.

Uma das características desejadas para se aplicar seletores ao cabeçalho de transporte pode ser a escolha de diferentes SAs por motivos de níveis de segurança ou mesmo QoS. O encapsulamento IPIP suporta decisões de roteamento baseadas em políticas, podendo encaminhar o pacote através de VPNs sobrepostas por exemplo.

Esta proposta parece caminhar para ser o padrão utilizado pelo IETF, apesar de existirem somente *drafts* [Gle04, JTLE04] sobre o assunto até o momento, sendo o *draft* atual, que descreve o mecanismo acima como IIPtran o único válido no momento de escrita deste trabalho. O projeto KAME[5] incorporou esta abordagem nas pilhas IPv6 e IPSec recentemente.

GRE sobre IPSec

A fim de resolver os mesmos problemas que a solução anterior (IPIP + IPSec *Transport Mode*) uma outra abordagem pode ser utilizada para permitir o roteamento dinâmico sobre IPSec. Esta abordagem utiliza o encapsulamento GRE [Tra00] ao invés do encapsulamento IPIP, sendo descrita em um *draft* não mais disponível no momento de escrita deste trabalho [Vyn02], mas utilizado e recomendado pela CISCO para prover roteamento sobre IPSec em seus gateways [Sys03b].

O encapsulamento GRE ocorre da mesma maneira que o encapsulamento IPIP, com a diferença que um cabeçalho GRE específico é adicionado ao pacote (4 bytes), além de um novo cabeçalho IP. Esse cabeçalho implica em maior *overhead* que a solução baseada em IPIP, mas tem a vantagem de carregar qualquer protocolo sobre o túnel IPSec, e não somente o IP como na solução IPIP ou mesmo em uma implementação IPSec pura.

O modo transporte também é indicado no caso de utilização do GRE como protocolo de encapsulamento antes do IPSec, o que implica que o gateway tenha endereços roteáveis via Internet, ou o modo túnel do IPSec deverá ser utilizado, gerando um *overhead* de 24 bytes no pacote IP original.

O túnel IPSec deve prover portanto restrições que aceitem somente pacotes que venham das *interfaces* GRE, com origem e destino dos gateways envolvidos na comunicação. A

[5]Detalhes do projeto KAME para plataforma BSD disponível em www.kame.net

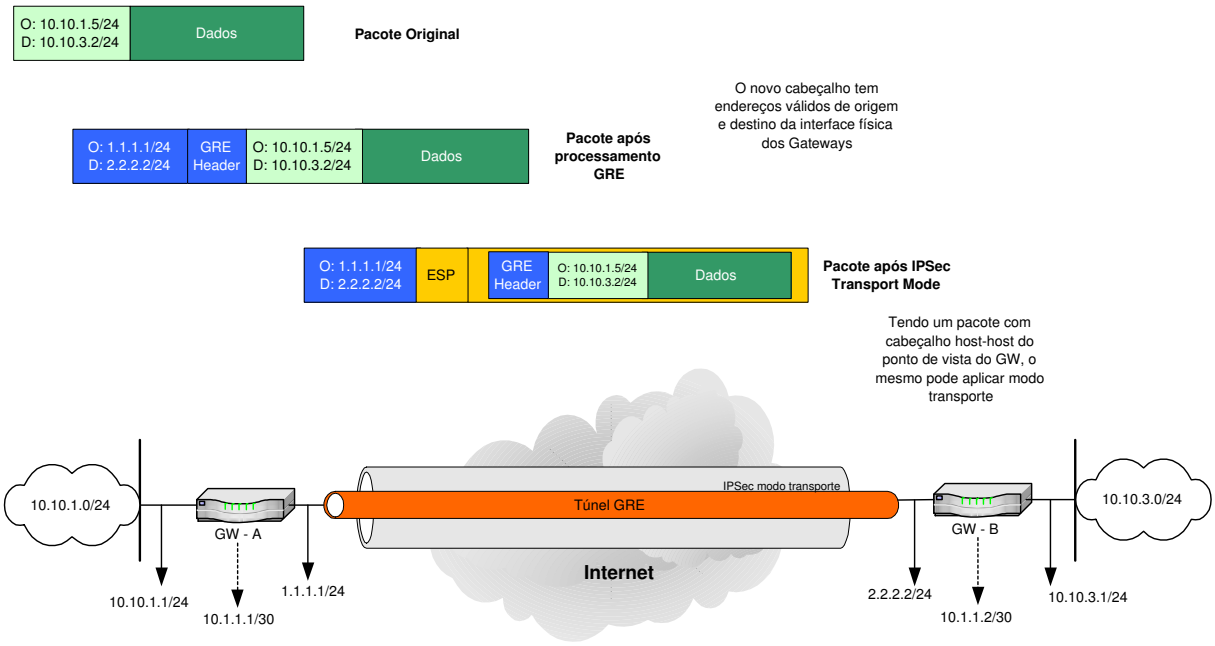

Figura 6.9: *GRE + IPSec Transport Mode - Funcionamento*

Figura 6.9 mostra o funcionamento da solução GRE + IPSec.

O *draft* proposto ao IETF analisa 3 tipos de implementações, conforme mostra a Figura 6.10. Os cenários onde o túnel GRE termina em pontos diferentes do túnel IPSec é indicado quando os gateways VPN não apresentam suporte ao roteamento. Como hoje é difícil dispositivos IPSec não incorporarem funções de roteamento, principalmente em implementações via *software* (FreeSWan, KAME etc.), além da complicação adicional de configuração roteador-gateway, a análise destes cenários foge ao escopo deste trabalho.

Da mesma maneira que qualquer outro protocolo de tunelamento utilizado sobre o IPSec, o controle de acesso deve ser executado antes do pacote chegar ao gateway VPN, evitando que tráfego não autorizado atravesse o túnel sob o encapsulamento do GRE, assim como nenhum pacote encapsulado pelo GRE deve ser aceito em claro, sem a proteção do IPSec. É recomendado em [Vyn02] que o dispositivo VPN implemente uma checagem de *Reverse-Path* baseado nas informações da tabela de roteamento montadas pelos algoritmos de roteamento, que devem ser autenticados dada a substituição de funções do SPD, além de não propagar informações de roteamento nas *interfaces* físicas que estão enviando e recebendo pacotes IPSec contendo pacotes GRE.

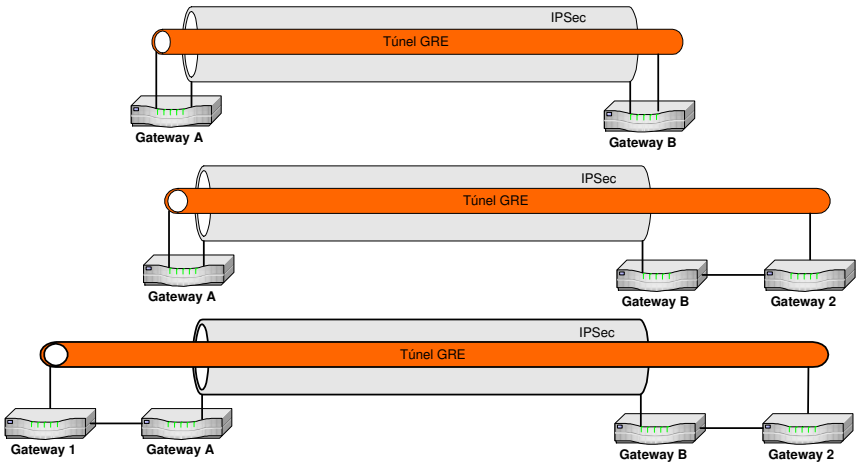

Figura 6.10: *GRE e IPSec - Modelos de Implementação*

GRE x IPIP

O IPIP apresenta interoperabilidade com o modo tunel do IPSec, o que não ocorre no GRE visto que o pacote é diferente devido ao cabeçalho GRE.

A habilidade do GRE de carregar protocolos diferentes do IP pode ser interessante em redes com outros protocolos de transporte ou roteamento, além da utilização do NHRP para mapeamento dinâmico do gateway, descrito adiante.

A Cisco propõe uma modificação na implementação do GRE chamada mGRE (*multi-point* GRE) [Sys03a]. Em uma implementação normal de IPIP ou GRE sobre IPSec, é necessário a criação de uma *interface* virtual para cada túnel entre dois gateways, pois os túneis funcionam como *links* ponto-a-ponto. No caso de 500 filiais e uma matriz em uma topologia *hub-and-spoke*, existem 500 *interfaces* no *hub* para cada túnel matriz-filial. Uma *interface* mGRE permite que vários túneis sejam terminados em uma única *interface*, simplificando a implementação e até mesmo o gerenciamento e desempenho dos algoritmos de roteamento, sem contar o mapeamento dinâmico dos gateways VPN (associação do endereço lógico da *interface* virtual ao endereço físico roteável via Internet). Esse método será exemplificado mais adiante.

O número de *interfaces* do Firewall faz a complexidade da configuração crescer exponencialmente [dG03]. Apesar da utilização de *interfaces* ponto a ponto, como no IPIP, a complexidade de configuração do Firewall central não sofrerá grandes impactos, devido a existir fisicamente uma única *interface* (física) com o gateway VPN, e os pacotes passarão cifrados pelo mesmo apenas com endereço físico do(s) gateway(s) central(is) e do gateway das filiais.

6.5 Considerações sobre mapeamento dos gateways VPN

Até o momento, o problema de conectividade foi analisado sob o ponto de vista de roteamento, sem preocupação sobre os *links* IPSec entre os gateways VPN da organização. De fato, a abstração em camadas propõe uma análise desse tipo, sendo que o roteamento entre sub-redes remotas ou não dentro de uma organização é parte do problema da camada da rede lógica. O roteamento resolve o problema de redundância e eliminação da necessidade de mudanças nos gateways devido a modificação da rede lógica (como adição de uma sub-rede em um determinado *site*), sendo a natureza dinâmica da rede refletida na rede lógica da organização pelos algoritmos de roteamento.

Em contrapartida, na camada VPN é possível encontrar várias topologias e fluxo de dados de acordo com a necessidade de comunicação. Os "*links*" IPSec podem ser definidos estaticamente ou estabelecidos dinamicamente, com ajuda de alguns mecanismos descritos a seguir, independentemente de se utilizar o roteamento dinâmico sobre qualquer uma das seguintes topologias.

6.5.1 *Hub-and-Spoke*

***Spoke-to-Hub only*, o modelo tradicional**

O modelo tradicional (ou ponto a ponto) representa a grande maioria das implementações existentes hoje nas empresas, devido à duas características básicas: baixo número de *sites* e ausência de comunicação *spoke-spoke* passando pelo *hub* (topologia estrela, numa abstração para a camada de rede lógica). No caso de necessidade de comunicação entre *sites* de filiais, um túnel direto geralmente é adotado, e devido ao baixo número de filiais existentes o controle deste tipo de solução é factível de gerenciamento e controle.

Mesmo em grandes organizações, pode ser necessário apenas o fluxo de comunicação matriz-filial e filial-matriz (ou entre poucas filiais). Neste caso, pode-se utilizar o IPSec em uma abordagem orientada a regras, explicada na Seção 6.4.1, com o SPD exercendo seu papel de controle de acesso.

Neste modelo, assume-se que a comunicação entre *sites* é previamente definida e estática (na grande maioria de túneis entre matriz e filial) e a camada de rede lógica se comporta de maneira análoga, pois a adição de novas sub-redes ou recursos em algum *site*, principalmente no *hub*, pode requerer uma reconfiguração de toda a VPN. A utilização de *wildcards* no controle de acesso pode resolver a conectividade entre alguns *sites* de modo bem restrito, mas a configuração do *hub* pode se tornar muito complexa com o

número de túneis aumentando, sendo o dimensionamento e posicionamento do mesmo de muita importância.

Portanto, este modelo só é indicado para tráfego entre matriz e filial somente, sendo que a rede lógica da empresa tenha uma natureza relativamente estática. Dessa forma, essa abordagem é extremamente escalável, sendo sua complexidade da ordem O(n) [Sys03b].

Wildcards* nos *spokes* e roteamento manual no *HUB

Para se conseguir conectividade entre filiais utilizando o modelo descrito na seção anterior, o destino de cada filial seria um *wildcard*, e o roteamento teria que fazer *split tunneling*, descrito no Capítulo 7, antes de atingir o gateway. Isso exige um Firewall bem configurado em cada filial. Caso contrário, todo o tráfego será tunelado pelo *HUB* (mesmo o tráfego Internet) podendo ocorrer problemas com PPoE *requests* no caso da utilização de ADSL por exemplo.

A adição de novas sub-redes nas filiais, se fugirem da faixa de sumarização[6] irão obrigatoriamente requerer reconfiguração do *spoke* e do *hub*. Existiriam dois túneis *hub-spoke* e um túnel *spoke-hub*(um para cada sub-rede). O gateway VPN também terá que tomar o cuidado de não encaminhar o pacote de uma filial destinada a outra para a rede interna protegida pelo mesmo. Essa configuração para um número muito grande de túneis pode se tornar inviável do ponto de vista de configuração do gateway da matriz (*hub*), sendo portanto não recomendada.

Comunicação ***Spoke-Spoke* visando aplicações**

Hoje é possível encontrar nas organizações um grande número de sistemas baseados em WEB (protocolo HTTP). Caso haja necessidade de comunicação apenas para sistemas baseados em *WEB*, não sendo portanto necessário uma conectividade a nível de rede, pode-se usar um *proxy* HTTP no *hub* central (matriz) para permitir acesso entre filiais aos sistemas locais de cada uma, conforme mostrado na Figura 6.11.

Em consequência, a VPN é limitada a apenas um tipo de serviço, sendo aplicável a situações bem específicas. Apesar disso sofre dos mesmos problemas de agregação e centralização do tráfego via *hub*, que passa a receber um fluxo de dados bem maior pelo *link* Internet. A configuração do *proxy* se torna um pouco mais complicada e trabalhosa, dependendo do nível de segurança que queira se manter no mesmo (com um *proxy web* pode-se restringir por exemplo o horário de acesso de uma determinada rede ou até mesmo usuário ou grupo de usuários [Mic02]), sendo possível barrar comunicações (conexões

[6]sub-redes que podem ou não ser agregadas em um sub-rede maior, como 10.10.1.0/24 e 10.10.2.0/24 agrupadas em 10.10.0.0/16

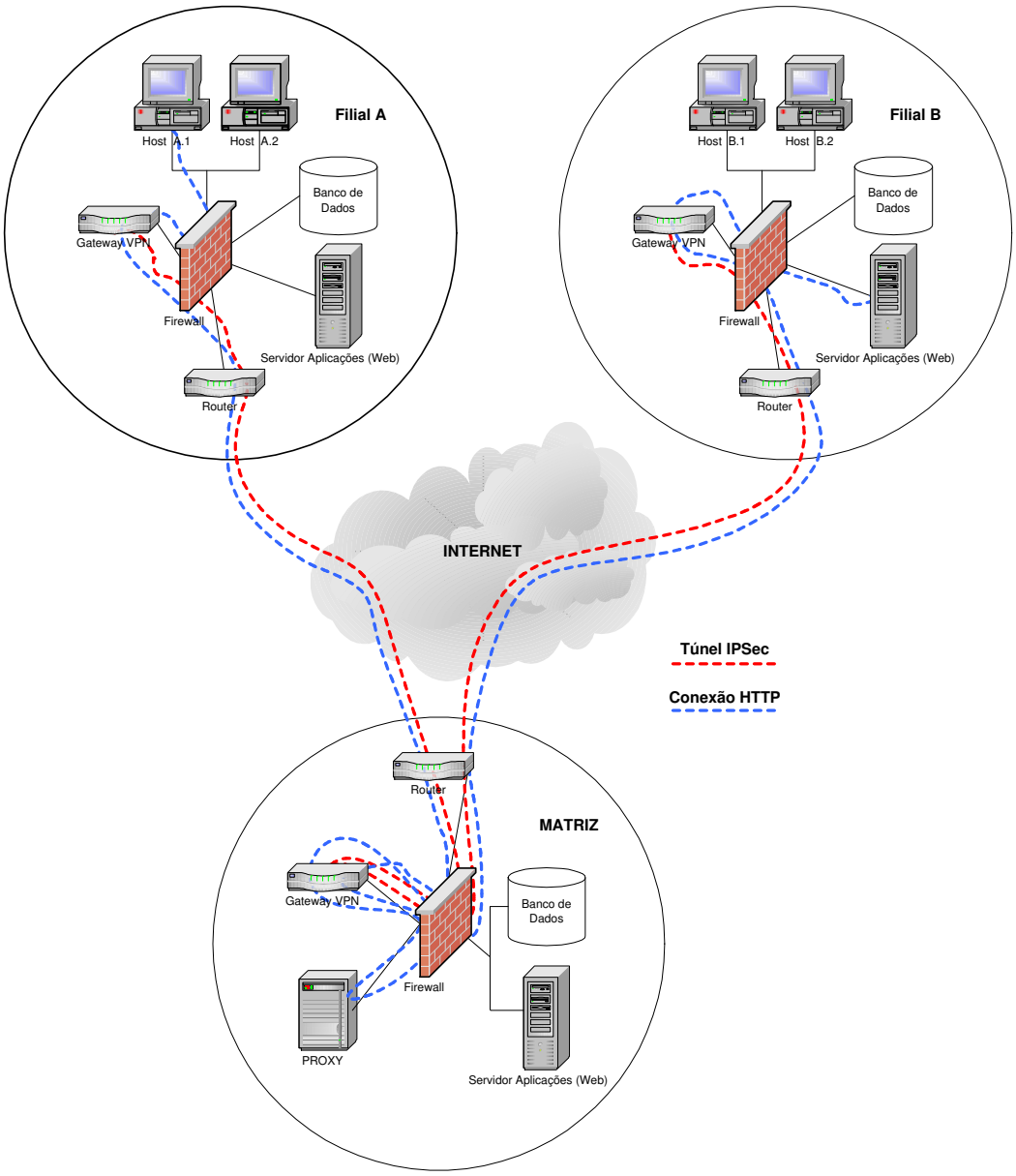

Figura 6.11: *IPSec + Proxy Web*

HTTP) entre filiais ou determinados sistemas via *proxy*. Recursos como o banco de dados ficam protegidos naturalmente pois permitem acesso somente via aplicação.

Essa configuração é perfeitamente aplicável a qualquer outro serviço que possa ser implementado via *proxy*, pois o importante é que os pacotes tenham sempre origem e destino filial-matriz ou matriz-filial respectivamente, passando nas checagens do SAD/SPD e garantindo a comunicação entre filiais. Qualquer outra comunicação que exija conectividade a nível de rede acontecerá somente entre filial e matriz, ou pode-se adotar um túnel que permita somente pacotes HTTP para o *proxy web* na matriz restringindo ainda mais a política de segurança para as filiais.

Comunicação *Spoke-Spoke* via *HUB* com roteamento dinâmico

Este modelo se assemelha a uma típica rede *frame-relay* onde várias filiais são ligadas diretamente à matriz e realizam a comunicação entre elas passando sempre pelo nó central. Do ponto de vista das camadas propostas para análise, tem-se um *full-mesh*, ou seja, pode-se alcançar uma conectividade *any-to-any* do ponto de vista da rede lógica usando uma topologia estrela na camada VPN. Este modelo segue o cenário descrito na Seção 6.4.1.

A implementação de novos *sites* é extremamente simples, bastando configurar os túneis IPIP ou GRE juntamente com o túnel IPSec até a matriz e configurar o algoritmo de roteamento nas *interfaces* virtuais que o mesmo se encarregará de distribuir toda a informação sobre a rede lógica da organização. Em contrapartida, a configuração da matriz se torna um pouco mais complicada, dado o número de túneis e interfaces a serem configurados bem como o dimensionamento da quantidade de gateways necessários para suprir as necessidades de tolerância a falhas e desempenho.

A tendência para este tipo de configuração é quando a maior parte do tráfego seja entre matriz e filial, pois no caso de comunicação entre filiais existirão 2 ciclos de criptografia (cifragem e decifragem, além de autenticação e integridade). A banda de acesso a Internet tende a ficar congestionada, pois receberá agregação de toda comunicação da WAN, mesmo o que não é pertinente (tráfego filial-filial).

O Firewall na matriz fica impossibilitado de analisar os pacotes entre filiais, pois o próprio gateway encaminhará o pacote em outro túnel, sendo o posicionamento citado em [dG02b] e pela grande maioria dos autores, que leva em consideração tráfego externo para a rede interna da matriz, sem muitos propósitos no sentido de existir um ponto único de inspeção (não há roteamento de ida e volta estando o gateway em uma interface dedicada do Firewall). É possível jogar o pacote em uma determinada *interface* de acordo com a *interface* de chegada segundo regras de Firewall configuradas manualmente, mas em um ambiente com muitas filiais tal configuração se torna impraticável.

No quesito segurança portanto, as filiais devem implementar algum dispositivo de filtragem, como um Firewall em cada filial (principalmente se o tráfego Internet da filial

não for passar pela matriz, o que é chamado de *split-tunneling*) ou utilização de recursos específicos da rede utilizada (como o *Windows Active Directory*).

O roteamento dinâmico facilita a adição de novas sub-redes ou novos *sites* além de ser um mecanismo importante para prover alta disponibilidade. O algoritmo de roteamento deve ser cuidadosamente escolhido conforme a plataforma adotada, pois em uma implementação IPIP existirão muitas *interfaces* no gateway e algoritmos como o OSPF que utilizam muita CPU podem ser um fator de impacto na solução.

Se o fluxo de dados permitir (camada de aplicação), dentro das considerações feitas nesta seção, esta configuração é a mais recomendada para uma topologia *hub-and-spoke* em uma rede corporativa de alta capilaridade.

6.5.2 *Mesh* e *Partial Mesh* com Túneis Estáticos

Prover conectividade através do IPSec através de uma topologia *hub-and-spoke* é deixar de lado um dos fatores que motivam a migração de uma WAN baseada em protocolos como o *Frame-Relay*: a criação de túneis diretos sem custos adicionais. Além de retirar da matriz uma carga de tráfego desnecessária, a comunicação direta pode proporcionar um ótimo desempenho para aplicações mais sensíveis como voz sobre IP, vídeo e outras aplicações ligadas a um requisito mínimo de QoS. O fato de existir um único ciclo de criptografia pode melhorar bastante a performance da VPN entre dois pontos isolados e por consequência da VPN como um todo.

Entretanto, quando a topologia é levada ao cenário proposto com centenas de pontos a integrarem a VPN corporativa, alguns pontos tornam a configuração estática de túneis diretos entre *sites* VPN totalmente inviável para uma configuração de *mesh* total. Caso haja utilização de *partial-mesh*, o número de *sites* que terão túneis diretos estabelecidos poderá levar ao mesmo impacto de um *full-mesh*, ou seja, falta de escalabilidade e gerenciamento inviável (a adição de um novo *site* por exemplo, requer reconfiguração de todos os gateways). A complexidade de um *mesh* estático é $O(n^2)$ [Sys03b].

O controle de acesso merece considerações especiais, não sendo mais possível concentrar tudo no *HUB*, pois os pacotes passarão direto de filial para filial. A política de segurança deve ser distribuída pelos *sites* da organização de modo a refletir a política definida para a rede como um todo.

O dimensionamento dos *hubs* pode ser calculado estatisticamente, sendo necessário que suportem o que vai estar realmente em uso (quase impossível um *full-mesh* estático, que exige um gateway muito bem dimensionado em cada filial, assim como na matriz), sendo portanto fator limitante no crescimento da VPN, dado que cada gateway de uma filial deverá suportar todos os demais túneis das outras filiais. No caso da configuração de

túneis estáticos[7], os mesmos consomem recursos do gateway mesmo quando não utilizados (alocação memória, CPU na renegociação etc.). No caso de uma empresa onde os gateways são ligados em um horário determinado comum, como abertura das lojas, pode levar a uma negociação de chaves que poderá gerar uma situação de sobrecarga dos gateways levando a VPN a uma paralisação.

Além disso, como todos os gateways enxergam os demais gateways como vizinhos (aplicando técnicas para conseguir roteamento dinâmico), o roteamento dinâmico passa a criar tabelas grandes em cada *site*, além de exigir muito processamento, passando também a limitar o tamanho da VPN.

No cenário proposto neste trabalho a única aplicação viável desta abordagem seria para um grau muito baixo de *partial-mesh*, onde a esmagadora maioria dos gateways das filiais se conecta apenas com a matriz, sendo o estabelecimento de túneis estáticos entre filiais para situações bem específicas e em raras exceções.

6.5.3 Topologia Hierárquica com *proxies* IPSec e roteamento dinâmico

Em uma organização como a DPaschoal existe uma divisão hierárquica em termos de negócios que compreende a matriz (central administrativa), as lojas (pontos de venda) e as regionais (unidades responsáveis por administrar um determinado grupo de lojas). Para organizações onde é possível definir-se *sites* com maior ou menor grau de importância de forma hierárquica, é possível utilizar uma topologia que combina uma mistura de *mesh* e *hub-and-spoke*, aliando-se a agregação de tráfego à divisão de negócios da organização, facilitando a administração e proporcionando melhor performance e escalabilidade da VPN.

Objetivo principal é diminuir o *fan-out* dos túneis além de concentrar o tráfego. Apesar de ter-se várias etapas de criptografia entre filial e matriz ou entre filiais de regionais diferentes, tem-se um melhor aproveitamento dos gateways, que requerem menor dimensionamento, além de facilitar o controle de acesso através de Firewalls instalados em pontos estratégicos.

As regionais funcionariam como *proxies* IPSec entre os *hubs* e as filiais [Cle03]. É importante ressaltar que o fluxo de dados é fator importante para análise, pois a real necessidade de comunicação, apesar de diminuir o número de túneis, pode levar a uma performance aquém da desejada se a comunicação *spoke-hub* for muito intensa. A matriz sofrerá pelo tráfego excessivo no *link* Internet além de queda no *throughput*, gerando uma sobrecarga desnecessária no *site* da regional, que funcionaria apenas como "passagem"

[7] o termo "túnel estático" no contexto deste capítulo significa "configurados estaticamente entre dois gateways", mas respeitando o tempo de vida da SA e sendo renegociado via IKE sempre que necessário

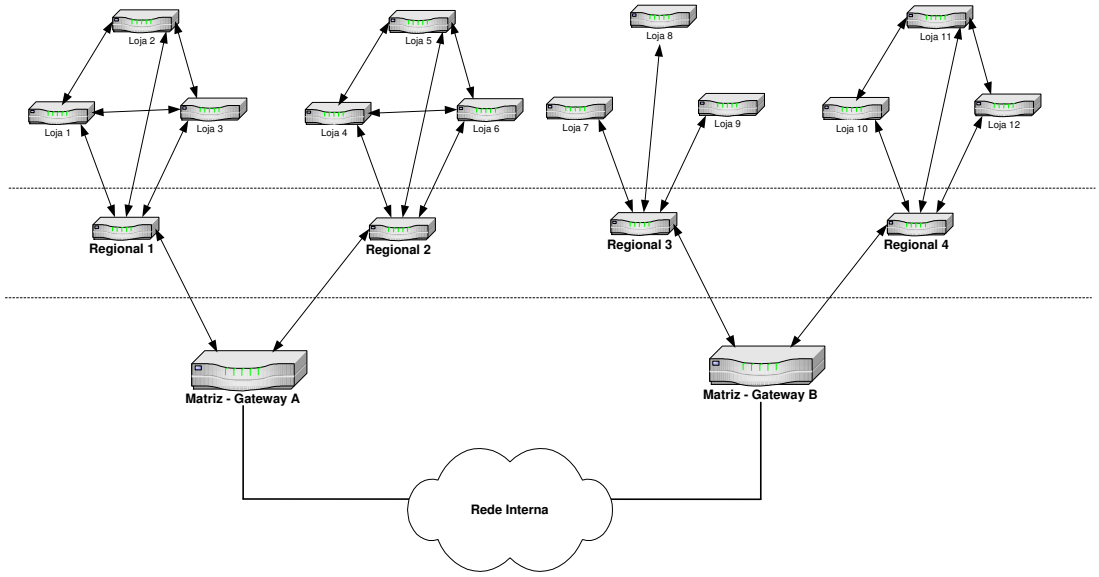

Figura 6.12: *Topologia Hierárquica - Misturando Mesh e Hub-And-Spoke*

entre filial e matriz. A Figura 6.12 mostra um exemplo de combinação de *mesh* entre as filiais de uma mesma regional e *hub-and-spoke* entre regionais e matriz.

6.5.4 *Mesh* Dinâmico

Foi explicado anteriormente a importância do roteamento dinâmico sobre o IPSec para garantir o gerenciamento e escalabilidade (entre outros fatores) de uma grande rede corporativa. Entretanto, até o momento não foi discutido o estabelecimento dos túneis IPSec sobre os quais os protocolos IPIP ou GRE realizarão suas tarefas.

O roteamento dinâmico é responsável portanto por descobrir qual o gateway VPN é responsável por um determinado endereço (no contexto da camada de rede lógica). A partir daí, o mapeamento do endereço lógico do gateway em um endereço físico roteável pela Internet pode ser feito de duas maneiras: definido estaticamente ou descoberto dinamicamente.

A primeira abordagem funciona perfeitamente em uma topologia VPN *hub-and-spoke*. Porém, a utilização de um maior ou menor grau de *mesh* torna-se complicada com um número de gateways muito grande, além da atribuição de endereços dinâmicos aos gateways pode tornar difícil a tarefa de estabelecer e manter os túneis IPSec em funcionamento.

Para este problema, quando a comunicação direta é requerida entre os diversos *sites*

de uma rede, uma solução que realize o mapeamento entre um endereço lógico da camada dois, e o endereço físico da camada VPN é de extrema importância para prover o que é chamado de "*mesh* dinâmico". A complexidade desta abordagem é algo do tipo "> O(n) e << O(n2)"[Sys03a]. Além disso, o dimensionamento dos gateways das filiais pode ser extremamente otimizado, tendo em vista que os túneis estarão estabelecidos somente quando houver necessidade, além de todas as vantagens de um túnel direto entre dois domínios de criptografia.

Existem algumas soluções proprietárias que fogem ao escopo deste trabalho. Nas subseções a seguir são apresentados algumas das propostas apresentadas ao IETF, sendo que algumas utilizam uma combinação de protocolos já definidos em RFCs. No momento da escrita deste trabalho esse assunto é abordado de forma ainda mais incipiente pelo IETF que o problema do roteamento dinâmico sobre IPSec. Portanto, o foco é realizar uma análise crítica das tendências discutidas no momento, sendo algumas já utilizadas por empresas como CISCO e Nortel Networks e até mesmo por soluções *open-source* como o FreeSwan.

Túneis Dinâmicos utilizando TED

Tunnel Endpoint Discovery (TED) é uma solução apresentada pela Cisco ao IETF [Flu02], e tem como objetivo descobrir o endereço físico de um gateway IPSec para que seja possível o estabelecimento de túneis diretos de forma dinâmica. O funcionamento do protocolo é ilustrado na Figura 6.13 e descrito pelos seguintes passos:

1. Um *Host* da rede A (*Host* A) envia um pacote destino a um *Host* de uma rede remota B (*Host* B).

2. O gateway VPN A intercepta o pacote e verifica que de acordo com as políticas de segurança deve seguir protegido pelo IPSec. Como não existe uma SA estabelecida para tunelar o pacote, o gateway VPN A descarta o mesmo e envia um *probe*[8] contendo o endereço origem do *Host* A e endereço destino do *Host* B, além da informação do endereço do gateway VPN A.

3. O gateway VPN B intercepta o pacote (*probe*) e verifica se é responsável por aplicar as políticas do IPSec para o *Host* destino B. Em caso afirmativo, envia um pacote de resposta ao gateway VPN A, incluindo o endereço do *Host* B e do *Host* A no payload do pacote.

[8]um pacote IKE (UDP porta 500 com um cabeçalho ISAKMP) gerado pelo gateway origem para descobrir qual o gateway destino responsável para aplicar o IPSec no recebimento do tráfego do pacote original

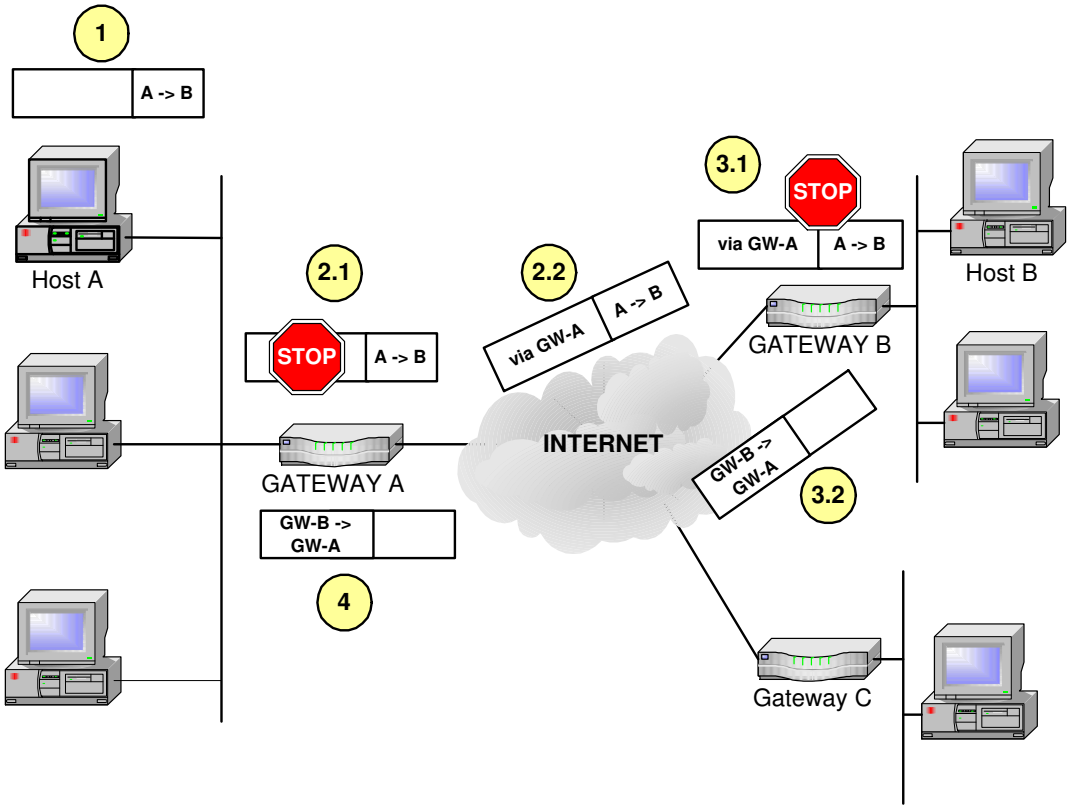

Figura 6.13: *Tunnel Endpoint Discovery - TED*

4. Quando o gateway VPN A recebe a resposta, consegue descobrir qual o gateway VPN é responsável por B, e assim iniciar uma negociação IKE entre eles para estabelecer uma SA que realize o tunelamento dos pacotes entre as redes A e B.

   Essa solução diminui consideravelmente a necessidade de configuração dos gateways VPN para estabelecimento de *mesh*, realizando a operação de forma dinâmica e trazendo os benefícios citados anteriormente para um *mesh* dinâmico.

Entretanto, essa solução utilizada atualmente pela Cisco em seus roteadores [Sys03b], apresenta algumas restrições do modo que foi proposta e é implementada atualmente de modo proprietário pela Cisco:

- Os pacotes de *probe* e resposta são enviados em claro. Isso permite análise de tráfego com base nos endereços contidos nos pacotes, que são dos *Hosts* finais envolvidos na comunicação.
- Um atacante pode enviar *probes* a um determinado gateway descobrindo os endereços pelos quais o mesmo é responsável
- Os *Hosts* protegidos por gateways que necessitam utilizar o TED para mapeamento dinâmico dos demais gateway devem utilizar endereços válidos e roteáveis na Internet. Isso é um problema quando a maioria das empresas utiliza o NAT por razões de segurança e economia de endereços IP.
- Não é possível utilizar IPIP ou GRE juntamente com o IPSec, pois o mapeamento é feito diretamente pelo IPSec e conta com o roteamento no backbone (Internet) para descobrir os gateways. Assim, enquanto o túnel IPSec não estiver estabelecido não será possível realizar a comunicação.
- Pela natureza do protocolo, com pacotes de *probe*, resposta e tempo de construção da SA, o TED pode adicionar impacto na performance da VPN.

De qualquer forma, a concepção do protocolo e sua submissão ao IETF abre campo para algumas sugestões que visam melhorar os serviços oferecidos pelo mesmo. Os pontos chaves são:

- A possibilidade de utilizar o roteamento da camada VPN (aplicada aos túneis GRE ou IPIP) para a descoberta dos gateways permite a utilização de endereços privados (NAT). Admitindo uma topologia fixa *hub-and-spoke* entre filiais e matriz, os probes seguiriam protegidos pelos túneis já existentes (com base no roteamento rodando sobre GRE ou IPIP) e ao serem recebidos pelo gateway destino gerariam

uma resposta contendo o endereço válido do gateway VPN destino, possibilitando o estabelecimento do túnel direto, utilização de NAT e comunicação *hub-and-spoke* enquanto o túnel direto é levantado (nenhum pacote do tráfego entre os *Hosts* A e B seria descartado). Nessa proposta o TED passaria a alimentar os protocolos GRE ou IPIP com novos pares de gateways IPSec para serem encapsulados e posteriormente submetidos ao modo transporte do IPSec (que detectaria automaticamente a necessidade de disparar o IKE para estabelecimento do túnel, utilizando seletores diferente do endereço IP para aplicação das políticas, dado o desconhecimento dos mesmos pelos *spokes*).

- As mensagens de *probe* e resposta deveriam ser autenticadas para evitar os ataques descritos anteriormente.

No momento de escrita deste trabalho o protocolo se apresenta como uma implementação proprietária da Cisco, mas dada a submissão ao IETF abre caminho para melhorias necessárias visando segurança e melhores funcionalidades. Atualmente é indicado para comunicação entre serviços instalados em *Hosts* com endereçamento válido, cujo roteamento via Internet é capaz de alcançar. Uma VPN visando comunicação entre *Hosts* quaisquer e envolvendo endereçamento inválido, deve adotar uma outra abordagem. Os comentários feitos aqui tem como objetivo sugerir modificações visando a viabilidade do TED em um ambiente corporativo.

Túneis Dinâmicos utilizando NHRP

O Next Hop Resolution Protocol (NHRP) é definido em [Dor98], e tem como objetivo mapear um dado endereço IP para um endereço de uma rede Non-Broadcast, Multi-Access (NBMA), e determinar qual o próximo *hop* para um destino não conectado à NBMA. Para uma solução VPN, o protocolo pode mapear o endereço de um determinado gateway no contexto da camada VPN em um endereço físico roteável pela Internet, possibilitando o mapeamento dinâmico de gateways VPN e o consequente estabelecimento de túneis diretos.

No caso do modelo proposto, levando em consideração as camadas e os túneis GRE que atuam no contexto da rede VPN fazendo a conexão com o IPSec (endereços da camada física), pode-se associar a camada física a uma NBMA. A diferença em relação ao TED é que o NHRP utiliza o roteamento fora do IPSec para mapear os pontos, enquanto o TED se baseia no roteamento existente no *backbone*, no caso a Internet.

O NHRP é utilizado em redes como Frame-Relay, e não pode ser utilizado em conjunto com o IPIP, devido a ser um protocolo que não roda sobre IP. Neste caso o GRE seria a solução viável para utilização do NHRP no mapeamento dinâmico dos gateways.

A interface GRE tradicional associa um par de endereços físicos origem e destino a um túnel GRE. Isso implica em uma interface virtual GRE para cada túnel IPSec. A solução mGRE (multi-point GRE) [Sys03a] propõe uma única interface virtual que possa associar vários destinos à interface física do gateway origem, com um mesmo endereço virtual de origem. Assim, os túneis GRE são estabelecidos sob a mesma interface, decidindo com base no roteamento qual endereço físico destino necessário, passando posteriormente ao processamento do IPSec.

O protocolo exige dois papéis a serem considerados na implementação, o Next Hop Client (NHC) e o Next Hop Server (NHS). O roteamento dinâmico fica responsável por descobrir qual o endereço da camada VPN (interface GRE) do gateway destino, e o NHRP converterá este endereço para um endereço físico permitindo o estabelecimento de um túnel IPSec direto caso não exista.

Imaginando o NHS posicionado na matriz, pode-se adotar uma topologia *hub-and-spoke* fixa entre filiais e matriz, fazendo com que o roteamento atravesse somente esses túneis estabelecidos permanentemente com a matriz (nunca os links spoke-spoke criados dinamicamente). Por esses túneis um *spoke* descobre o endereço lógico do próximo gateway (cada *spoke* realiza o papel de NHC, se registrando junto ao NHS no momento de estabelecimento do túnel *hub-and-spoke*, e utiliza o NHRP para traduzir para um endereço físico e alimentar o GRE com um novo túnel. Esse passo por consequência sobrescreve a tabela de roteamento (com o endereço destino da interface GRE remota, que estará associado a um endereço físico), fazendo com que a interface GRE encapsule o pacote com o endereço destino do gateway correto e passando ao IPSec para processamento em modo transporte.

O tráfego pode seguir pelos túneis *hub-and-spoke* até que o novo túnel *spoke-spoke* seja criado, e a partir daí utilizar o novo túnel para comunicação direta. Após um tempo de vida pré-configurado o túnel direto é destruído poupando recursos da VPN. A Figura 6.14 mostra o funcionamento do NHRP no mapeamento de um gateway dinamicamente.

Os passos detalhados na Figura 6.14 são descritos a seguir:

1. Um PC (192.168.1.25) na rede do *spoke* A quer estabelecer uma conexão com o servidor web na rede do *spoke* B (192.168.2.37). O pacote é enviado ao gateway VPN do *spoke* A, que tem em sua tabela de roteamento o endereço da camada VPN (10.0.0.12) via interface GRE para alcançar o servidor web.

2. O gateway VPN consulta seu cache NHRP e verifica que não existe endereço da camada física associado ao host 10.0.0.12. O gateway envia um pacote de pergunta ao servidor NHRP (NHS).

3. O *hub* que atua como NHS responde ao *spoke* A informando o endereço físico desejado. Esses endereços foram armazenados em cache quando os *spokes* estabeleceram

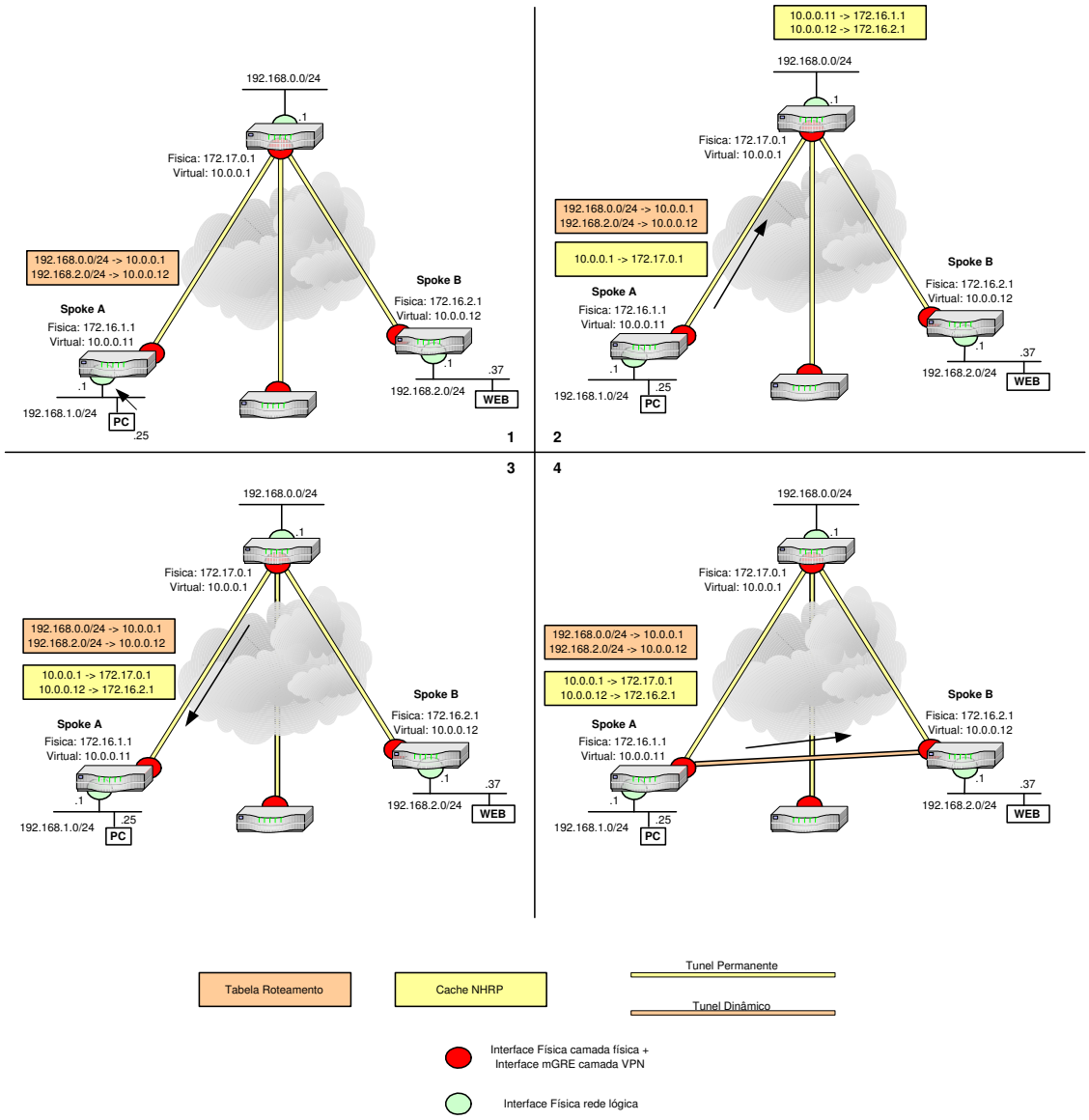

Figura 6.14: *Next* Host *Resolution Protocol - NHRP*

o túnel permanente com o *hub*.

4. Com base na informação recebida o gateway do *spoke* A dispara o IKE para estabelecer uma SA diretamente entre os *spokes* A e B. É importante lembrar que uma SA é unidirecional, fazendo com que todo o processo de mapeamento de B para A seja realizado no ato do envio do primeiro pacote de resposta do web server. Após um período a entrada NHRP é retirada das tabelas dos *spokes* e destruindo o túnel IPSec.

Como o protocolo NHRP mapeia o endereço da interface GRE na interface física, é possível que os gateways das filiais tenham endereços alocados dinamicamente pelo provedor (DHCP), pois logo que estabelecem o túnel permanente com a matriz se registram no NHS. Isso permite a adição de novos *sites* de forma muito fácil e prática, tendo em vista que o roteamento dinâmico e o NHRP propagam todas as informações necessárias.

A abordagem proposta de utilizar o GRE em uma interface *multi-point* possibilita maior facilidade e flexibilidade no gerenciamento e expansão da VPN, pois caso contrário seria necessário uma interface por túnel GRE (ponto a ponto). Numa VPN de 500 *sites* por exemplo o *hub* teria no mínimo 500 interfaces virtuais.

Apesar do IPSec, GRE e NHRP serem protocolos definidos pelo IETF, a sua combinação para uma solução a ser utilizada em VPNs para grandes corporações ainda não tem uma definição concreta. Na verdade, o IPSec *Working Group* tem trabalhado muito pouco a respeito de mapeamento dinâmico dos gateways VPN.

É importante analisar no cenário proposto que somente existe relação de vizinhança entre o *hub* e os *spokes*, evitando que os protocolos de roteamento propaguem informações sobre túneis dinâmicos que podem gerar o consumo excessivo de recursos da VPN devido a natureza temporária dos túneis *spoke-spoke*. Outro ponto a ser analisado é que o *hub* se torna um ponto único de falha, e no caso da perda de conexão entre filial e matriz o *site* da filial fica totalmente isolado. Por outro lado, a centralização de recursos no *hub* pode proporcionar economia nos *sites* das filiais e maior robustez na arquitetura disponibilizada na matriz.

Túneis Dinâmicos utilizando DNS e *Opportunistic Encryption*

No momento de escrita deste trabalho, o IETF apresenta dois drafts em discussão para mapeamento dinâmico dos gateways VPN. Ambos utilizam o mesmo conceito: a combinação dos protocolos IPSec, DNS [Moc87a, Moc87b] e DNSSEC [Eas99] para descoberta do gateway VPN responsável por um determinado *Host* (se houver algum) e a chave pública necessária para estabelecer a comunicação.

A solução proposta visa o estabelecimento dinâmico de SAs conforme a necessidade, utilizando puramente o IPSec para estabelecimento dos túneis. O DNS fornece a in-

formação necessária a um gateway que não tem conhecimento sobre como se comunicar de forma segura com um *Host* remoto. Como o DNS não é um protocolo seguro, a utilização do DNSSEC é importante para garantir a segurança da solução, que confia no DNS para obter os parâmetros necessários para estabelecer um canal seguro.

As soluções descritas em [Ric04, Red04] visam um escopo maior que o desejado para este trabalho, que é a utilização do IPSec para comunicação segura entre dois *Hosts* qualquer (via gateway ou não) na Internet. O FreeS/Wan, implementação open-source para o Linux, apresenta a partir de sua versão 1.91 suporte a esse tipo de abordagem, chamada *Opportunistic Encryption*.

Os detalhes destas soluções, que não visam o IPSec como links ponto-a-ponto (ausência de interfaces GRE ou IPIP e consequente ausência de roteamento dinâmico), serão descritos a seguir, sendo complementadas por uma análise de como seriam adaptadas para utilização no cenário corporativo proposto, além de sugestões de modificações para facilitar a integração do ambiente corporativo.

Supondo um *Host* qualquer em uma rede A protegida por um gateway IPSec (GW-A) queira se comunicar com um *Host* B remoto. Os seguintes passos serão seguidos:

1. Ao enviar o pacote, o GW-A irá verificar que o mesmo não tem nenhuma SA estabelecida (ou mesmo definida) para a comunicação entre A e B.

2. O GW-A executa uma consulta no DNS reverso (in-addr.arpa.) para descobrir qual o gateway responsável pelo *Host* B, e descobre o endereço do GW-B e sua chave pública. Como a consulta foi feita de modo seguro ao DNS (utilizando por exemplo o DNSSEC), a autenticação do GW-B vem da confiança estabelecida entre GW-A e DNS, pois o GW-A deve confiar na chave pública e no endereço IP do GW-B ao realizar uma consulta pelo endereço do *Host* B

3. Com base nas informações obtidas, o GW-A inicia um processo de negociação IKE com o GW-B para realizar a comunicação segura entre os *Hosts* A e B.

A diferença entre os drafts propostos está no registro utilizado para armazenar informações criptográficas para estabelecimento dinâmico de túneis IPSec. Enquanto o [Ric04] utiliza o RR IPSECKEY, a solução descrita com base no *Opportunistic Encryption - OE* do FreeS/WAN utiliza um registro TXT.

Do ponto de vista de uma VPN corporativa, é importante ressaltar alguns itens importantes:

- A configuração do controle de acesso fica complicada, devido a não ser possível restringir conexões de gateways baseando-se apenas na chave pública. A utilização de certificados digitais pode ser uma fonte rica em informações para o controle de acesso [Ste03].

- Por consequência, todo pacote que chegue via *Opportunistic Encryption* deve ser tratado como um pacote não confiável, dada a natureza do estabelecimento dos túneis [Red04], sendo submetido a regras de filtragem e outras verificações.

- Existem dois meios de se utilizar OE. O primeiro envia os pacotes em claro até que o túnel seja estabelecido (garantindo a conectividade mesmo de forma insegura) enquanto o segundo descarta todos os pacotes até que seja possível o estabelecimento do canal seguro. A primeira opção é totalmente desaconselhável para um ambiente corporativo, devido ao risco de um ataque a VPN comprometer a comunicação como um todo. O segundo meio implica em certos *delays* devido a magnitude de tempo para se estabelecer uma SA.

- existem problemas de cache de informações providas pelo DNS, que em uma eventual troca de chaves por motivo de segurança pode paralisar a comunicação até que uma nova consulta ao DNS seja feita.

- uma configuração em larga escala deve ser cuidadosamente implementada, para que vários túneis para o mesmo destino não sejam criados, gerando impacto na performance e dimensionamento da VPN.

- Algumas formas de ataques DoS são possíveis devido ao gateway estar aberto a qualquer tipo de conexão, baseado apenas na autenticação do DNS [Red04] (por isso a recomendação da filtragem dos pacotes como não confiáveis).

- Todos os *Hosts* devem ser registrados no DNS reverso para que o gateway responsável pela sua proteção na VPN seja encontrado

De qualquer maneira, o DNS como fonte centralizadora de várias informações sobre os *Hosts* na Internet é uma realidade, e o advento do DNSSEC o torna uma ótima fonte para obtenção de informações a respeito de *Hosts* e redes.

No caso de uma VPN corporativa, pode-se pensar em um servidor DNS análogo ao servidor NHRP, acessível via túnel permanente pré-configurado (*hub-and-spoke* entre filiais e matriz) e pelos gateways pertencentes à organização. Dessa forma, o DNS interno só responderá aos gateways presentes na VPN evitando que conexões indesejáveis sejam estabelecidas via OE. Dessa maneira torna-se bem mais simples o registro automático dos *Hosts* no DNS reverso (na verdade o roteamento passa a estar implícito no DNS).

Uma maneira mais simples de utilizar o DNS seria a obtenção do gateway e o endereço da CA para obtenção do certificado (ao invés de uma chave pública), proporcionando meios mais ricos de estabelecer controle de acesso. Claro que em um ambiente como a Internet, visando-se a conexão segura entre dois pontos quaisquer, surgem questões de certificação cruzada, coisa que pode ser facilmente controlada dentro de uma VPN

"fechada" de uma organização, que pode inclusive implementar sua própria CA (e uma infra-estrutura de chaves públicas).

Outra maneira de confiar ao DNS a tarefa de mapeamento dos gateways, seria a consulta do endereço físico através do endereço virtual da interface GRE ou IPIP, funcionando de modo análogo a solução utilizando NHRP e possibilitando o roteamento dinâmico e a utilização do IPSec como link ponto-a-ponto.

6.6 Conclusão

Os tópicos discutidos aqui ainda estão em definição pelo IETF (alguns como o mapeamento dinâmico dos gateways ainda são tratados de forma bem incipiente). A falta de conhecimento do potencial do IPSec em uma VPN corporativa leva a grande maioria das empresas que partem para uma solução baseada neste protocolo a utilizarem uma topologia estrela com comunicação filial-matriz somente.

As idéias apresentadas visam manter o IPSec competitivo entre soluções como MPLS. Soluções baseadas em rede geralmente são adotadas visando facilidade de implementação e gerenciamento, colocando-se QoS (o maior ganho deste tipo de tecnologia) em segundo plano. Além disso, é possível colocar a maioria dos *sites* utilizando IPSec no mesmo ISP, gerando um ganho muito grande em performance, dado que os pacotes raramente deixam o backbone do ISP nestas condições. É interessante lembrar ainda que existem serviços de conectividade IP com SLAs bem definidos.

Além de pouco abordada, a solução IPSec para redes de alta capilaridade provoca discussões interessantes como as apresentadas neste capítulo, raramente consideradas pelo *network designer* ao conceber as possíveis soluções para uma VPN. Além disso, são disponibilizadas na maioria das vezes em "caixas pretas" pelos fabricantes de soluções.

Apesar do IETF discutir a utilização do IPIP para roteamento dinâmico sobre IPSec e o uso do DNS para mapeamento de gateways, não existe uma tendência forte a ser seguida e os fabricantes adotam muitas vezes soluções proprietárias. O próprio IETF não apresentou até o momento um documento sobre integração de roteamento dinâmico e mapeamento dos gateways, conforme analisado neste capítulo.

Entretanto, a disponibilização de roteamento dinâmico sobre IPSec já garante um enorme potencial do protocolo em uma rede de alta capilaridade, mesmo que seja utilizado em uma topologia *hub-and-spoke*.

Além de tudo que foi discutido neste capítulo, o Capítulo 7 acrescenta mais algumas considerações importantes que não puderam ser abordadas de forma profunda neste trabalho.

Capítulo 7

Considerações Adicionais

7.1 Introdução

Além das soluções para os problemas de gerenciamento, conectividade e segurança apresentados no capítulo anterior, e foco do estudo proposto neste trabalho, existem uma série de detalhes relevantes ao sucesso de uma VPN que não puderam ser incluídos no escopo deste trabalho. Estes detalhes são muitas vezes deixados de lado pela empresa ou provedor de serviços, e acabam impactando de alguma forma no correto funcionamento da VPN.

Claro que em um *backbone* compartilhado de um SP a empresa pode não ter que se preocupar com muitos dos detalhes apresentados neste capítulo. Entretanto, quando a capilaridade é fator presente juntamente com a Internet, cada *site* apresenta uma série de complicações compondo um cenário na maioria das vezes heterogêneo, o que torna o desafio de sucesso da VPN ainda maior.

Os tópicos apresentados neste capítulo representam um complemento às considerações relevantes à implantação de uma solução VPN IPSec baseada em CPE. Apesar de não apresentar a mesma profundidade técnica do Capítulo 6, este capítulo realiza uma "costura" sobre os pontos importantes que com certeza farão parte do ambiente corporativo. Muitos dos tópicos abordados a seguir podem servir de base para um novo trabalho, visando sempre o complexo ambiente de redes corporativas de alta capilaridade.

7.2 Considerações sobre os gateways VPN

7.2.1 Colocação e Interação com Firewalls

Firewalls servem para prevenir que tráfego não autorizado entre ou saia da rede privada e geralmente não estão preocupados com a segurança do tráfego depois que o mesmo sai da

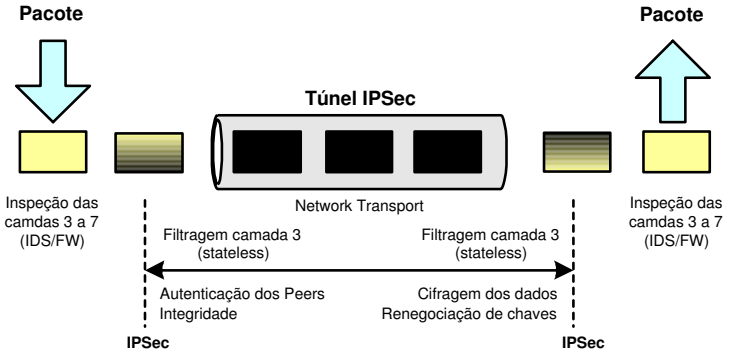

Figura 7.1: *Layered Security Model*

rede. Já o gateway VPN trabalha de forma a permitir que apenas tráfego legítimo transite dentro da rede interna e também assegurar que o mesmo continue sendo considerado seguro após sua saída da rede [Str01].

O gateway VPN e o Firewall são dispositivos de segurança normalmente usados em conjunto e algumas vezes até integrados no mesmo dispositivo [Str01]. Existem algumas regras de segurança que devem ser consideradas quando da definição do posicionamento do gateway VPN em relação ao Firewall:

- Deve-se tomar cuidado para não comprometer a política de segurança da rede
- O gateway VPN não deve estar localizado de modo a ser um único ponto de falha
- O gateway VPN deve aceitar somente tráfego cifrado da rede externa
- O gateway VPN deve aceitar tráfego cifrado ou não da rede interna
- Ele deve se defender de ataques vindos da Internet
- Deve obedecer o modelo de segurança em camadas (e consequentemente o princípio de "*Defense in Death*" [Str03]), permitindo que outros dispositivos realizem filtragem e/ou análise dos dados de outras camadas, caso o dispositivo não implemente tais funcionalidades, conforme mostra a Figura 7.1. Esse ponto é muito importante quando falamos em prover roteamento dinâmico sobre o IPSec, onde o Firewall assume um papel importante no controle de acesso, conforme descrito no Capítulo 6.

Os Firewalls não podem aplicar regras de filtragem a pacotes cifrados, por isso é importante a análise da colocação do gateway VPN em relação ao firewall. Se essa colocação for feita em uma rede já existente, possivelmente será necessário analisar todas as alterações

de tráfego que ela pode causar a fim de garantir que as premissas de segurança da rede sejam mantidas. Existem várias maneiras de se fazer a colocação do gateway.

Conforme apresentado em [dG02b], a análise da colocação do gateway VPN principal na matriz em relação ao acesso remoto, serviu de base para a análise da colocação deste dispositivo em relação à arquitetura *site-to-site*, que merece considerações diferentes. Os autores em geral consideram o fluxo de dados para o acesso remoto RW–>LAN Matriz e LAN Matriz –> RW. Já em uma WAN corporativa baseada em IP VPNs, a comunicação entre filiais e a utilização de algum tipo de *mesh* coloca o Firewall em difícil situação, sendo necessário muitas vezes a duplicação e/ou pulverização da política de segurança, deixando como objetivo para o Firewall em relação ao gateway a proteção de ataques diretos e não constituição de ponto único de falha.

Em frente ao Firewall

Essa colocação do gateway VPN como ponto de conexão à Internet, faz dele um único ponto de falha que pode ser explorado por um atacante, comprometendo dessa forma todo o funcionamento da rede. Um exemplo são ataques tipo DoS, que os GWs baseados em IPSec têm extrema dificuldade de evitar. Com uma implementação deste tipo, permite-se a passagem de tráfego cifrado e não cifrado a partir da rede insegura, fazendo com que o gateway receba tráfego que não seja realmente destinado a ele, no qual não se incide nenhum tipo de análise. Vale lembrar que nem todos os dispositivos têm a capacidade de diferenciar o tráfego não cifrado do tráfego cifrado, podendo ocasionar descarte de pacotes indevidamente. O gateway exigiria neste caso saber quais os dispositivos estão habilitados a receber tráfego não cifrado, podendo gerar uma complexa e árdua configuração, além da capacidade de filtragem e roteamento separadas das funções de GW VPN.

Atrás do Firewall

Nesta situação, algumas regras devem ser configuradas no Firewall para que ele permita a passagem direta do tráfego destinado ao gateway VPN, mesmo porque ele não consegue aplicar regras de filtragem no tráfego cifrado endereçado ao mesmo. O Firewall deve deixar passar pacotes IP do tipo 50 (AH) e 51 (ESP) e pacotes UDP na porta 500 (IKE). Essa "abertura" feita no Firewall para permitir a passagem do tráfego destinado à VPN, apesar de necessária, é perigosa, pois enfraquece a proteção fornecida pelo mesmo [Str01]. Além disso, esta configuração também implica em um único ponto de falha, o que é totalmente desaconselhável.

No Firewall

É uma solução viável, dita como a melhor por alguns fabricantes, embora exija mais complexidade por parte do equipamento, que precisa ter habilidade em rotear, executar criptografia de chave pública e chavear entre sessões cifradas ao mesmo tempo em que se realiza controle de acesso e geração de logs. Isto pode gerar sobrecarga no equipamento, mas o pior é que neste tipo de solução, este equipamento se constitui em um único ponto de falha ainda mais grave porque um ataque à VPN pode comprometer toda a estrutura do Firewall. Em termos de escalabilidade, uma solução modularizada com o gateway VPN separado fisicamente do Firewall leva vantagem principalmente no custo, pois um *upgrade* em um dispositivo integrado tende a ser mais caro. Além disso, a complexidade de configuração pode aumentar, pelo princípio de se ter "muitos ovos em um mesmo cesto" [Sys03b].

Paralelo ao Firewall

Nesta situação, existem duas conexões com a rede não confiável: uma para o Firewall e outra para o gateway VPN. O tráfego VPN passa pelo gateway e todo o resto passa pelo Firewall. Esta configuração não se caracteriza por um único ponto de falha, porém o gateway VPN deve se defender sozinho de ataques, e o tráfego não cifrado não é submetido a nenhum tipo de controle antes de entrar na rede interna, desobedecendo o modelo de segurança em camadas. Apesar de facilitar a migração e manutenção do GW VPN, facilitando inclusive o "empilhamento" de GWs, gera problemas de segurança já mencionados e dificulta a configuração do roteador localizado na borda da LAN.

Não é difícil de se configurar o *WAN-side router*. Como todo o tráfego VPN é tunelado e todos os túneis têm um "*endpoint*" no gateway VPN, o roteador precisa apenas de uma lista de roteamento para o gateway VPN. Já a configuração do *LAN-side router* é mais complicada porque o tráfego também tem que estar tunelado e fica difícil saber em um simples roteador o que deve entrar na VPN e o que deve ser encaminhado ao Firewall.

Algumas implementações conectam o Firewall e o GW VPN diretamente à LAN, causando um problema ainda maior, pois os clientes internos (*Hosts*) não sabem quem é o *default* gateway. A conexão entre Firewall e GW VPN neste caso se torna necessária, e um dos dispositivos deve receber todo o tráfego e encaminhar ao outro o que não lhe diz respeito (em geral o Firewall faz este papel). Vale lembrar ainda que a utilização do IPSec proposta neste trabalho necessita de dispositivos de filtragem externos ao protocolo, devido aos túneis serem tratados com *links*.

Ao lado do Firewall

Neste caso, o Firewall recebe todo o tráfego da rede, protegendo o gateway VPN de ataques diretos vindos da rede externa. Quando identifica que se trata de tráfego cifrado, ele envia para o gateway VPN que o decifra e devolve para o Firewall que o analisa e envia para a rede segura.

Esta solução é dada por muitos como a mais segura e confiável, porém ela implica em um aumento do tráfego já que o gateway VPN precisa de duas conexões com o Firewall para processar a mesma informação: uma para receber e outra para enviar.

Antes de decidir por este tipo de colocação do gateway, é bom medir o aumento de complexidade das regras de filtragem que isso pode causar, porque muitas vezes os cenários de acesso de clientes VPN são bastante complexos, por exemplo: parceiros da *extranet*, funcionários com acesso remoto e filiais da empresa. A administração dos equipamentos fica mais complicada e pode gerar brechas para um possível ataque [dG02b].

Vale lembrar que em uma topologia *hub-and-spoke*, onde as filiais (*spokes*) se comunicam através do *hub*, fica inviável o Firewall analisar os pacotes que estão trafegando entre uma filial e outra, sendo necessário a duplicação da política de segurança no GW VPN ou descentralizar o controle de acesso para os Firewalls das filiais, o que é altamente recomendável utilizando configuração remota, segura e centralizada.

Ao se optar por esta solução, é necessário também decidir qual a posição exata do gateway VPN em relação a DMZ, que pode ser:

- Em conjunto com outros equipamentos de uma DMZ

  Neste caso, o gateway VPN fica posicionado junto aos outros equipamentos da DMZ que podem ser acessados por usuários participantes ou não da rede interna. Portanto, a complexidade de configuração deste tipo de instalação vai depender do tipo de usuário que tem acesso a VPN.

  Para os casos de VPN ligando parceiros de uma *extranet*, estes podem acessar todos os serviços que um usuário externo pode, porém de maneira cifrada. O problema nesse caso, é que os pacotes vindos da rede desses parceiros não são submetidos às regras de filtragem pois estão cifrados antes da passagem pelo gateway VPN [dG02b] e depois são transitados diretamente entre gateway e recurso desejado.

- Numa DMZ separada

  Quando o gateway VPN está em uma DMZ separada, não irão ocorrer os problemas listados no caso acima porque ela proporciona um isolamento do tráfego decifrado em relação ao tráfego vindo direto da Internet [dG02b]. A complexidade de configuração das regras do filtro escrutinador são maiores, pois utiliza mais uma interface para administração e aplicação das regras.

A DMZ do gateway VPN pode ser usada para inclusão de outros serviços que os usuários de *extranet* ou de redes externas tenham necessidade [E. 00], evitando dessa forma que a rede interna seja acessada para responder solicitações de HTTP, FTP e outras de usuários que não sejam totalmente confiáveis. No caso de usuários de filiais da própria empresa, podem ser colocados também os serviços necessários a eles [dG02b] nessa DMZ. O problema é a duplicação de recursos e uma solução seria a instalação de *proxies* para os mesmos [dG02b].

Uma outra solução possível é deixar somente o gateway VPN na DMZ, sendo o tráfego encaminhado para outra DMZ ou para a rede interna. As vantagens dessa colocação são: diminuição da granularidade da filtragem e adoção de uma solução mais geral para tráfego VPN, de modo que um único gateway seja a terminação de vários tipos de túneis, vindos de uma *extranet*, uma filial ou uma máquina de acesso remoto.

- Numa configuração de múltiplas DMZs

  Neste caso, existe um filtro externo e um interno exclusivamente para a VPN. As vantagens desse tipo de colocação são a simplificação de endereçamento, a divisão entre o tráfego Internet comum e o tráfego para redes confiáveis via VPN e a possibilidade de uma filtragem exclusiva no roteador interno, das solicitações de conexões vindas da faixa de endereços internos atribuídos às máquinas da *extranet*, parceiros de redes corporativas, de filiais ou de acesso remoto.

  Este tipo de colocação implica em duplicação de recursos físicos, o que pode ser resolvido colocando-se o filtro externo e o VPN em um único equipamento. Porém esta configuração exige cuidados por apresentar um único ponto de falha.

  No caso de uma *extranet* ou parceiros corporativos, pode-se colocar os recursos necessários a eles nesta DMZ, embora se perca dessa forma a vantagem de poder filtrar o tráfego recém decifrado, antes de sua chegada aos outros equipamentos da rede.

Considerações sobre os gateways das filiais

Conforme descrito em relação à comunicação entre filiais *spoke-spoke*, seja ela numa topologia estrela ou *mesh*, o Firewall da matriz pouco tem a fazer em relação ao tráfego que transita entre as filiais direta ou indiretamente.

Adotando a abordagem mais recomendada onde o GW é colocado em uma interface dedicada do Firewall, e dado o elevado número de túneis, fica inviável o GW enviar o pacote destinado a uma filial e recebê-lo de volta, por problemas de roteamento e complexidade de configurações de Firewall (lembrando que nem sempre estamos falando

de uma única rede, mas possíveis e várias sub-redes em cada *site*), que necessitarão de regras adicionais para gerenciar pacotes em claro que estão chegando do gateway e da matriz com destino às filiais, lembrando sempre que o túnel termina no gateway VPN e não no Firewall.

O que acontece na maioria das vezes é o gateway "chavear" os pacotes entre os túneis invalidando completamente a função do Firewall, principalmente se o objetivo é criar um roteamento dinâmico na camada VPN. O Firewall não faz parte desta camada, e a interação *Firewall-Gateway*-Roteamento em uma mesma camada seria altamente complexo e portanto não recomendável, pondo em risco o correto funcionamento e segurança da rede corporativa.

Dessa forma, o gateway pode implementar políticas de segurança ou deixar que os Firewalls das próprias filiais se "defendam". Aliás, a integração do Firewall com o gateway IPSec pode ser uma opção interessante do ponto de vista de custo, dado o dimensionamento do mesmo ser esperado um dispositivo não tão robusto como o da matriz. Um computador com *Linux* utilizando *Free/SWan* é um exemplo, onde o próprio sistema operacional apresenta funções de Firewall com o *IPTables*.

7.2.2 Dimensionamento

O alto número de túneis levará a análise de dimensionamento do gateway a um lugar de destaque no desenho da solução VPN. A questão basicamente se dividirá em dois pontos: características do gateway e número de gateways utilizados.

O primeiro ponto envolve decisões entre utilização de implementações IPSec baseadas em software (como o FreeS/Wan) ou em hardware (como o Contivity da Nortel). Além disso, características proprietárias como cartões aceleradores para criptografia, equipamentos com mais de uma fonte e tolerância a falhas através de múltiplas interfaces ou gateways (*clustering*) farão parte da composição do equipamento.

Conforme mostra a própria página do projeto FreeS/Wan[1], problemas de performance podem aparecer acima de 50 túneis. De modo geral, essa característica irá afetar a utilização de máquinas de propósito geral para funções de autenticação e criptografia.

É possível identificar dois gargalos na utilização do IPSec: a autenticação (mais especificamente a geração de segredos pelo algoritmo Diffie-Hellman) e a cifragem dos pacotes. Como os links Internet hoje raramente passam de 2 megabits/segundo, a cifragem não será o maior problema devido ao alto *throughput* conseguido mesmo pelas máquinas de propósito geral. O grande "vilão" será a utilização do Diffie-Hellman, podendo uma rede onde as filiais iniciam a conexão com o(s) gateway(s) da matriz em um mesmo horário gerar uma paralisação da VPN. O mesmo se aplica à utilização de PFS, recomendado

[1] disponível em www.freeswan.org

pela Cisco [Sys03b] somente em casos onde seja extremamente necessário.

Entretanto, a análise de performance envolve uma série de fatores que merecem uma análise caso a caso, além das considerações feitas aqui. Cada rede tem uma característica própria e fica difícil estabelecer uma "receita de bolo" para dimensionamento do gateway VPN. Uma consideração importante é o fortalecimento de um equipamento (em termos de dimensionamento) em detrimento à utilização de vários equipamentos para a função de gateway. Apesar de simplificar extremamente a configuração e implantação de uma solução VPN, a utilização de um único equipamento constitui em um ponto único de falha. Dado o alto preço de tais equipamentos, é raro encontrar uma organização que permita seu investimento parado em uma prateleira para efeitos de *backup* (a reposição de tais equipamentos é muitas vezes ligada à utilização de protocolos e mecanismos proprietários para implementação de suas funcionalidades e requerem outro equipamento compatível). Vários gateways parecem uma solução mais robusta e viável no mercado corporativo, principalmente em conjunto com a proposta de roteamento dinâmico apresentada neste trabalho.

7.3 Escolha dos algoritmos criptográficos

Apesar da flexibilidade do IPSec em se prover uma gama enorme de algoritmos criptográficos e de autenticação, na maioria das vezes essa flexibilidade deve ser dispensada em detrimento da segurança e performance. A idéia de se utilizar a camada VPN como sendo um *backbone* provendo um *link* remoto entre *sites* da corporação, impulsiona ainda mais a utilização de algoritmos criptográficos/autenticação que atendam a equação "performance x segurança".

Conforme críticas encontradas em [Sch99], o IPSec pode se tornar inseguro devido a sua complexidade, e a utilização do protocolo com uma granularidade de algoritmos muito alta pode comprometer a segurança do sistema, fazendo com que por um erro de configuração por exemplo, um algoritmo fraco seja escolhido para proteção de informações sensíveis.

Algoritmos como o DES, reconhecidamente fraco para os dias atuais, podem ser uma má escolha quando há disponível o 3DES muito mais seguro. A utilização de um algoritmo padrão como o AES é recomendada neste trabalho, a fim de facilitar o gerenciamento e aumentar a segurança. Conforme já mencionado, a VPN não vem para resolver problemas já existentes nas redes atuais [Tec00], e é utilizada neste trabalho com a proposta de prover comunicação segura entre dois pontos. Além do AES levar vantagem em relação ao DES (considerado inseguro) e ao 3DES (baixo desempenho), na cripto-análise encontrada em [Sch99], o método de escolha do AES como sucessor do 3DES é muito elogiado, em contraste ao método de desenvolvimento do IPSec [Sch99]. Maiores detalhes da utilização

de algoritmos específicos por tipos de tráfego pode ser encontrados em [Jan02].

7.4 Faixas de endereços sobrepostas e hierarquia de endereçamento

Apesar de não ser problema exclusivo de uma VPN, mas de qualquer WAN, a sobreposição de sub-redes pode acontecer principalmente quando se conectam um grande número de sites, como é o caso do cenário proposto. Neste caso, os serviços e a comunicação em geral não funcionarão corretamente, pois o roteamento será afetado não sabendo se deve encaminhar um determinado pacote para uma rede remota ou entregá-lo na rede interna à qual pertence.

Por isso é importante planejar cuidadosamente a faixa de endereçamento de cada site antes de conectá-los via VPN. A utilização de sub-redes deve ser cuidadosamente estudada, evitando sobreposição e uma futura falta de endereços. Este ponto merece uma atenção especial, pois a alocação de faixas de endereços de forma agrupada pode diminuir o número de túneis e entradas na tabela de roteamento, bem como facilitar a configuração das regras de filtragem.

Pode-se ter em um mesmo site várias sub-redes internas, mas um número muito menor poderá ser divulgada para os demais sites devido à possibilidade de agrupamento das mesmas em uma máscara de sub-rede mais genérica. Como exemplo, um site que possua as sub-redes 10.10.10.0/25 e 10.10.10.128/25 pode divulgar que conhece a sub-rede 10.10.10.0/24. Já um site que possua as sub-redes 10.10.10.0/24 e 198.10.132.0/24 deverá obrigatoriamente divulgar as duas rotas, e caso o IPSec esteja sendo utilizado como um túnel por sub-rede teremos um túnel a mais que no primeiro caso. Além disso, um mapa bem elaborado dos endereços da rede corporativa pode se tornar uma poderosa ferramenta de administração, facilitando a identificação de recursos e Hosts, bem como a configuração dos Firewalls envolvidos na filtragem.

7.5 Split Tunneling

Um assunto controverso na configuração das filiais é se as mesmas irão acessar a Internet diretamente para tráfego não corporativo (por exemplo um site de busca como o Google) ou se o tráfego destinado à Internet deverá obrigatoriamente passar pela matriz.

De certa forma, permitir o acesso direto da filial à Internet implica em um ganho de performance e economia de recursos. Esta abordagem é chamada de *split tunneling*. Porém, deve-se levar em conta que a segurança em cada filial deve ser cuidadosamente

estudada e reforçada (com Firewalls e outros mecanismos), de modo a garantir que um eventual ataque vindo da Internet não comprometa a segurança da rede corporativa.

Tunelar todo o tráfego para a matriz pode gerar problemas de performance e dimensionamento, apesar de ter-se um único ponto de inspeção dos pacotes destinados à Internet. Em contrapartida, dada a abordagem de se utilizar o IPSec como *links* seguros entre os sites, deixando o controle de acesso para os Firewalls e outros dispositivos, é necessário de qualquer maneira "pulverizar" a política de segurança em vários pontos, sendo necessária de qualquer maneira a presença do Firewall em cada filial.

A necessidade de acesso direto à Internet deve ser estudada caso a caso, e caso as filiais tenham necessidade deste tipo de tráfego além do tráfego corporativo, não deve ser possível a um atacante utilizar este ponto de saída como entrada para rede interna da filial e consequentemente da organização como um todo. Vale lembrar que em alguns sites que necessitam de mensagens DHCP/PPPoE (utilizando por exemplo ADSL com IP Dinâmico) para o servidor do ISP não poderão contactá-lo se todas as rotas apontam para a matriz.

7.6 O acesso remoto

A necessidade de conectar funcionários fora do seu ambiente de trabalho de forma segura pode surgir como necessidade em uma solução VPN. No entanto, esse tipo de acesso envolve uma série de considerações diferentes do cenário analisado neste trabalho, e pode-se encontrar uma análise deste ambiente em [Edm04]. O ponto chave no entanto é a integração desses dois ambientes: se o usuário remoto irá se conectar sempre à matriz ou diretamente à filial desejada, se existirá um ou mais gateways a parte dos envolvidos na formação da WAN, específicos para o acesso remoto, e uma enorme gama de detalhes que fogem ao escopo deste trabalho, mas merecem ser citados para que não seja criada a idéia de que o acesso remoto é uma simples consequência da VPN em uma WAN corporativa. Este cenário como foi dito merece considerações bem específicas, e sua integração com a VPN merece atenção especial.

7.7 Integração com parceiros

Muitas vezes os parceiros comerciais poderão se conectar à rede corporativa através de uma VPN. Como já citado para o caso do acesso remoto, as soluções apresentadas para a WAN corporativa não deem ser diretamente aplicadas à parceiros, por dois motivos:

- qualquer rede fora do domínio da organização deve ser considerada uma rede Hostil

- é impossível garantir a segurança de uma rede Hostil, sendo um possível ponto de ataque caso se estabeleça a segurança através de uma simples relação de confiança entre parceiros comerciais.

Deste modo, é recomendável que os parceiros comerciais sejam interligados à VPN de forma a permitir acesso somente aos recursos desejados (e os mesmos devem estar bem definidos), se possível em uma DMZ separada garantindo a segurança da rede da organização. Informações de roteamento e conectividade *any-to-any* devem ser evitadas, e as regras de filtragem e do IPSec devem ser bem especificadas para cada parceiro adicionado à VPN. Por maior que seja o nível de confiança entre parceiros comerciais, a comunicação através de uma VPN deve seguir à risca a política de segurança da organização, considerando qualquer acesso de outras empresas um acesso "externo".

7.8 Conclusão

Este capítulo teve como objetivo apresentar alguns detalhes importantes que devem ser considerados em uma solução VPN baseada em IPSec. Em geral, as considerações apresentadas para cada tópico visam completar os problemas apresentados no capítulo anterior com um maior nível de abstração. Isso se deve a dois fatores: a particularidade de cada rede e a impossibilidade de abordar o assunto de forma profunda dado o escopo deste trabalho. Desta forma, alguns dos tópicos como o acesso remoto e integração com parceiros pode servir de base para um novo estudo, mais profundo e com um cenário mais específico que o tratado neste trabalho.

O acesso remoto ainda pode de certa forma ser analisado de modo análogo a um ambiente de alta capilaridade pelo número de túneis, dependendo do número de acessos. Em contrapartida merece considerações bem específicas, devidamente abordadas em [Edm04]. A integração deste tipo de acesso com o cenário proposto exige um nível de pesquisa mais profundo, assim como a integração com parceiros comerciais, que em conjunto com o acesso remoto e a WAN corporativa irá compor a solução VPN como um todo. Cada parceiro irá requerer um grau de segurança e considerações diferentes, dependendo do tipo de serviço disponibilizado ou utilizado.

De qualquer forma, o advento de uma VPN baseada em IPSec abre portas para utilização de ambos os cenários (acesso remoto e de parceiros). Este capítulo, além de abordar detalhes importantes para a WAN corporativa, apresenta alguns desses pontos que podem motivar ainda mais a utilização de uma solução VPN utilizando o protocolo IPSec.

Capítulo 8

Conclusão

8.1 Considerações Finais

O objetivo deste trabalho foi analisar soluções VPN para um ambiente onde a capilaridade da rede é fator impactante no desenho da solução. O IPSec é considerado um padrão para estabelecimento de VPNs através de redes não seguras, além de ser considerado o protocolo mais seguro atualmente [Sch99]. Soluções de mercado como o MPLS entretanto, vem ganhando terreno junto às grandes empresas.

Isso se deve em grande parte ao fato do IPSec não ser conhecido a fundo na maioria das organizações. Características como segurança são deixadas de lado em função da urgência dos negócios corporativos, que exigem conectividade entre os diversos *sites* remotos e a um baixo custo. Apesar de não ser um protocolo novo, o campo de aplicações do IPSec ainda é vasto para pesquisa de soluções de VPNs complexas, e até mesmo no acesso remoto, conforme abordado em [Edm04]. Uma das provas disso é a discussão de novas versões do protocolo IKE e ESP propostas em drafts visando resolver parte dos problemas apresentados na primeira versão do protocolo [Atk98c].

Além disso, a idéia geral do IPSec apresentada nos livros de VPN em termos de conceito parece muito simples. Mas numa real implementação, e principalmente em um cenário complexo, existem vários ítens que nunca são abordados, principalmente em forma de uma análise lógica e agrupando essas valiosas informações e considerações em um único trabalho. AS VPNs IPSec baseadas em CPE não são de forma alguma *plug-and-play*, e a descoberta desse fato no meio de uma implementação pode custar muito caro a qualquer empresa.

Apesar disso existem meios de se conduzir a solução de forma consistente, levando em consideração aspectos de segurança e escalabilidade apresentados neste trabalho, poupando grande esforço das empresas que possuem cenário semelhante. Os conceitos apresentados e analisados aqui podem ser decisivos na análise de uma solução IPSec baseada

em CPE proposta por qualquer fabricante, além de manter o IPSec competitivo entre as soluções existentes atualmente, afinal, o fato de um protocolo definido atualmente ter pontos a serem estudados e melhorados não implica na definição de novos protocolos que resolvam esses problemas (e com certeza irão trazer outros novos).

A abordagem apresentada de utilização do IPSec como links seguros ponto a ponto através do tunelamento via IPIP ou GRE pode representar um investimento em uma solução segura, viável e escalável. Atualmente é possível em uma topologia *hub-and-spoke* com roteamento dinâmico conseguir-se um alto grau de escalabilidade, segurança e tolerância a falhas. As empresas que considerarem as soluções propostas para uma topologia tipo estrela viáveis para o fluxo de dados da rede, encontrarão neste trabalho uma solução caso o protocolo escolhido seja o IPSec em uma abordagem CPE. O IPIP tem a vantagem de estar em discussão (drafts) pelo IETF atualmente, o que pode indicar uma futura padronização.

O trabalho demonstra por meio da apresentação dos conceitos básicos de uma VPN, que ainda gera muita confusão no mercado corporativo, que existem várias soluções para o problema da comunicação. Entretanto, nem sempre as soluções mais simples e/ou que garantam um determinado nível de qualidade de serviço podem ser consideradas seguras. Muitas das vezes uma VPN baseada em MPLS pode perfeitamente servir de base para uma VPN baseada em IPSec com um grau de segurança muito mais elevado.

É importante ressaltar ainda o item "confiança no provedor de serviços". A partir do momento que a VPN foge totalmente ao controle da organização virando uma espécie de "caixa preta", implica que toda a segurança da rede está nas mãos do elo mais fraco, que no caso das VPNs baseadas em rede são os provedores de serviço. Este trabalho expõe os serviços oferecidos em cada abordagem, e demonstra a necessidade da implementação da segurança corporativa conforme a sensibilidade dos dados que irão trafegar pela VPN (além dos possíveis pontos de entrada/saída da rede). Essa segurança só pode ser alcançada realmente com a implementação de uma VPN segura, seja sobre a Internet ou sobre um backbone privado.

Até este ponto é possível montar uma solução escalável e segura baseada em IPSec, que conforme apresentado leva uma série de vantagens sobre os demais protocolos utilizados para implementação de uma VPN segura. No entanto, o mapeamento dinâmico dos gateways para se conseguir *mesh* dinâmico ainda depende da implementação proprietária de certos fabricantes. A utilização do DNS é considerada atualmente pelo IETF, mas o principal problema de se conseguir *mesh* de maneira gerenciável e viável ainda não foi devidamente abordado para um ambiente corporativo. O presente trabalho apresenta algumas sugestões para consideração no desenvolvimento de novas funcionalidades para o IPSec, que atualmente visa através do DNS prover conexões entre redes de diferentes organizações, mais precisamente na utilização de serviços disponibilizados por diferentes

redes de forma segura.

Com este trabalho foi possível reunir uma análise que vai dos conceitos básicos de uma VPN, passando pela análise de abordagens e protocolos e a apresentação dos principais problemas do IPSec em uma rede de alta capilaridade: o roteamento dinâmico sobre IPSec e o mapeamento dinâmico dos gateways. Além disso, uma série de detalhes relevantes como o posicionamento e dimensionamento do gateway VPN são devidamente abordados, poupando muito esforço e desperdício de recursos no desenho de uma solução corporativa. O IPSec apresenta muitas das características desejadas para uma grande rede, e conforme demonstrado, pode ser perfeitamente utilizado desde que sua complexidade seja devidamente analisada e considerada.

8.2 Trabalhos futuros

No início deste trabalho o simples fato do "número elevado de túneis" não parecia algo assustador ou preocupante. No entanto esta pesquisa revelou um cenário ainda pouco explorado, que apesar de soluções comerciais se proporem a resolver o problema, a interoperabilidade e padronização do IPSec almejados inicialmente ainda estão longe de serem atingidos.

Com isso o trabalho ganhou em volume, até atingir o ponto desejado que foi elencar algumas soluções sob um ponto de vista crítico, visando o trabalho em andamento do IETF em paralelo com as soluções comerciais.

A partir deste ponto uma série de trabalhos podem ser realizados, como testes comparativos entre as soluções apresentadas nos quesitos recuperação de falhas, desempenho e gerenciamento. O próprio Capítulo 7 demonstra muitos dos tópicos não abordados de forma profunda neste trabalho.

A autenticação especificamente também é fator importante, e a análise de soluções envolvendo uma infra-estrutura de chaves púbicas (PKI) em termos de implementação, pode ser de grande valia para uma solução VPN completa. As discussões sobre PKI vão desde certificação cruzada até facilidade de uso e implementação.

Análise de QoS em redes IPSec baseadas em CPE é um tópico ainda pouco discutido, além de integração do IPSec com redes específicas (como *Windows Active Directory*) nos cenários propostos.

A integração do acesso remoto nestes cenários e redes hostis (como parceiros comerciais) também podem dar continuidade a esta pesquisa, garantindo o sucesso da popularidade do IPSec no mercado de VPNs.

Glossário

B2B Business-to-Business, Troca eletrônica de informações entre parceiros comerciais, como indústria e revenda.

B2C Business-to-Consumer, Troca eletrônica de informações entre empresas e seus clientes finais (como loja virtual).

Backbone Conjunto de roteadores que formam o "*core*", onde os dados de várias redes trafegam de uma LAN para outra.

Backup Cópia de segurança dos dados ou dispositivo que pode substituir um outro em funcionamento em caso de falha.

Broadcast Mensagem destinada a todos os Hosts de um determinado domínio de colisão.

bytes de padding
Bytes necessários para se conseguir um pacote de tamanho sempre fixo para utilização dos algoritmos de criptografia e/ou autenticação. Funcionam como um "enchimento".

Cable Modem
Tecnologia de transferência de dados e acesso à Internet utilizando a infraestrutura da TV a cabo.

Call-back Método pelo qual o RAS identifica o número chamador ou pede para que o usuário informe um número e disca de volta para o usuário, dentro de uma lista de números permitidos e identificando de onde veio a conexão.

Cavalo de Tróia
Código malicioso que se instala na máquina sem a percepção do usuário a fim de abrir brechas de segurança para eventuais ataques de hackers.

Clustering Método de tolerância a falhas que faz com que dois (ou mais) dispositivos físicos pareçam logicamente um único dispositivo, sendo que na falha de

um deles o outro assuma automaticamente e de modo transparente aos serviços oferecidos.

CPE Customer Premisse Equipment, Equipamento de início do túnel que fica localizado no cliente e não no Service Provider.

DDG Serviço disponível onde a ligação é paga pelo recebedor da chamada conforme contrato com a companhia telefônica. São os número iniciados por 0800 no Brasil.

Dial-Up Conexão discada via linha telefônica comum.

DMZ De-militized Zone, Sub-rede localizada entre a rede interna e a rede externa.

DoS Denial of Service ou Negação de Serviço. Ataque que explora a vulnerabilidade de um determinado servidor não poder distinguir requisições falsas das legítimas, explorada por meio da solicitação falsa em massa de um serviço específico, saturando o servidor e evitando que o mesmo responda a requisições legítimas.

EDI Eletronic Data Interchange - Troca de dados largamente utilizada entre as empresas através do envio e recebimento de arquivos textos com layout específico e acordado entre as partes.

End-Point Máquina ou *Host* onde termina e/ou começa uma conexão, túnel etc.

Firewalls Distribuídos
Arquitetura proposta por Bellovin, onde o controle exercido pelo Firewall na borda da rede passa a ser distribuído para as máquinas finais, mudando o conceito de perímetro e centralização da segurança de borda.

GW Gateway VPN.

hacker Apesar de ser utilizado na maioria das vezes como um "atacante" no mundo da informática, a palavra hacker indica uma pessoa com altos conhecimentos de segurança e como burlar muitos dos sistemas existentes. Cracker seria uma palavra mais indicada para a utilização dos conhecimentos de um hacker de maneira negativa.

hash Pra não criptografar uma mensagem muito grande, são aplicados algoritmos, com base em um segredo ou chave, que geram uma porção menor do conteúdo original, denominados hash. Os algoritmos mais utilizados são

o MD5 e o SHA-1. Uma propriedade importante destes algoritmos é que duas mensagens diferentes não podem gerar o mesmo hash, por motivos de segurança.

Hop Roteador ou gateway no caminho entre dois end-poits.

Hot-Swap Processo em que um em caso de falha em um dispositivo atuando como primário é substituído automaticamente e de forma transparente por um outro dispositivo (secundário) em estado de espera.

HSRP Hot Standby Router Protocol, descrito sob RFC 2281 visando o Hot-Swap.

HUB Concentrador, no caso de VPNs, quando se fala em topologia, é o *site* principal, geralmente a matriz, com o qual todos os demais *sites* tem que se conectar.

IETF Internet Engineering Task Force.

Initiator *Host* ou Gateway que inicia o estabelecimento do canal seguro para passagem dos dados.

IPIP Protocolo de tunelamento IP sobre IP, descrito na RFC 2003.

ISDN Integrated Services Digital Network, é um sistema de conexões telefônicas digitais que estiveram em uso por mais de uma década. Este sistema permite voz e dados serem transmitidos simultâneamente através do globo terrestre usando conexão digital fim-a-fim.

ISP Internet Service Provider - Empresa responsável por prover acesso à rede mundial (Internet) a todos os seus clientes.

Joint-Ventures Fusão de algumas empresas em um contrato legal específico.

LAN Local Area Network, Rede Local.

MPLS Multi-Protocol Label Switching, protocolo utilizado para estabelecer canais virtuais visando principalmente a engenharia de tráfego

MTU Maximum Transmission Unit, ou tamanho máximo do pacote que passa em um determinado segmento de rede. Se o mesmo exceder o MTU será fragmentado.

NAT Network Address Translation, técnica que utiliza o mapeamento de endereços inválidos geralmente utilizados em redes internas par endereços IP válidos, de modo que os Hosts sejam capazes de se comunicar via Internet, enviando e recebendo pacotes corretamente.

OC-Lines Links de fibra óptica, que são classificados conforme velocidade do link.

overhead cabeçalhos adicionados além dos cabeçalhos do protocolo original.

overlay Sobreposição.

payload Porção de dados de um pacote qualquer.

POP Point of Presence, ou ponto de presença. É o ponto onde o SP provê uma conexão para que seus clientes possam acessar seu backbone e utilizar os serviços contratados.

QoS Quality of Service, Qualidade de serviço exigida e/ou garantida por determinado tipo de rede, geralmentes através de um SLA, podendo considerar por exemplo garantias de throughput por tipo de aplicação.

RAS Remote Access Server, responsável por aceitar e gerenciar as conexões Dial-Up, provendo acesso à rede.

Responder *Host* ou Gateway que recebe de um outro *Host* ou Gateway um pedido para estabelecer um canal seguro.

Road-Warriors Pessoas que utilizam o acesso remoto em vários lugares, pois na maioria das vezes estão sempre em viagem, utilizando portanto pontos de acesso à Internet em cafés, aeroportos, hotéis etc.

RW O mesmo que Road-Warrior.

SP Service Provider - Empresa responsável por prover soluções de comunicação a outras corporações.

Spoke São *sites* "satélites", ou seja, no caso do objeto de estudo uma filial ou escritório. Numa topologia estrela, temos o centro como o Hub e as pontas como Spokes.

SSL Security Socket Layer, protocolo que visa segurança no nível de aplicação, descrito no capítulo de protocolos.

SSO Single Sign-On, método de autenticação onde o usuário utiliza um único mecanismo de autenticação, se autenticando apenas uma vez e utilizando todos os serviços necessários sem necessidade de identificação posterior até que o mesmo efetue um logout

Supply Chain Cadeia de fornecimento entre Indústria, revenda e consumidor. Envolve forte integração de sistemas e análise estatíscas de demanda, a fim de que o ressuprimento seja feito corretamente em toda cadeia, sem faltas ou sobras, permitindo ganhos diversos como melhor planejamento de infra-estrutura.

Switch Repetidor de dados que considera o endereço de enlace e com isso isola o tráfego às portas correspondentes de cada endereço, evitando colisões.

T-Carriers Links tradicionais de dados no padrão americano, conforme velocidade. Na Europa são utilizados linhas do tipo E-Carriers, também variando a classificação conforme velocidade.

Throughput Volumes de dados que são transmitidos em uma determinada unidade de tempo.

TI Tecnologia da Informação, Expressão usada para descrever profissionais, setores, empresas etc. ligadas à área de informática.

VLAN Virtual LAN - utilização de um switch para criar duas ou mais sub-redes isolando o tráfego entre elas, necessitando um roteador para passar os pacotes entre as vlans.

VRRP Virtual Router Redundancy Protocol, descrito sob RFC 2338 visando facilitar a clusterização.

WAN Wide Area Network, Interconexão de LANS.

Wardialing Técnica de ataque onde os hackers buscam vários modens em estado de espera para uma tentativa de conexão

xDSL DSL (Digital Subscriber Line) é uma tecnologia utilizada para prover acesso banda-larga utilizando pares metálicos de telefonia comum presente na maioria das casas/empresas. xDSL Se refere a diferentes variações de DSL, como ADSL, HDSL, RADSL, entre outros.

Referências Bibliográficas

[Alt02] Gary Alterson. Comparing BGP/MPLS and IPSec VPNs. *SANS Institute - GIAC Security Essentials (GSEC)*, 2002.

[And03] Andrew S. Tanenbaum. *Computer Networks*. PH PTR, 4th edition, 2003.

[Atk98a] S. Kent; R. Atkinson. IP Authentication Header. In *Request for Comments 2402*, 1998.

[Atk98b] S. Kent; R. Atkinson. IP Encapsulating Security Payload (ESP). In *Request for Comments 2406*, 1998.

[Atk98c] S. Kent; R. Atkinson. Security Architecture for the Internet Protocol. In *Request for Comments 2401*, 1998.

[Bak00] H. X. Mel; Doris M. Baker. *Cryptography Decrypted*. Addison-Wesley, 2000.

[Bel96] S. M. Bellovin. Problem Areas for the IP Security Protocols. In *Proceedings of the Sixth Usenix UNIX Security Symposium*, San Jose, California, USA, 1996.

[Bel99] Steven M. Bellovin. Distributed Firewalls. ATT Research, http://www.research.att.com/ smb/papers/distfw.html, Novembro 1999. Consulta em 24/07/2003.

[Bel04] S. M. Bellovin. Guidelines for Mandating the Use of IPSec. In *Internet Draft*, draft-bellovinuseipsec-03.txt, 2004.

[Cal03] Calum Macleod. Freeing the Shackles with Secure Remote Working. SC Infosec Opnionwire, http://www.infosecnews.com/opinion/2003/10/22_01.htm, Outubro 2003. Consulta em 23/10/2003.

[Car98] D. Harkings; D. Carrel. The Internet Key Exchange (IKE). In *Request for Comments 2409*, 1998.

[Cle03] Cleymone Ribeiro dos Santos; Edmar R. S. de Rezende; João Porto de Albuquerque; Paulo Lício de Geus. Impactos da Utilização de IPv6 em Ambientes Seguros. Submetido ao SSI-2003, 2003.

[Com98] Netscape Communications. Introduction to SSL. Netscape, http://developer.netscape.com/docs/manuals/security/sslin/contents.htm, Setembro 1998. Consulta em 23/05/2003.

[Coo00] D. B. Chapman; E. D. Zwicky; S. Cooper. *Building Internet Firewalls*. Editora O'Reilly, second edition, 2000.

[Dav03] David Aylesworth. Why you should replace frame relay with a VPN. COMPUTERWORLD, http://www.computerworld.com/printthis/2003/0,4814,82304,00.html, Junho 2003. Consulta em 24/06/2003.

[dG02a] Emílio Tissato Nakamura; Paulo Lício de Geus. *Segurança de Redes em Ambientes Cooperativos*. Editora Berkeley, São Paulo, Brasil, 2002.

[dG02b] Francisco J. C. Figueiredo; Paulo Lício de Geus. Colocação do VPN na configuração do Firewall. In *III Simpósio sobre Segurança em Informática*, pages 175–181, S. José dos Campos, SP, Brasil, 2002.

[dG03] Paulo Lício de Geus. Curso de administração e segurança de redes. Universidade Estadual de Campinas - UNICAMP, 2003.

[Dor98] J. Luciani; D. Katz; D. Piscitello; B. Cole; N. Doraswamy. NBMA Next Hop Resolution Protocol (NHRP). In *Request for Comments 2332*, 1998.

[dRPLdG02] Edmar R. S. de Rezende; Paulo Lício de Geus. Análise de Segurança dos Protocolos utilizados para Acesso Remoto VPN em Plataformas Windows. In *IV Simpósio sobre Segurança em Informática*, page Disponível em CDROM, S. José dos Campos, SP, Brasil, 2002.

[dS03] Lino Sarlo da Silva. *Virtual Private Network - Aprenda a construir VPNs em plataformas Linux e Windows*. Editora NOVATEC, 2003.

[Dun01] Neil Dunbar. IPSec Networking Standards - An Overview. *Information Security Technical Report*, 6(1):35–48, 2001.

[E. 00] E. T. Nakamura. Um modelo de Segurança de Redes para Ambientes Cooperativos. Dissertação de mestrado, IC/UNICAMP, 2000.

[Eas99] D. Eastlake. Domain Name System Security Extensions. In *Request for Comments 2535*, 1999.

[Edm04] Edmar R. S. de Rezende. Segurança no acesso remoto VPN. Dissertação de mestrado, IC/UNICAMP, 2004.

[Flu02] S. Fluhrer. Tunnel EndPoint Discovery. In *Internet Draft*, draft-fluhrer-ted-01.txt, 2002.

[For98] Frame Relay Forum. *The basic Guide to Frame Relay Networking*. 1998.

[Gle04] Paul Knight; Bryan Gleeson. A Method to Provide Dynamic Routing in IPSec VPNs. In *Internet Draft*, draft-knight-ppvpn-ipsec-dynroute-03.txt, 2004.

[Gre] Tim Greene. Network World puts SSL through its paces. NetworkWorldFusion, http://www.nwfusion.com/newsletters/vpn/2004/0112vpn1.html, January.

[Gro02] Yankee Group. The Evolution of Virtual Private Networks. *The Yankee Group Report*, Outubro 2002.

[Har03] Jon Harrison. VPN Technologies - A Comparison. *Data Connection Limited - http://www.dataconnection.com*, 2003.

[Hat02] O. Kolesnikov; B. Hatch. *Building Linux Virtual Private Networks*. Editora New Riders, 2002.

[Hel76] W. Diffie; M. Hellman. *New Directions in Cryptography*. IEEE Transactions on Information Theory, 1976.

[Hin95] S. Deering; B. Hinden. Internet Protocol version 6. In *Standars Track Request for Comments 1883*, 1995.

[Jan02] Jansen Carlo Sena. Um modelo para proteção do tráfego de serviços baseado em níveis de segurança. Dissertação de mestrado, IC/UNICAMP, 2002.

[Jas02] Jason Wright. Security Market - Bullish on VPNs. Infosecurity Magazine, http://www.infosecuritymag.com/2002/jun/bullish.shtml, Junho 2002. Consulta em 09/07/2003.

[Jim04] Jim Metzler. Crafting SLAs for Private IP Services. Webtorials - IT Bussiness Brief, Fevereiro 2004.

[Jon03] Jonathan Gossels; Brad C. Johnson, and Cheng Tang. Wardialing - The Forgotten Front in the War against Hackers. SC Infosec Opnionwire, http://www.infosecnews.com/opinion/2003/07/30_02.htm, Julho 2003. Consulta em 04/08/2003.

[JTLE04] Y. Wang J. Touch; L. Eggert. Use of IPSec Transport Mode for Dynamic Routing. In *Internet Draft*, draft-touch-ipsec-vpn-071.txt, 2004.

[Ken98] R. Glenn; S. Kent. The NULL Encryption Algorithm and Its Use With IPsec. In *Request for Comments 2410*, 1998.

[Kle90] D. V. Klein. Foiling the cracker: A security of, and implications to, password security. In *II USENIX Workshop on Security*, pages 5–14, 1990.

[Kni] Paul Knight. *Dynamic Routing Inside IPSec VPNs - New Treats and Defenses*. Nortel Networks, Black Hat Briefings.

[Kra96] H. Krawczyk. Skeme: A versatile secure key exchange mechanism for internet. In *Proceedings of the Symposium of Network and Distributed System Security*, San Diego, 1996.

[Li98] T. Li; B. Cole; P. Morton; D. Li. Cisco Hot Standby Router Protocol (HSRP). In *Request for Comments 2281*, 1998.

[Lin98] S. Knight; D. Weaver; D. Whipple; R. Hinden; D. Mitzel; P. Hunt; P. Higginson; M. Shand; A. Lindem. Virtual Router Redundancy Protocol. In *Request for Comments 2338*, 1998.

[Max02] Max Smetannikov. Better, or just different? - WorldCom's project for Toyota calls to light the trade-offs of Network-based versus CPE-based VPNs. HOSTINGTECH, http://www.hostingtech.com/nm/02_04_nm_better_print.html, Abril 2002. Consulta em 23/09/2003.

[Mey96a] G. Meyer. The PPP Compression Control Protocol (CCP). In *Request for Comments 1962*, 1996.

[Mey96b] G. Meyer. The PPP Encryption Control Protocol. In *Request for Comments 1968*, 1996.

[Mic02] Microsoft. *Windows 2000 Server Administration Guide - Configuring Active Directory and ISA Server*. Mircrosoft, 2002.

[Moc87a] P. Mockapetris. DOMAIN NAMES - CONCEPTS AND FACILITIES. In *Request for Comments 1034*, 1987.

[Moc87b] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. In *Request for Comments 1035*, 1987.

[Net] Nortel Networks. Dynamic Routing Inside IPsec VPNs - New Threats and Defenses. Nortel Networks Manuals.

[Net04a] Nortel Networks. Layered Network Security Defense - Protecting the enterprise network. *Nortel Networks White Paper*, 2004.

[Net04b] Nortel Networks. The seven attributes of a successful IP-VPN. *Nortel Networks White Paper*, 2004.

[Pat01] B. Patel. Securing L2TP Using IPSEC. In *Request for Comments 3193*, 2001.

[Per96] C. Perkins. IP Encapsulation within IP. In *Request for Comments 2003*, 1996.

[Pos81] J. Postel. Internet Protocol DARPA Internet Program Protocol Specification. In *Request for Comments 791*, 1981.

[Red04] M. Richardson; D. Redelmeier. Opportunistic Encryption using The Internet Key Exchange (IKE). In *Internet Draft*, draft-richardson-ipsec-opportunistic-17.txt, 2004.

[Ric04] M. Richardson. A Method for Storing IPSec Keying Material in DNS. In *Internet Draft*, draft-ietf-ipseckey-rr-11.txt, 2004.

[Sch96] B. Schneier. *Applied Cryptography*. Joe Wiley & Sons, second edition, 1996.

[Sch99] N. Ferguson; B. Schneier. A Cryptographic Evaluation of IPSec. In *Counterpane Internet Security Inc.*, 1999.

[Sch00] C. Ellison; B. Schneier. Ten Risk of PKI: What you're not being told about PKI. In *Computer Security Journal*, volume 16, 2000.

[Sec02] RSA Security. Implementing a Secure Virtual Private Network. RSA Security, http://www.rsasecurity.com, 2002. Consulta em 10/12/2003.

[Sim94] W. Simpson. The Point-to-Point Protocol (PPP). In *Request for Comments 1661*, 1994.

[Sta98] W. Stallings. A Secure Foundation for VPNs. Info Security Magazine, http://www.infosecuritymag.com/articles/1998/vpn.shtml, março 1998. Consulta em 25/05/2003.

[Ste03] Andreas Steffen. Virtual Private Networks - Coping with Complexity. In *17th DFN-Workshop on Communications Networks*, 2003.

[Str01] R. Yuan; W. T. Strayer. *Virtual Private Networks - Technologies and Solutions*. Editora Addison-Wesley, 2001.

[Str03] Olivier Strahler. Network Based VPNs. *SANS Institute - GIAC Security Essentials (GSEC)*, 2003.

[Sys] Cisco Systems. *Cisco IOS Enterprise VPN Configuration Guide*. Cisco Configuration Guides, Chapter 2 - Network Design Considerations.

[Sys00] Cisco Systems. IPSec. *Cisco Systems White Paper*, 2000.

[Sys03a] Cisco Systems. Deploying Complex and Large Scale IPSec VPNs. *Networkers 2003 - Session SEC-2012*, 2003.

[Sys03b] Cisco Systems. Deploying site-to-site IPSec VPNs. *Networkers 2003 - Session SEC-2011*, 2003.

[Sys03c] Kevin Regan Consulting Systems Engineer Cisco Systems. Secure VPN Design Considerations. *Network Security*, Maio 2003.

[Tea04] FreeS/WAN Team. AH removed from FreeS/WAN. FreeS/WAN Web-Site, http://www.freeswan.org/no_ah.html, fevereiro 2004. Consulta em 29/02/2004.

[Tec00] B. Gleeson; A. Lin; Nortel Networks; J. Heinanen; Telia Finland; G. Armitage; A. Malis; Lucent Technologies. A Framework for IP Based Virtual Private Networks. In *Request for Comments 2764*, 2000.

[Tec03] NetScreen Technologies. Requirements for Deploying Scalable, Secure, Dynamic VPNs. *NetScreen White Paper*, 2003.

[Tho98] A. Shacham; R. Monsour; R. Pereira; M. Thomas. IP Payload Compression Protocol (IPComp). In *Request for Comments 2393*, 1998.

[Tow99] W. Townsley. Layer Two Tunneling Protocol (L2TP). In *Request for Comments 2661*, 1999.

[Tra00] D. Farinacci; T. Li; S. Hanks; D. Meyer; P. Traina. Generic Routing Encapsulation (GRE). In *Request for Comments 2784*, 2000.

[Tue03] Vince Tuesday. Bad Policy Makes for Weak Passwords. COMPUTERWORLD, http://www.computerworld.com/printthis/2003/0,4814,87540,00.html, Dezembro 2003. Consulta em 01/12/2003.

[Tur98] D. Maughan; M. Schertler; M. Schneider; J. Turner. Internet Security Association and Key Management Protocol (ISAKMP). In *Request for Comments 2408*, 1998.

[Uylio] Uyless Black. *Internet Security Protocols*. Prentice Hall, New Jersey, 2000, 2º edição.

[VPN04] VPN Technologies: Definitions and Requirements. VPN Consortium, http://www.vpnc.org/vpn-technologies.html, janeiro 2004. Consulta em 20/01/2004.

[Vyn02] A. Kethan; C. Wang; M. Beadles; L. French; E. Vyncke. Use of GRE for routing support in IPSec VPNs. In *Internet Draft*, draft-kethan-sp-greipsec-00.txt, 2002.