Segurança no Acesso Remoto VPN

Edmar Roberto Santana de Rezende

Dissertação de Mestrado

Instituto de Computação
Universidade Estadual de Campinas

Segurança no Acesso Remoto VPN

Edmar Roberto Santana de Rezende[1]

Fevereiro de 2004

Banca Examinadora:

- Prof. Dr. Paulo Lício de Geus (Orientador)
- Prof. Dr. Ricardo Felipe Custódio
  Departamento de Informática e de Estatística, UFSC
- Prof. Dr. Ricardo Dahab
  Instituto de Computação, UNICAMP
- Prof^{a}. Dr^{a}. Islene Calciolari Garcia (Suplente)
  Instituto de Computação, UNICAMP

[1]**Financiado por Robert Bosch Ltda**

Segurança no Acesso Remoto VPN

Este exemplar corresponde à redação final da Dissertação devidamente corrigida e defendida por Edmar Roberto Santana de Rezende e aprovada pela Banca Examinadora.

Campinas, 27 de fevereiro 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.

À minha família, minha namorada
e meus amigos, meus três pilares
ao longo dessa caminhada.

Houve um tempo em que se fazia
ciência a partir de quatro elementos:
água, terra, fogo e ar. Naquele tempo
não se sabia que é possível fazer
qualquer coisa com apenas dois:
vontade e imaginação.

Agradecimentos

A Deus que, mesmo quando não me lembrei Dele, se fez presente em todos os momentos.

Aos meus pais, Edmar e Marise, pelo amor sincero e incondicional, por estarem ao meu lado mesmo distantes e, sobretudo, por sempre terem sido minha motivação maior.

À minha namorada Daniela, pelo amor que a distância só foi capaz de aumentar.

Aos meus irmãos, Flávia, Emília Fernanda, Eduardo e Erick, e meu sobrinho Henrique, pelo carinho e pelos incontáveis momentos de alegria.

À minha avó Marieta e ao meu eterno avô Lázaro pelo carinho, e a todos os meus familiares, que sempre compreenderam minha ausência.

Ao meu orientador, Paulo Lício de Geus, pelo apoio não só profissional como pessoal, e também pelas inúmeras oportunidades proporcionadas.

Aos professores do Instituto de Computação, em especial ao Prof. Cid Carvalho de Souza, pela atenção e constante acompanhamento durante a realização do estágio docente, e ao Prof. Ricardo Pannain, pela oportunidade profissional concedida na PUC-Campinas.

Aos integrantes do LAS, Cleymone, João Porto, Fernando, Felipe, Ruppert, Diogo, Arthur, Eduardo, Martim e Thiago, aos novos integrantes e aos antigos amigos Jansen, Flávio, Fabrício, Diego, Marcelo e Alessandro pela convivência agradável e conversas enriquecedoras.

À amiga Helen, pela dedicação e enorme ajuda na revisão deste trabalho, e também ao amigos Robledo e Rita, fundamentais nos momentos decisivos.

Aos meus companheiros de república, Rafael, Fabiano, Eduardo, Fernando e Chico, e aos antigos ilhados, Patrick e Hortência, pela amizade e companheirismo, em especial ao Antônio (Roska), pela força em minha chegada à Campinas.

Aos meus grandes amigos, Os Malditos — Chenca, Flavinho, Lásaro, Marcelo, Baboo, Quintão, Fernando, Celso e Anibal —, Pistolinhas — Zeh, Baiano, Guido e Triste —, Magrão, Glauber (do Fantástico), Bartho, Wanderley, Márcio, Pará, Borin, Messias ... e a todos que de alguma forma deixaram um pouco de si e levaram um pouco de mim.

À empresa Robert Bosch pelo apoio financeiro, em especial ao Cláudio Nobre pela atenção.

Resumo

As Redes Privadas Virtuais (*Virtual Private Network* – VPN) são um componente importante dentro de um ambiente cooperativo, principalmente em seu aspecto econômico, ao permitirem que conexões dedicadas e estruturas de acesso remoto, que possuem custos bastante elevados, sejam substituídas por conexões públicas. Contudo, a conseqüente utilização de uma rede pública para o tráfego de informações privadas e a extensão do perímetro de segurança das organizações, trazem consigo sérias implicações de segurança. O acesso remoto VPN, onde o usuário remoto acessa diretamente os recursos da organização, possui implicações de segurança específicas ainda mais sérias que precisam ser consideradas. Neste contexto, a escolha de um conjunto de mecanismos de segurança capazes de prover uma solução adequada para os diversos possíveis cenários de acesso remoto constitui uma decisão fundamental para a segurança do ambiente cooperativo.

Neste trabalho foi realizado um amplo estudo dos diversos aspectos envolvidos na elaboração de uma solução segura e viável de acesso remoto VPN. Através desta análise foi possível identificar os principais requisitos e avaliar algumas das soluções existentes que compõem esse complexo cenário. Como resultado da avaliação desses fatores foi possível desenvolver uma solução de acesso remoto VPN utilizando o software FreeS/WAN, uma implementação Open Source do protocolo IPSec baseada em Linux. Devido à expressiva parcela de mercado ocupada por produtos Microsoft, também foram abordadas algumas soluções de clientes VPN baseados em Windows.

Abstract

A Virtual Private Network (VPN) is an important component in a cooperative computing environment, since it allows expensive dedicated connections and remote access infrastructures to be substituted by cheaper public connections. However, the use of a public network for transporting private information, and the consequent extension of an organization's security perimeter, brings serious implications for information security. Remote access VPN, in which a remote user has direct access to an organization's resources, has even more serious, specific, security implications that must be addressed. In this context, the choice of the most appropriate security mechanisms for enabling remote access whilst ensuring the security of the cooperative environment, in a diverse range of possible scenarios, is a fundamental decision.

This work presents the results of a detailed study of the diverse aspects involved in the elaboration of a secure and viable remote access VPN solution. From this study, it has been possible to identify the principal requirements for remote access VPN and review some of the existing solutions available for this complex scenario. Using these results, a remote access VPN solution has been developed using the FreeS/WAN software, an open-source implementation of the IPSec protocol for Linux. Due to the significant market share occupied by Microsoft products, some Windows based client VPN solutions are also discussed.

Sumário

Lista de Figuras

Capítulo 1

Introdução

1.1 Motivação

Durante anos, o acesso remoto foi tipicamente caracterizado por usuários remotos acessando recursos privados de uma organização através de uma rede de telefonia pública, com a conexão discada terminando em um servidor de acesso à rede localizado na rede da organização.

É importante notar que, para tal acesso, freqüentemente assume-se que a infra-estrutura de comunicação utilizada para acessar o servidor, neste caso a rede de telefonia pública, é relativamente segura, não apresentando nenhuma ameaça significativa à confidencialidade e integridade da comunicação. Com base nesta suposição, a segurança da conexão se limitava a um controle de acesso no servidor de acesso à rede, baseado em um par usuário/senha. Contudo, na realidade, as comunicações sobre uma rede de telefonia pública nunca foram invioláveis a um atacante.

A enorme difusão da Internet e a crescente disponibilidade do acesso de banda larga, em conjunto com o desejo de redução dos altos custos do acesso discado, têm conduzido ao desenvolvimento de mecanismos de acesso remoto baseados na Internet. Esse tipo de acesso remoto, comumente chamado de acesso remoto VPN, utiliza a tecnologia de Redes Privadas Virtuais (VPN), possibilitando que uma infra-estrutura de rede pública, como a Internet, seja utilizada como backbone para a comunicação entre o usuário remoto e a rede privada.

Em alguns casos, o usuário remoto acessa primeiramente um Provedor de Acesso à Internet (*Internet Service Provider* – ISP), e em seguida estabelece uma conexão virtual adicional sobre a Internet até a rede privada. A facilidade de acesso e o alcance global da Internet, no entanto, possibilitam a existências de vários outros cenários de acesso remoto VPN. Contudo, a tarefa de satisfazer os requisitos de segurança das várias classes de usuários de acesso remoto apresenta vários desafios.

Junto aos inúmeros benefícios trazidos pelo acesso remoto VPN, surgem também uma série de implicações, principalmente quanto à segurança das informações, que passam a correr riscos com relação à sua confidencialidade e à sua integridade, já que passam a trafegar através de uma rede pública. Além disso, a extensão do perímetro de segurança da rede privada, que passa a englobar a máquina remota, pode expor a rede da organização a novas ameaças que devem ser avaliadas e solucionadas.

Como a segurança é um fator crucial, o profundo conhecimento dessas novas ameaças e a adoção de um conjunto de mecanismos de segurança capazes de atender aos requisitos impostos nestes cenários torna-se vital para o desenvolvimento de uma solução de acesso remoto VPN segura e viável.

Todas essas vantagens e novas possibilidades representam um forte incentivo à migração do velho modelo de acesso discado para um modelo mais seguro de acesso remoto VPN.

Neste trabalho foi realizado um amplo estudo dos diversos aspectos envolvidos na elaboração de uma solução de acesso remoto VPN segura.

Através de uma análise inicial dos protocolos normalmente utilizados, foi possível nortear as decisões seguintes fundamentadas no uso do protocolo IPSec, devido às suas características de segurança mais capazes.

Uma posterior avaliação dos cenários mais comuns de acesso remoto baseado em IPSec possibilitou a identificação de um conjunto de requisitos comuns apresentado na maioria dos casos.

Identificados os requisitos, a etapa seguinte consistiu em levantar as soluções existentes para cada um desses requisitos em particular, e avaliar tais soluções quanto aos seus aspectos positivos e negativos, facilitando assim futuras decisões.

Como conseqüência das etapas anteriores foi implementada uma solução de acesso remoto VPN baseada no uso do software FreeS/WAN em sistemas Linux, visando atender aos diversos requisitos mencionados. Além disso, soluções de clientes VPN baseadas em sistemas Windows também foram abordadas.

Complementando a análise dos aspectos de segurança envolvidos em um ambiente de acesso remoto VPN, foram abordadas também algumas considerações adicionais a respeito do posicionamento de um gateway VPN na topologia de segurança de uma organização.

1.2 Organização do trabalho

Baseado nas etapas do desenvolvimento deste trabalho, os diversos aspectos envolvidos na elaboração de uma solução de acesso remoto VPN foram agrupados e discutidos na seqüencia apresentada a seguir.

Inicialmente são apresentadas no Capítulo 2 as Redes Privadas Virtuais (VPN), fornecendo os conceitos básicos necessários ao entendimento desta tecnologia.

No Capítulo 3 são apresentadas as características básicas e uma análise de segurança dos principais protocolos utilizados atualmente para acesso remoto VPN.

No Capítulo 4 são apresentados alguns dos cenários mais comuns de acesso remoto VPN utilizando IPSec, procurando identificar e explorar os requisitos de cada um, a fim de obter um conjunto geral de requisitos que seja comum à maioria dos casos.

No Capítulo 5 são discutidas algumas das soluções existentes para cada um dos requisitos dos cenários de acesso remoto VPN, com o objetivo de obter um conjunto de mecanismos que viabilizem o acesso remoto VPN utilizando IPSec.

No Capítulo 6 são detalhadas as decisões de implementação e alguns dos aspectos específicos da configuração de uma solução de acesso remoto VPN baseada em FreeS/WAN. Além disso, são abordadas também algumas soluções de clientes VPN baseadas em Windows, principalmente nos sistemas Windows 2000 e Windows XP.

No Capítulo 7 são feitas algumas considerações a respeito do posicionamento do gateway VPN na topologia de segurança de uma organização, procurando identificar as principais vantagens e desvantagens de cada alternativa.

Por fim, são apresentadas no Capítulo 8 algumas considerações e conclusões gerais sobre todas as etapas envolvidas no desenvolvimento deste trabalho, além de algumas sugestões de possíveis tópicos de pesquisa.

Também são apresentados no Apêndice A alguns exemplos de arquivos de configuração e um detalhamento maior dos parâmetros utilizados na implementação do acesso remoto VPN utilizando FreeS/WAN.

Capítulo 2

Redes Privadas Virtuais (VPN)

As Redes Privadas Virtuais (VPN) possuem uma importância cada vez maior para os negócios das organizações, ao possibilitarem o uso de uma infra-estrutura de rede pública, como a Internet, para o estabelecimento de conexões entre a rede da organização e suas filiais, parceiros estratégicos e usuários remotos.

No caso específico de um usuário remoto acessando a rede de uma organização, a substituição dos mecanismos de acesso remoto tradicional por mecanismos baseados no uso de VPNs sobre a Internet pode trazer vantagens significativas em relação ao custo, escalabilidade e viabilidade da solução.

A seguir serão apresentados alguns dos conceitos básicos que fundamentam as Redes Privadas Virtuais. Tais conceitos influem diretamente no nível de segurança provido por uma determinada solução de acesso remoto VPN, e por isso são necessários ao entendimento desta tecnologia.

2.1 Visão geral

As Redes Privadas Virtuais (*Virtual Private Network* – VPN) são um componente importante dentro de um ambiente cooperativo, principalmente no seu aspecto econômico, ao permitirem que conexões dedicadas e estruturas de acesso remoto tradicionais, que possuem custos bastante elevados, sejam substituídas por conexões públicas.

Seu principal objetivo é permitir que uma infra-estrutura de rede pública, como por exemplo a Internet, seja utilizada como backbone para a comunicação segura entre pontos distintos.

Para os usuários que se comunicam através de uma VPN, é como se duas redes fisicamente separadas fossem logicamente uma única rede.

Esse tipo de VPN, que é transparente ao usuário, pode ser chamada de *gateway-to-gateway* VPN, ilustrada na Figura 2.1, onde o túnel VPN é iniciado e finalizado nos

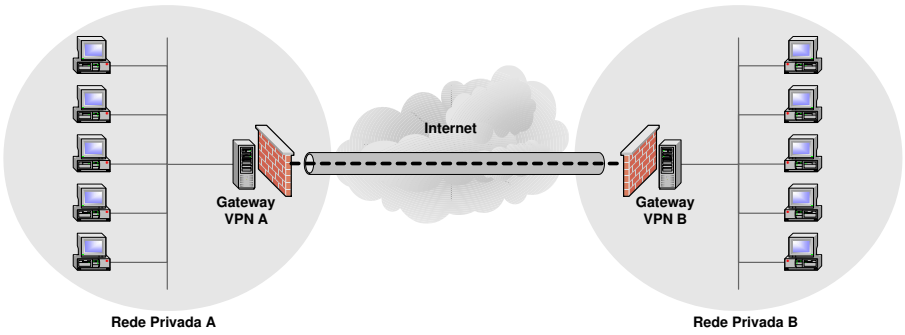


Figura 2.1: *Gateway-to-gateway* VPN

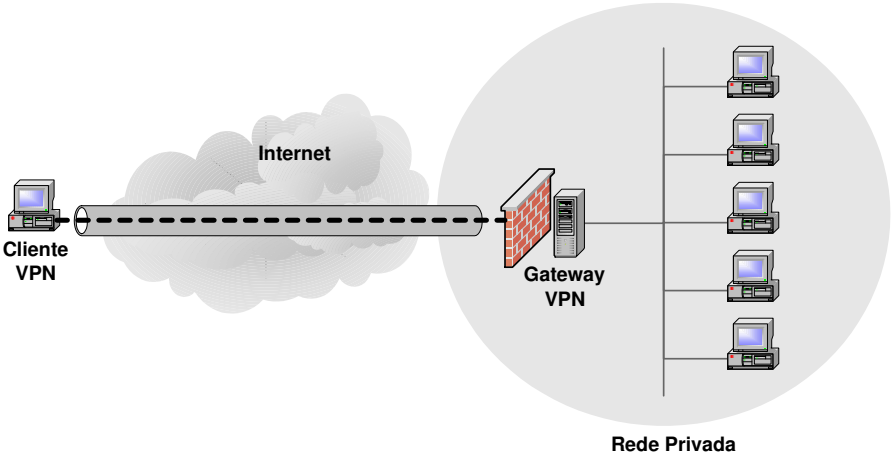


Figura 2.2: *Client-to-gateway* VPN

gateways das organizações. Dessa forma, é possível conectar matrizes, filiais e departamentos geograficamente dispersos, sem a necessidade de gastos com linhas dedicadas.

Outro tipo de VPN é a *client-to-gateway* VPN, onde o túnel é iniciado no próprio equipamento do usuário, como mostrado na Figura 2.2, através de um software cliente VPN.

Esses dois tipos de VPN podem ser utilizados para compor uma *Intranet* VPN, que conecta departamentos e filiais dentro de uma organização, ou uma *Extranet* VPN, que conecta a organização a parceiros estratégicos, clientes e fornecedores.

A *Intranet* VPN exige uma tecnologia de ponta para as conexões de alta velocidade presentes em LANs, além de alta confiabilidade, para assegurar a prioridade em aplicações de missão crítica. A facilidade de gerenciamento para acomodar mudanças com novos usuários, novas filiais e novas aplicações também é importante.

Já a *Extranet* VPN requer uma solução padrão para assegurar a interoperabilidade entre as várias soluções de parceiros, sendo que o controle de tráfego é importante para

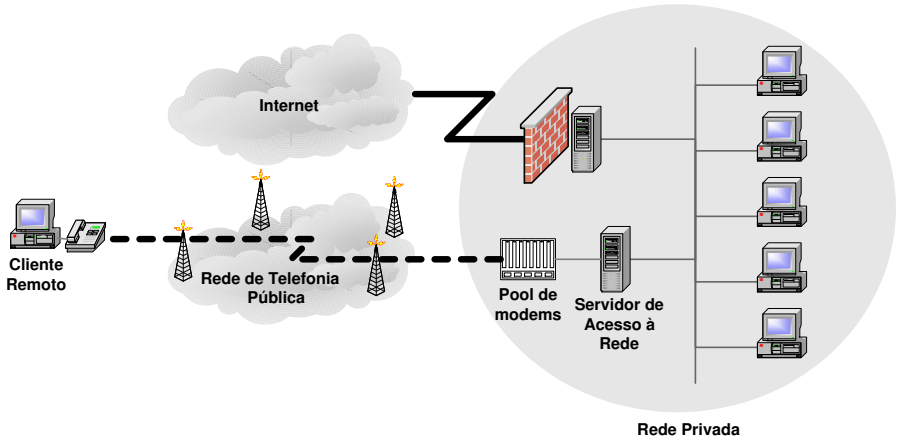


Figura 2.3: Acesso remoto tradicional

se evitar os gargalos e garantir a rápida resposta aos dados críticos.

Além da economia com as linhas dedicadas, a VPN também pode ser utilizada como solução alternativa aos acessos remotos tradicionais.

O acesso remoto tradicional, mostrado na Figura 2.3, pode ser tipicamente caracterizado por usuários dial-up acessando uma rede privada através de uma Rede de Telefonia Pública (*Public Switched Telephone Network* – PSTN), com a conexão dial-up terminando em um Servidor de Acesso à Rede (*Network Access Server* – NAS) dentro do domínio designado.

Uma solução alternativa baseada no uso de VPNs apresentaria, nesse caso, características híbridas entre uma *Intranet* VPN, ao fornecer conexão a funcionários em ambientes remotos, e uma *Extranet* VPN, disponibilizando alguns de seus serviços a fornecedores e parceiros estratégicos.

Essa solução, na qual o túnel VPN é iniciado no cliente, que se conecta a um Provedor de Acesso à Internet (*Internet Service Provider* – ISP), como ilustrado na Figura 2.4, substituindo os acessos remotos diretos, é conhecida como acesso remoto VPN. A manutenção dos componentes do acesso remoto tradicional, que incluem o pool de modems e as linhas telefônicas, pode ser considerada bem mais cara e também menos escalável do que uma solução VPN.

O acesso remoto VPN possui uma grande aplicabilidade em um ambiente cooperativo, onde os usuários remotos podem deixar de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet. Uma autenticação forte é um requisito importante neste cenário, já que os recursos da organização são acessados diretamente pelos usuários, e a segurança física é difícil de ser implementada em soluções remotas.

Assim, quando a VPN é utilizada, o serviço aparece para o usuário como se ele estivesse

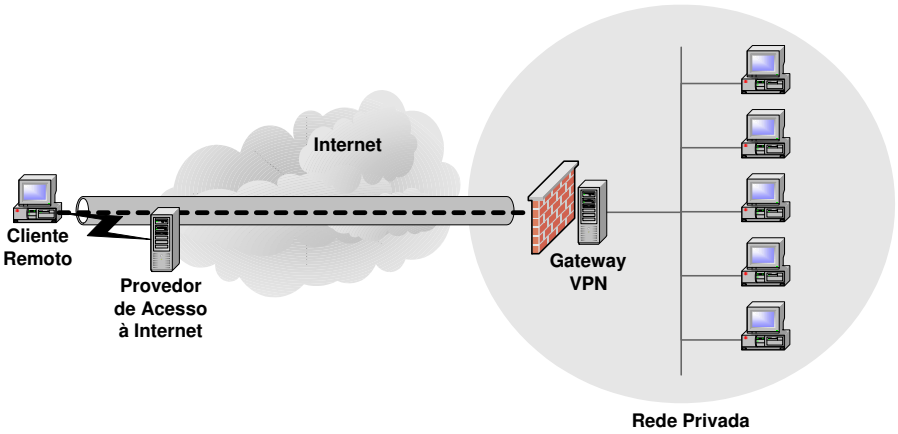


Figura 2.4: Acesso remoto VPN

conectado diretamente à rede privada, quando na realidade ele utiliza uma infra-estrutura pública.

A utilização da rede pública para a comunicação entre matriz, filiais e parceiros comerciais significa custos mais baixos e maior flexibilidade e escalabilidade com relação a usuários remotos e a mudanças nas conexões, se comparada com as conexões privadas, que possuem altos custos para mudanças em sua infra-estrutura.

De fato, a utilização da Internet facilita o gerenciamento das conexões, pois não é mais necessário criar um ponto de acesso privado para cada uma delas, e sim apenas um, para a Internet, aproveitando-se ainda da conectividade global, que é mais difícil de ser alcançada com o uso de conexões dedicadas. Esse conjunto de fatores facilita a interação entre as organizações, que podem assim buscar a evolução natural em seus processos de negócios.

2.2 Conceitos básicos

A fim de prover uma comunicação segura através de uma rede pública intermediária, as Redes Privadas Virtuais se fundamentam em dois conceitos básicos: a criptografia e o tunelamento.

A criptografia é utilizada para fornecer uma comunicação "privada", visando garantir a confidencialidade, a autenticidade e a integridade das conexões, e é a base para a segurança das soluções VPN.

Já o tunelamento é utilizado para o estabelecimento de uma comunicação "virtual" que utiliza uma infra-estrutura de rede intermediária como backbone, sendo responsável pelo encapsulamento, transmissão e desencapsulamento dos dados entre dois pontos distintos.

2.2.1 Criptografia

As Redes Privadas Virtuais permitem que uma rede pública, como por exemplo a Internet, seja utilizada como backbone para a comunicação entre pontos privados.

Apesar das inúmeras vantagens oferecidas por esta tecnologia, o uso de uma rede pública para a transmissão de dados privados pode trazer sérias implicações quanto à segurança dessas informações.

Dessa forma, é imprescindível que a VPN seja capaz de prover um conjunto de funcionalidades que garanta requisitos como:

- **Confidencialidade:** levando-se em conta que a VPN se baseia no uso de uma infra-estrutura de rede pública para prover conectividade entre pontos privados, a tarefa de interceptar uma seqüência de dados torna-se relativamente simples. Por isso é imprescindível que os dados que trafegam pela rede pública sejam protegidos de forma que, mesmo que sejam capturados, não possam ser entendidos, preservando assim a confidencialidade da comunicação.

- **Integridade:** além da possibilidade de interceptação dos dados que trafegam pela rede pública, existe também a possibilidade de que eles sejam modificados ao longo do caminho. Assim, é necessário garantir de alguma forma que quaisquer tentativas de adulteração nesses dados sejam detectadas, preservando dessa forma a garantia de integridade das informações.

- **Autenticidade:** além de proteger os dados de uma possível interceptação ou modificação não autorizadas, também é importante garantir que os dados recebidos realmente foram enviados pela entidade com a qual se pretendia estabelecer a comunicação. Da forma análoga, é importante garantir que os dados enviados realmente foram recebidos pela entidade com a qual se pretendia estabelecer a comunicação. Isso evita uma possível falsificação de identidade por parte de um usuário mal intencionado, garantindo a autenticidade das partes envolvidas.

Além desses requisitos básicos, é interessante que a tecnologia utilizada para o desenvolvimento de uma solução VPN ofereça mecanismos de segurança adicionais como, por exemplo, controle de acesso, restringindo o acesso de usuários não autorizados, auditoria, registrando eventos relevantes, além de outros mecanismos que reforcem a segurança da comunicação e das entidades envolvidas.

2.2.2 Tunelamento

Quando uma VPN é utilizada, o usuário tem a impressão de estar conectado diretamente à rede privada, quando na realidade ele utiliza uma infra-estrutura pública. Esta

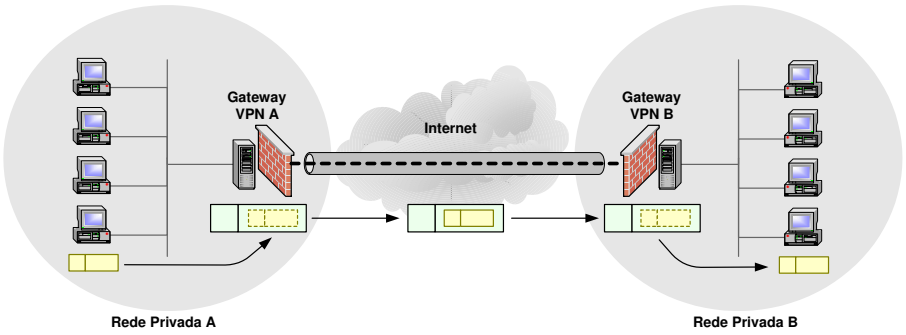


Figura 2.5: Tunelamento

"conexão virtual" se torna possível através do uso de técnicas de tunelamento.

O tunelamento é um mecanismo que permite a utilização de uma infra-estrutura de rede intermediária para a transferência de dados entre duas rede distintas. Neste caso, os dados transferidos podem ser pacotes do mesmo protocolo utilizado na rede intermediária, ou então de protocolos diferentes.

Ao invés de enviar o pacote da forma como ele foi gerado pelo nó original, o protocolo de tunelamento o encapsula utilizando um cabeçalho adicional, como mostrado na Figura 2.5. Esse novo cabeçalho provê informações de roteamento, de forma que esse pacote possa assim atravessar a rede intermediária. Os pacotes encapsulados são então roteados entre os extremos do túnel sobre uma rede intermediária qualquer.

O caminho lógico através do qual os pacotes encapsulados seguem através da rede intermediária é denominado túnel. Uma vez que esses pacotes alcançam seu destino na rede intermediária, eles são desencapsulados e encaminhados ao seu destino final.

O tunelamento, portanto, inclui todo o processo de encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento dos pacotes.

2.3 Protocolos

Uma VPN é formada pelo conjunto tunelamento, que permite o tráfego em uma rede pública, e criptografia, que visa garantir a segurança dessa conexão.

Existem diversos protocolos de comunicação capazes de prover o tunelamento necessário às VPNs, que diferem entre si na camada do modelo ISO/OSI onde atuam.

Alguns dos protocolos de tunelamento mais populares que atuam na camada de enlace, a camada 2 do modelo ISO/OSI, são o PPTP (*Point-to-Point Tunneling Protocol*) [Ham99], o L2F (*Layer 2 Forwarding*) [VLK98] e o L2TP (*Layer Two Tunneling Protocol*) [Tow99]. O IPSec (*Internet Protocol Security*) [KA98c], atual padrão do IETF (*Internet Engineering Task Force*) para o desenvolvimento de VPNs, atua na camada de rede, a

camada 3 do modelo ISO/OSI.

Existem também diferenças significativas entre esses protocolos no modo como a criptografia é utilizada. O L2TP, por exemplo, faz uso apenas de serviços de autenticação dos extremos do túnel, enquanto o PPTP e o IPSec podem fazer uso da autenticação, da integridade e da confidencialidade da comunicação.

A escolha de um protocolo adequado que atenda às necessidades de cada cenário de VPN constitui uma decisão fundamental para a segurança dos dados que trafegam pela rede pública.

2.4 Conclusão

As Redes Privadas Virtuais possuem uma importância fundamental para as organizações, principalmente em seu aspecto econômico, pois permitem que conexões dedicadas e estruturas de acesso remoto tradicionais, que possuem custos bastante elevados, sejam substituídas por conexões públicas, baseadas na Internet.

A utilização da Internet facilita também o gerenciamento de conexões, pois não é mais necessário criar um ponto de acesso privado para cada uma delas, e sim apenas um, para a Internet, tirando-se vantagem ainda da conectividade global, que é mais difícil de ser alcançada através de conexões dedicadas.

Um uso de VPNs que tem se tornado bastante popular é o chamado acesso remoto VPN. Desenvolvido como uma alternativa aos acessos remotos tradicionais, ele possui uma grande aplicabilidade em um ambiente cooperativo, onde os usuários remotos podem deixar de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet.

Para a realização dessa comunicação através de uma rede pública como a Internet, as VPNs se fundamentam em dois conceitos básicos, a criptografia e o tunelamento.

A criptografia visa garantir a segurança das informações que trafegam através da VPN, já o tunelamento oferece os mecanismos necessários para o transporte dessas informações sobre uma rede pública intermediária, utilizada como backbone para a comunicação.

Neste contexto, a escolha de um protocolo adequado que venha a suprir as necessidades de segurança e funcionalidade impostas pelo acesso remoto VPN constitui uma decisão fundamental para a viabilidade de uma solução VPN.

Capítulo 3

Análise dos Protocolos

Os conceitos que fundamentam a VPN são a criptografia e o tunelamento. A criptografia é utilizada para garantir a autenticidade, a confidencialidade e a integridade das conexões, e é a base para a segurança das soluções VPN. Já o tunelamento, é responsável pelo encapsulamento e transmissão dos dados, sobre uma rede pública, entre dois pontos distintos.

A carência de mecanismos capazes de proteger o acesso remoto VPN culminou na especificação de diferentes padrões. Em determinadas situações, é possível combinar soluções no intuito de obter o conjunto de serviços desejados.

Além disso, os diversos protocolos existentes diferem entre si na camada do modelo ISO/OSI onde atuam, ou no modo em que a criptografia é utilizada, o que influencia diretamente no nível de segurança do acesso remoto VPN.

A seguir serão apresentadas as características básicas e uma análise de segurança dos principais protocolos utilizados atualmente para acesso remoto VPN. A análise apresentada neste capítulo é uma extensão do trabalho apresentado no IV Simpósio sobre Segurança em Informática [dRdG02].

3.1 Point-to-Point Tunneling Protocol (PPTP)

O PPTP (*Point-to-Point Tunneling Protocol*) [Ham99] é um protocolo que foi originalmente desenvolvido por um grupo de empresas chamado PPTP Forum, constituído pela 3Com, Ascend Communications, Microsoft, ECI Telematics e US Robotics.

A idéia básica do PPTP era dividir as funções do acesso remoto de tal modo que indivíduos e empresas pudessem utilizar a infra-estrutura da Internet para prover uma conectividade segura entre clientes remotos e redes privadas.

O PPTP tem como finalidade principal prover um mecanismo para o tunelamento de tráfego PPP (*Point-to-Point Protocol*) [Sim96b] sobre redes IP.

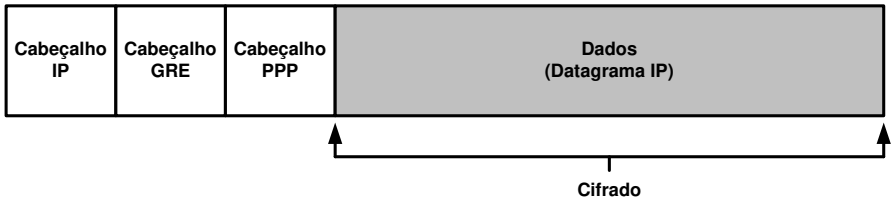


Figura 3.1: Encapsulamento de um datagrama IP feito pelo PPTP

Antes do envio de um datagrama IP, o PPTP cifra e encapsula este datagrama em um pacote PPP que, por sua vez, é encapsulado em um pacote GRE (*Generic Routing Encapsulation*) [Far00], como mostrado na Figura 3.1.

Da mesma forma que outros protocolos de segurança, o PPTP também requer a negociação de parâmetros antes de, efetivamente, proteger um tipo de tráfego entre duas entidades. Porém, o seu procedimento de negociação é feito sem qualquer proteção, permitindo que um atacante modifique parâmetros ou obtenha dados como o endereço IP dos extremos do túnel, nome e versão do software utilizado, nome do usuário e, em alguns casos, o hash criptográfico da senha do usuário [ZCC00].

Além disso, as mensagens do canal de controle PPTP são transmitidas sem qualquer forma de autenticação ou proteção de integridade, o que expõe esse canal de controle a um seqüestro de conexão (*connection hijacking*) [NdG02]. Também é possível gerar falsas mensagens de controle ou alterar essas mensagens em trânsito sem qualquer detecção.

Outra vulnerabilidade do PPTP é o fato do cliente só precisar se autenticar após a conclusão do processo de estabelecimento de parâmetros. Esta característica permite que atacantes façam com que um servidor inicie diversos processos de negociação falsos, o que pode resultar em negação de serviço (DoS) [NdG02] e até mesmo na total paralisação do servidor.

3.1.1 Considerações sobre o PPTP da Microsoft

Implementações específicas de um protocolo podem conter, além dos problemas de segurança detectados na própria especificação, falhas que podem comprometer o uso deste protocolo.

Em relação ao PPTP, a Microsoft possui uma implementação com extensões proprietárias incluída na maioria das versões do Microsoft Windows. Pelo fato deste sistema operacional ser amplamente utilizado e o seu suporte ao PPTP representar uma solução viável e de baixo custo para a configuração de VPNs, análises de segurança desta implementação do PPTP merecem atenção especial.

Uma primeira fragilidade do PPTP da Microsoft está em um dos formatos de arma-

zenamento e transmissão de hashes de senhas nas várias versões do Microsoft Windows, conhecido como LanMan. Senhas do Windows NT possuem 14 caracteres de extensão. Porém, quando armazenadas no formato LanMan, que é *case-insensitive*, todos os caracteres são convertidos para *uppercase*, diminuindo o número de possíveis hashes e, conseqüentemente, facilitando ataques de força-bruta. Porém, a maior vulnerabilidade do LanMan é a divisão da cadeia de 14 caracteres em duas de 7 caracteres. Hashes para cada uma das cadeias são gerados separadamente. Este procedimento reduz um ataque de força-bruta da senha ao esforço necessário para descobrir colisões para duas senhas curtas de 7 caracteres [Sen02].

Uma vez que os dados do processo de negociação de parâmetros do PPTP são transmitidos sem a proteção de qualquer serviço de confidencialidade, um atacante pode obter o hash da senha de um usuário armazenada no formato LanMan e, com base neste dado, descobrir a senha original. Deve-se ainda levar em consideração o fato de que muitos usuários escolhem senhas previsíveis e sujeitas a ataques de dicionário [Kle90], o que certamente facilita a violação de senhas representadas e transmitidas em LanMan.

Apesar do Windows NT possuir um novo formato para a manipulação de senhas, caso a compatibilidade com o LanMan esteja ativa, as senhas serão manipuladas utilizando este formato. Desta forma, o uso do protocolo PPTP certamente representa uma exposição perigosa da senha dos usuários de um ambiente Windows. Vale ressaltar que o ataque a hashes de 7 caracteres pode ser realizado através da utilização de computadores pessoais de baixo custo [Sch96].

Outra vulnerabilidade grave da implementação do PPTP em sistemas Windows está no tamanho e no processo de geração de chaves criptográficas para o serviço de cifragem. Dois modos de confidencialidade são oferecidos através do algoritmo RC4 [Sch96]: um que utiliza chaves de 40 bits e outro com chaves de 128 bits. No primeiro caso, além da utilização de chaves pequenas, altamente suscetíveis a ataques de força-bruta, as chaves geradas são baseadas nas senhas dos usuários. Em outras palavras, várias sessões de um mesmo usuário irão utilizar a mesma chave, a não ser que este usuário altere o valor de sua senha. Este fato agrava-se ainda mais se o atacante obtiver a senha de um usuário no formato LanMan.

No segundo modo de cifragem, que utiliza chaves de 128 bits, consideradas atualmente seguras, o valor gerado para uma chave é baseado, novamente, na senha do usuário, porém combinada com um número aleatório específico para cada sessão. Apesar deste procedimento ser mais seguro que o anterior, o uso constante da senha do usuário diminui consideravelmente o número de tentativas que podem compor um ataque [Sen02].

O uso de ferramentas que automatizam o ataque a senhas pode obter sucesso em alguns minutos, considerando o uso de senhas comuns, fragilizando ainda mais o processo de geração de chaves criptográficas baseadas nas senhas dos usuários. No caso de um ataque

de força bruta, algumas ferramentas podem obter sucesso num prazo de no máximo 250 horas, caso a senha seja composta somente por caracteres alfabéticos [Sen02].

O conjunto de vulnerabilidades do PPTP implementado em sistemas Windows fez com que a própria Microsoft recomendasse a desabilitação do formato LanMan em cenários onde é possível o uso de outras opções. Os resultados de análises de segurança detalhadas sobre a implementação Microsoft do protocolo PPTP podem ser encontrados em [SM98], [SMW99].

3.2 Layer Two Tunneling Protocol (L2TP)

O *Layer 2 Tunneling Protocol* (L2TP) [Tow99] foi desenvolvido com base no *Layer 2 Forwarding* (L2F) [VLK98] e no *Point-to-Point Tunneling Protocol* (PPTP) [Ham99], e tem por principal objetivo, assim como o PPTP, o encapsulamento de pacotes PPP.

Uma das diferenças entre o L2TP e o PPTP está no protocolo utilizado na camada inferior do modelo ISO/OSI. Enquanto o PPTP deve ser sempre utilizado acima do IP, o L2TP pode ser utilizado sobre redes IP, X.25, Frame Relay ou ATM (*Asynchronous Transfer Mode*).

Sob o ponto de vista da segurança da comunicação, dado que o L2TP realiza o encapsulamento de pacotes PPP, ele pode então fazer uso dos mecanismos de autenticação PPP, bem como do Protocolo de Controle de Cifragem (*Encryption Control Protocol* – ECP) [Mey96] e do Protocolo de Controle de Compressão (*Compression Control Protocol* – CCP) [Ran96] utilizados pelo PPP.

O L2TP provê também suporte à autenticação do túnel, permitindo que ambos os extremos do túnel sejam autenticados.

Contudo, não existem mecanismos robustos de proteção do túnel L2TP definidos, o que expõe tanto os pacotes de dados quanto os pacotes de controle deste protocolo a algumas formas de ataque.

Dentre as vulnerabilidades possíveis podemos destacar: a obtenção da identidade do usuário através da observação dos pacotes; a modificação dos pacotes de dados e controle; o seqüestro do túnel L2TP ou da conexão PPP dentro do túnel; ataques de negação de serviço contra a conexão PPP ou o túnel L2TP; a interrupção da negociação PPP ECP com o intuito de remover a proteção de confidencialidade; e a interrupção ou o enfraquecimento do processo de autenticação PPP sendo possível até mesmo conseguir acesso à senha do usuário [Pat01a].

Diante de todos os problemas de segurança apresentados pelo protocolo L2TP, seu uso em cenários onde existe uma rede não-confiável, como a Internet, entre os extremos de um túnel, deve sempre ser combinado com outros protocolos capazes de suprir a sua ausência de serviços de segurança.

Um conjunto de propostas tem sido desenvolvido para conciliar o uso do L2TP com o IPSec [Pat01a], [Sri00].

Na Seção 3.4 são discutidos os aspectos referentes à utilização do L2TP sobre o IPSec em maiores detalhes.

3.3 IP Security (IPSec)

O IPSec (*Internet Protocol Security*) [KA98c] é uma arquitetura definida pelo IETF (*Internet Engineering Task Force*), cujo principal objetivo é oferecer mecanismos de segurança a pacotes IP. Tais serviços são providos através de dois cabeçalhos de extensão, o AH (*Authentication Header*) [KA98a] e o ESP (*Encapsulation Security Payload*) [KA98b], e através do uso de protocolos e procedimentos para gerência de chaves criptográficas, como o IKE (*Internet Key Exchange*) [HC98].

O AH foi desenvolvido para garantir a autenticidade e a integridade dos pacotes IP. Sua utilização oferece proteção contra modificações nos campos de valor fixo do pacote IP, proteção contra spoofing [NdG02], e opcionalmente, proteção contra ataques de replay [NdG02].

Já o ESP provê a cifragem dos dados, para garantir que somente o destinatário possa ler o payload do pacote IP. Opcionalmente, também pode garantir a autenticidade e a integridade do pacote, e proteção contra ataques de replay.

Os dois cabeçalhos podem ser utilizados separadamente ou podem ser combinados para prover as características de segurança desejadas para o tráfego IP.

A principal diferença entre os serviços de autenticação e integridade providos pelo AH e pelo ESP está na abrangência da proteção. O AH protege todos os campos de um pacote, excetuando-se aqueles cujos valores são alterados em trânsito. Quando oferecidos pelo ESP, esses serviços abrangem somente o próprio cabeçalho do ESP e a porção de dados do pacote.

3.3.1 Algoritmos criptográficos

Diversos algoritmos criptográficos podem ser utilizados pelo AH e ESP, porém existe um conjunto mínimo cuja implementação é obrigatória. São eles: HMAC-MD5-96 e HMAC-SHA-1-96 para os serviços de autenticação e integridade do AH e ESP; DES-CBC para a confidencialidade provida pelo ESP; e, algoritmos nulos de autenticação e confidencialidade utilizados pelo ESP quando um dos seus serviços não é requisitado. No entanto, este conjunto obrigatório não é suficiente para prover segurança de forma adequada a todos os tipos de informação [SAdG02].

Estudos têm mostrado que particularidades do MD5 permitem acelerar o processo para gerar mensagens que produzam o mesmo hash, utilizando máquinas de baixo custo [Sch96].

Em relação ao DES, o tamanho de chave utilizada, 56 bits, é atualmente vulnerável a ataques de força-bruta tornando-o inadequado para preservar informações cujo sigilo é de extrema significância [Bel97].

Sendo assim, a implementação de outros algoritmos mais capazes seria de extrema importância, porém se algoritmos mais seguros não estão padronizados, nem todas as implementações os conterão.

3.3.2 Associações de Segurança (SA)

Para que duas entidades consigam enviar e receber pacotes utilizando os serviços do IPSec é necessário o estabelecimento de Associações de Segurança (Security Association – SA), que especificam os algoritmos a serem utilizados, as chaves criptográficas, os tempos de vida destas chaves, entre outros parâmetros.

Existem duas formas de estabelecimento de associações de segurança: estática e dinâmica. No primeiro, os parâmetros são inseridos manualmente em ambos os extremos da comunicação. No segundo, os parâmetros são negociados por protocolos como o IKE, sem a intervenção do administrador.

A escalabilidade do IPSec está relacionada ao estabelecimento dinâmico de SAs que devem ser definidas por conexão ou, no máximo, por usuário, para prover maior segurança. Abusar intencionalmente do mecanismo de estabelecimento de SAs pode constituir diversos ataques de DoS [NdG02].

Especificado pelo IETF como um componente adicional ao IPSec, o IKE é o protocolo responsável pelo estabelecimento e manutenção dinâmica de associações de segurança. Fundamentalmente o IKE é baseado nos protocolos OAKLEY [Orm98] e SKEME [Kra96], que provêem mecanismos para a definição e a troca de chaves criptográficas, e ISAKMP [MMS98], um arcabouço que define estruturas e procedimentos gerais para a criação, deleção, modificação e negociação de SAs.

SAD e SPD

O SAD (*Security Association Database*) [KA98c] é um componente do IPSec utilizado para armazenar as SAs ativas de uma máquina num dado momento. Em outras palavras, toda SA estabelecida deve conter uma entrada inserida pelo administrador do sistema ou pelo protocolo IKE nesta base de dados. Porém, antes de enviar pacotes, o IPSec não consulta as SAs do SAD diretamente para a inclusão dos cabeçalhos de segurança.

SAs são instâncias resultantes das restrições de proteção impostas por regras que formam a política de segurança local armazenadas em uma estrutura denominada SPD (*Security Policy Database*) [KA98c].

Funcionamento básico

O processo de estabelecimento de associações de segurança é composto por duas fases distintas. Na Fase 1 do IKE, uma SA denominada ISAKMP SA (*ISAKMP Security Association*) é definida para proteger todo o tráfego subseqüente do protocolo IKE entre duas máquinas.

A ISAKMP SA pode ser criada através de três métodos que se diferenciam pela quantidade e tipos de mensagens trocadas entre o *initiator*, máquina que dá início ao processo de estabelecimento de uma SA, e o *responder*, máquina à qual a solicitação do *initiator* destina-se: o *Main Mode*, mais seguro, contendo seis mensagens; o *Aggressive Mode*, menos seguro e contendo somente três mensagens; e o *Base Mode*, que utiliza quatro mensagens e procura manter-se como um meio termo entre a segurança do primeiro modo e a eficiência do segundo. O *Base Mode* foi criado após a especificação original do IPSec e, portanto, muitas plataformas ainda não o contemplam [Fra01].

Dentre as incumbências da ISAKMP SA estão a geração de um segredo compartilhado utilizado na derivação das chaves criptográficas para os algoritmos de proteção desta SA e a autenticação de ambas as máquinas envolvidas na comunicação. Para realizar este último procedimento, a especificação do IKE oferece quatro métodos: o segredo pré-compartilhado, onde o valor que será derivado para a criação das chaves criptográficas é inserido manualmente pelo administrador; duas formas de autenticação com criptografia de chaves públicas; e assinatura digital, onde são requeridas operações baseadas no uso das chaves privada e pública que devem estar associadas às máquinas. No primeiro método, a verificação de identidade é baseada somente no valor do segredo pré-compartilhado. Desta forma, sua obtenção é suficiente para falsificar uma negociação. Além disso, não há, neste método, um mecanismo definido para a substituição de antigos valores por novos, limitando-o a ambientes pequenos e pouco escaláveis. Os outros métodos contemplam a interação com entidades confiáveis para a distribuição de chaves públicas através da estruturação, por exemplo, de uma Infra-estrutura de Chaves Públicas (ICP) [AL99].

Definida a ISAKMP SA e sob sua proteção, inicia-se a Fase 2 do IKE, onde as SAs específicas do IPSec, denominadas IPSec SAs (*IPSec Security Associations*), são estabelecidas entre o *initiator* e o *responder* através de um único método denominado *Quick Mode*, composto por três mensagens. Cada IPSec SA é gerada a partir da análise das regras que compõem a política de segurança armazenada no SPD com o objetivo de proteger uma determinada espécie de tráfego IP. Em outras palavras, no momento em que um determinado pacote é filtrado por alguma regra e pelo menos uma dentre as SAs ne-

cessárias para prover os serviços requeridos não está presente no SAD, o IKE é acionado para estabelecer a(s) IPSec SA(s) restantes. Quando um pacote deve ser submetido à proteção de mais de uma SA e duas ou mais ainda não estão estabelecidas, uma única negociação de *Quick Mode* pode ser utilizada para a criação das várias SAs. Este conjunto de SAs, destinado à proteção de um tráfego em comum, é denominado na especificação por *SA bundle* [Fra01].

3.3.3 Modo transporte e modo túnel

Ambos os cabeçalhos, AH e ESP, possuem dois modos de operação: transporte e túnel.

No modo transporte, os cabeçalhos de segurança utilizados por um pacote são inseridos após o cabeçalho IP. Este modo, em geral, é utilizado para proteção fim-a-fim da comunicação entre duas máquinas e representa uma solução adequada para auxiliar na segurança de pacotes em redes locais.

O modo túnel tem seu uso recomendado na proteção do tráfego entre uma máquina e um gateway. Antes de ser enviado, o pacote original é inserido completamente na porção de dados de um novo pacote que contém os cabeçalhos de segurança e cujos endereços correspondem aos extremos do túnel.

No modo transporte, os cabeçalhos de segurança provêem proteção primária para os protocolos das camadas superiores. No modo túnel, os cabeçalhos protegem o pacote IP encapsulado, provendo proteção para todos os campos do cabeçalho IP original.

3.3.4 Solução IPSec para o acesso remoto VPN

Uma solução bastante utilizada atualmente para o acesso remoto VPN é o uso do IPSec em modo túnel.

Nesse cenário, o túnel IPSec é estabelecido entre o cliente remoto e o gateway VPN da organização, constituindo um canal seguro para o tráfego dos dados sobre a rede pública intermediária.

Todo o tráfego IP é encapsulado pelo IPSec, sendo o pacote IP original transmitido através do túnel, tirando-se proveito de todos os serviços de segurança oferecidos pelo IPSec.

A Figura 3.2 mostra o uso do IPSec em modo túnel utilizando apenas os serviços do protocolo AH, garantindo a integridade e a autenticidade tanto do pacote IP original, quanto do pacote IPSec utilizado para prover o tunelamento.

Na Figura 3.3 é mostrado o modo túnel do IPSec utilizando os serviços do cabeçalho ESP, provendo confidencialidade a todo o pacote IP original, e integridade e autenticação ao pacote IP original e parte do pacote IPSec utilizado para prover o tunelamento.

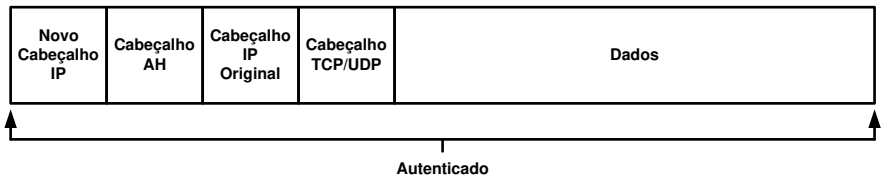


Figura 3.2: IPSec em modo túnel utilizando os serviços do cabeçalho AH

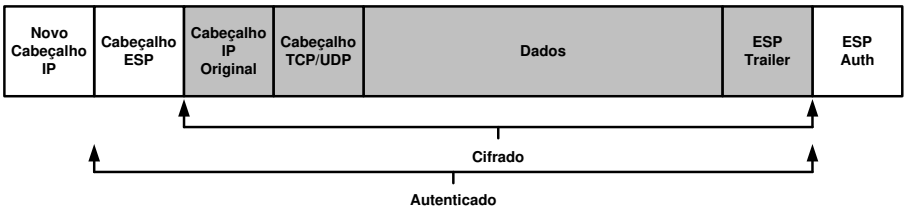


Figura 3.3: IPSec em modo túnel utilizando os serviços do cabeçalho ESP

No entanto, é importante notar que o uso do IPSec somente com os serviços de autenticação e integridade, ou somente com o serviço de confidencialidade, pode causar uma falsa sensação de segurança na comunicação, tornando o túnel IPSec vulnerável a alguns tipos de ataques. Uma análise detalhada dessas vulnerabilidades pode ser encontrada em [Bel96].

Apesar dos problemas apresentados constituírem uma ameaça à segurança do túnel IPSec, quando utilizado de forma adequada esse protocolo provê um excelente nível de segurança para a comunicação, sendo uma das principais tecnologias atualmente disponíveis para a implementação de VPNs.

Contudo, alguns aspectos relacionados à utilização do IPSec para o acesso remoto VPN ainda carecem de padronização. O modo túnel do IPSec não provê suporte à atribuição e configuração de endereços IP, o que se faz necessário no caso do acesso remoto VPN, já que um dos extremos do túnel é uma máquina remota que não possui endereço IP fixo e que após o estabelecimento do túnel precisa estar associado a um endereço IP da rede interna. Além disso, muitos dos esquemas de autenticação existentes, comumente usados para autenticação de usuários, são de natureza assimétrica, e não são suportados pelo IKE (*Internet Key Exchange*), utilizado pelo IPSec. Apesar do IKE prover um suporte poderoso para a autenticação de máquina, ele apresenta somente um suporte limitado para formas de autenticação de usuário e não provê suporte para autenticação assimétrica de usuário.

Outra característica desejável ao IPSec seria o suporte à múltiplos protocolos, uma vez que esse protocolo só é capaz de transportar pacotes IP em seu modo túnel.

Todos esses ítens são requisitos importantes para o acesso remoto VPN. Existem alguns

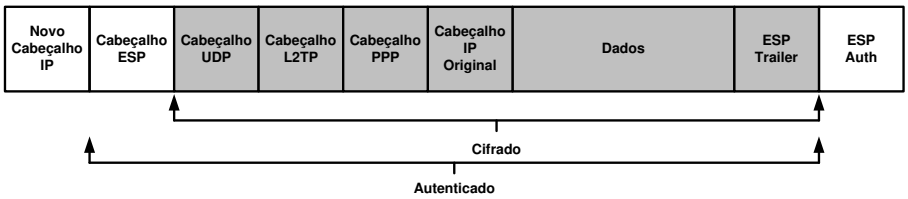


Figura 3.4: Encapsulamento de um pacote IP feito pelo L2TP sob a proteção do cabeçalho ESP do IPSec

trabalhos em andamento, no sentido de criar uma solução padrão para os problemas envolvendo o uso do IPSec em um ambiente de acesso remoto, que estão sendo discutidos atualmente no IPSec Working Group, grupo do IETF (*Internet Engineering Task Force*) que desenvolve mecanismos de segurança para o protocolo IP [Gle00].

3.4 L2TP sobre IPSec (L2TP/IPSec)

Com o intuito de solucionar os problemas de segurança apresentados pelo L2TP, diversas propostas têm sido desenvolvidas, visando suprir suas deficiências através dos serviços de segurança oferecidos pelo IPSec.

A utilização do L2TP sobre o IPSec apresenta vantagens significativas para o acesso remoto VPN, pois a comunicação se beneficia dos serviços de confidencialidade, autenticidade, integridade e proteção contra replay, providos pelo IPSec, e ao mesmo tempo usufrui da autenticação de usuários, configuração e atribuição de endereços IP nos extremos do túnel, e suporte a múltiplos protocolos providos pelo túnel L2TP.

Quando executado sobre o IP, o L2TP é transportado através de datagramas UDP. Desta forma, a aplicação da proteção do IPSec sobre o L2TP pode basear-se simplesmente no uso de seletores que filtram o tráfego L2TP [Sen02]. É importante notar que neste caso o IPSec é utilizado em modo transporte, ou seja, não existe a criação de um túnel IPSec.

A Figura 3.4 exibe o encapsulamento de um pacote IP feito pelo L2TP sendo utilizado sobre o IPSec, protegido somente pelo ESP.

Tal procedimento no entanto implica em um certo custo. Há um overhead considerável na pilha de protocolos, particularmente porque o IPSec também é necessário por propósitos de segurança, dado que o cliente remoto pode estar conectado através de uma conexão discada de baixa largura de banda.

O overhead é causado pela adição de vários cabeçalhos extra no envio de dados e protocolos de controle necessários ao controle da conexão, e pode trazer alguns problemas, como por exemplo, a fragmentação de pacotes IP.

Como conseqüência da fragmentação dos pacotes, pode-se ter uma queda significativa no desempenho, podendo causar também perda de pacotes e um aumento considerável no consumo de memória no gateway VPN, para realizar a remontagem dos pacotes fragmentados, o que poderia inviabilizar esta solução. Além disso, algumas formas de ataque se aproveitavam da fragmentação de pacotes IP para burlar os firewalls [NdG02].

Usando L2TP para o tunelamento, protegido pelo IPSec, teríamos uma aplicação web, por exemplo, rodando sobre a seguinte pilha de protocolos:

HTTP/TCP/IP/PPP/L2TP/UDP/ESP/IP

Enquanto que utilizando apenas o IPSec em modo túnel reduziríamos consideravelmente o overhead, usando a seguinte pilha de protocolos:

HTTP/TCP/IP/ESP/IP

Uma área de potenciais problemas também, seria o uso do PPP, devido ao fato que as características de uma camada de enlace implementada através de um túnel L2TP sobre um backbone IP são completamente diferentes de uma camada de enlace rodando sobre uma linha serial, como discutido na própria especificação do L2TP [Tow99]. Parâmetros da conexão PPP mal escolhidos, por exemplo, podem levar a freqüentes resets e timeouts, particularmente se a compressão estiver sendo usada. Isso ocorre porque o túnel L2TP pode desordenar ou até mesmo perder pacotes, o que normalmente não ocorre em linhas seriais. A taxa geral de pacotes perdidos pode ser significativa também devido ao congestionamento da rede [Gle00].

Outro problema na integração do L2TP com o IPSec é a impossibilidade do segundo levar em consideração os valores dos campos de pacotes IP encapsulados pelo primeiro.

Outros procedimentos de interação entre os dois protocolos têm sido sugeridos no intuito de prover o desenvolvimento de soluções para aspectos ainda não padronizados do IPSec. Apesar destas soluções serem práticas e de baixo custo, pelo fato do protocolo L2TP já ser um padrão definido, existem críticas severas quanto ao uso de um protocolo que não foi projetado para ambientes seguros na execução de procedimentos vitais para um protocolo de segurança como o IPSec [Fra01].

3.5 Conclusão

A carência de mecanismos capazes de proteger o acesso remoto VPN culminou na especificação de diferentes padrões.

Com a análise dos principais protocolos utilizados para acesso remoto VPN, foi possível observar alguns dos pontos positivos e negativos de cada tecnologia, facilitando assim a opção por uma tecnologia mais adequada às necessidades de cada cenário.

O PPTP, por apresentar uma estrutura bastante simples, pode ser uma solução adequada em situações onde não é exigida uma solução robusta de segurança.

O L2TP não possui mecanismos de proteção do túnel definidos, por isso seu uso em cenários onde existe uma rede não-confiável, como a Internet, entre os extremos de um túnel, deve sempre ser combinado com outros protocolos capazes de suprir a sua ausência de serviços de segurança.

A utilização do L2TP sobre o IPSec é uma alternativa que apresenta muitas das funcionalidades necessárias para o acesso remoto VPN.

O uso da confidencialidade, autenticidade, integridade e proteção contra replay, providos pelo IPSec, unidos a autenticação de usuários, configuração e atribuição de endereços IP nos extremos do túnel, e suporte a múltiplos protocolos providos pelo túnel L2TP, são algumas das vantagens apresentadas por essa solução. Porém, causa um overhead considerável na pilha de protocolos utilizada, o que se reflete em um forte impacto em ambientes reais de acesso remoto. Como conseqüência disso, podem surgir problemas de segurança relacionados à fragmentação de pacotes IP causada, além do impacto direto no desempenho, na disponibilidade e na viabilidade da solução VPN.

O IPSec em modo túnel é uma solução que vem sendo padronizada e que atende perfeitamente aos requisitos de segurança das soluções VPN, e por isso tem se mostrado a solução mais adequada ao acesso remoto VPN. No entanto, ainda carece de padronizações em alguns aspectos de funcionalidade e interoperabilidade do acesso remoto VPN dependendo do término de trabalhos em andamento para a completa viabilidade da solução. Tais aspectos e suas possíveis soluções serão discutidos em maiores detalhes no decorrer deste trabalho.

Capítulo 4

Cenários de Acesso Remoto

O IPSec tem se mostrado uma alternativa interessante para o acesso remoto VPN. Contudo, existem vários cenários possíveis de acesso remoto, que apesar de possuírem requisitos bastante específicos, na maioria dos casos, possuem muitos pontos em comum. Um profundo entendimento desses requisitos é necessário para que se possa avaliar efetivamente a conveniência de um conjunto de mecanismos para qualquer cenário particular de acesso remoto.

Em virtude da existência de algumas particularidades no uso do IPSec em um ambiente de acesso remoto, o IETF criou o *IP Security Remote Access Working Group* (IPSRA). Esse novo grupo de trabalho do IETF é responsável pela identificação e padronização de alguns mecanismos ainda inexistentes no IPSec, que permitam atender a essas particularidades do acesso remoto.

Neste capítulo, baseado nas especificações do *IPSRA Working Group* [KR03a], serão apresentados alguns dos cenários mais comuns de acesso remoto VPN utilizando IPSec, procurando identificar e explorar os requisitos de cada um, a fim de obter um conjunto geral de requisitos que seja comum à maioria dos casos.

4.1 Visão Geral

De forma geral, todos os cenários de acesso remoto seguro têm uma aparência de alto nível semelhante à mostrada na Figura 4.1.

Em todos os casos, um cliente remoto deseja acessar recursos de uma rede privada através de um Gateway VPN, que é uma máquina com suporte ao IPSec, e em alguns casos pode também desejar prover a outros sistemas acesso seguro aos próprios recursos do cliente. Existem diversos detalhes que podem variar, de acordo com o cenário em particular. Por exemplo, o cliente pode estar localizado dentro de outra rede corporativa, ou conectado a um provedor de acesso à Internet através de uma conexão discada ou DSL.

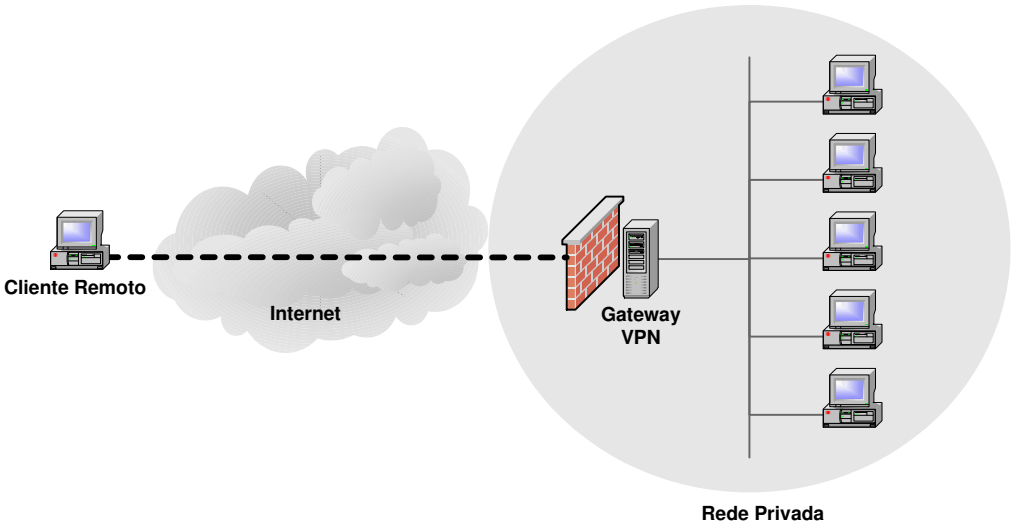


Figura 4.1: Cenário típico de Acesso Remoto Seguro

Podem existir diversas máquinas intermediárias entre o cliente remoto e o Gateway VPN, mas no final das contas, todas essas configurações podem ser vistas em alto nível como algo equivalente.

Em geral, existem várias categorias básicas de requisitos relevantes para os cenários de acesso remoto seguro. Dentre os principais requisitos podemos destacar: (i) a autenticação dos extremos da comunicação, (ii) a configuração do sistema remoto, (iii) a configuração das políticas de segurança, (iv) o registro de eventos e (v) a passagem por intermediários.

Autenticação dos extremos da comunicação significa verificar as identidades dos participantes da comunicação, tanto do cliente quanto do gateway VPN. Configuração do sistema remoto significa ajustar os parâmetros necessários de configuração de rede do sistema cliente. Configuração das políticas de segurança remete à configuração das políticas de acesso em ambos, gateway VPN e cliente remoto. Registro de eventos engloba a geração e coleta de informações sobre o estado das conexões que podem ser necessárias para propósitos de manutenção da segurança e integridade globais das redes conectadas. Passagem por intermediários refere-se à capacidade de passar tráfego seguro através de intermediários, alguns dos quais podem modificar os pacotes de alguma maneira. Tais intermediários incluem os dispositivos de firewall e NAT. Essas várias categorias serão tratadas em mais detalhes a seguir.

4.1.1 Autenticação dos extremos da comunicação

Em primeiro lugar, é importante diferenciar a autenticação da origem dos dados da autenticação do usuário final. Autenticar a origem dos dados no contexto do IPSec significa

prover garantia de que um pacote se originou em um ponto específico da comunicação, tipicamente um usuário, máquina ou aplicação. O IPSec oferece mecanismos para tal através dos cabeçalhos AH ou ESP. Autenticação do usuário final dentro do contexto do IPSec consiste em prover garantias de que o usuário final é realmente quem diz ser. O IPSec oferece mecanismos para isso atualmente como parte do IKE (*Internet Key Exchange*)[HC98].

Apesar desses dois tipos de autenticação se diferirem, eles não estão totalmente desvinculados. Na realidade, a autenticação da origem dos dados confia na autenticação dos extremos da comunicação, porque é possível inserir pacotes com um endereço IP particular na Internet de qualquer local. Em muitos casos não se pode ter garantias de que um pacote se originou em uma máquina em particular, ou até mesmo se ele se originou na rede onde aquela máquina se encontra. Para solucionar isto, deve-se autenticar primeiramente aquele ponto em particular de alguma maneira, e então associar a informação de endereço (por exemplo endereço IP, protocolo ou porta) a este ponto em uma relação de confiança estabelecida pelo processo de autenticação.

No contexto do acesso remoto, a entidade autenticada pode ser uma máquina, um usuário (aplicação) ou ambos. Os métodos de autenticação atualmente suportados pelo IPSec variam de segredos pré-compartilhados a vários esquemas de assinatura e cifragem empregando chaves privadas e seus certificados de chaves públicas correspondentes. Esses mecanismos podem ser utilizados para autenticar somente o usuário final, somente a máquina, ou ambos, o usuário final e a máquina.

Autenticação no nível de máquina

Em casos onde nenhuma entrada do usuário é exigida para que uma credencial de autenticação seja utilizada, a entidade autenticada será primariamente a máquina na qual a credencial está armazenada e o nível de garantia desta autenticação está diretamente relacionado a quão segura a credencial de máquina é mantida durante seu armazenamento e uso. Isto é, um segredo compartilhado ou uma chave privada correspondente a um certificado de chave pública podem estar armazenados dentro da máquina ou podem estar contidos em outro dispositivo que é seguramente acessível pela máquina, como por exemplo, um *smartcard*. Se o conhecimento necessário para o uso de tal credencial de autenticação está totalmente contido dentro da máquina em questão, ou seja, nenhuma entrada do usuário é necessária, então é difícil garantir que o uso de tais credenciais não esteja autenticando qualquer coisa diferente da máquina em questão.

Em alguns casos, pode-se exigir que um usuário satisfaça certos critérios antes de ter acesso às credenciais armazenadas. Em tais casos, o nível de autenticação do usuário é algo difícil de se avaliar. Se existe um controle de acesso suficientemente forte no sistema onde a credencial reside, então pode haver uma ligação forte entre o usuário do sistema e a

credencial. Porém, no momento em que a credencial é apresentada ao servidor, o próprio servidor não possui tal garantia. O servidor pode ter algum nível de garantia de que um dispositivo em particular (aquele onde a credencial reside) é aquele do qual a tentativa de acesso está sendo realizada, mas não há nenhuma garantia explícita relacionada à identidade do usuário do sistema. Para que o servidor possa ter alguma garantia adicional em relação à identidade do usuário, uma credencial adicional de usuário de algum tipo deve ser exigida.

Autenticação em nível de usuário

Em alguns casos, o usuário pode possuir um token de autenticação, que pode ser uma chave pré-compartilhada, uma chave privada, uma senha, ou algo do gênero, e pode fornecer este token ou algo derivado do mesmo quando a autenticação é necessária. Se este token ou sua derivação é entregue diretamente ao outro extremo do túnel sem ser modificado pelo sistema cliente, e se o sistema cliente não provê nenhuma credencial adicional de si próprio, então somente o usuário está sendo autenticado. Ou seja, enquanto pode haver alguma garantia sobre o usuário que está originando pacotes, não há nenhuma garantia sobre a máquina em particular da qual o usuário está realizando o acesso.

Autenticação combinada de usuário/máquina

Para autenticar ambos, o usuário e o sistema, alguma forma de entrada de usuário é necessária em adição à credencial que é armazenada de forma segura no dispositivo. Em alguns casos, tal entrada de usuário pode ser usada para complementar a credencial armazenada no dispositivo (por exemplo, uma chave privada cifrada com uma senha), enquanto que em outros casos a entrada do usuário é fornecida independentemente da credencial armazenada. No caso onde uma senha é aplicada à credencial antes de seu uso, o nível de garantia derivado da aplicação bem sucedida da credencial varia de acordo com o ponto de vista.

Da perspectiva de um sistema consistindo de usuário, cliente, servidor e uma coleção de proteções de sistema e procedimentos de segurança, pode-se dizer que o usuário foi autenticado em um nível que depende da resistência dos procedimentos de segurança e das proteções do sistema que estão instalados. Porém, do ponto de vista do servidor, há pouca garantia em relação à identidade do usuário. Dessa forma, esquemas que exigem que credenciais armazenadas sejam modificadas pela entrada do usuário antes de seu uso só provêem autenticação no nível de usuário dentro do contexto de grandes sistemas, e assim, o nível de garantia derivado é diretamente proporcional ao atributo de segurança mais fraco do sistema inteiro.

Ao considerar o acesso remoto de uma perspectiva geral, suposições relacionadas ao

sistema global são responsáveis por provas incorretas. Isto porque o servidor e o cliente podem não estar dentro do mesmo domínio de controle. Cenário de redes externas (*extranets*) são um bom exemplo disto. Conseqüentemente, os mecanismos de autenticação de usuário/máquina comumente desejáveis neste contexto são aqueles que provêem um alto nível de garantia para ambos, servidor e cliente, independentemente da extensão do sistema ao qual o usuário, o cliente e o servidor fazem parte.

Autenticação no acesso remoto

No caso geral de acesso remoto, os requisitos de autenticação são tipicamente assimétricos. Do ponto de vista do cliente, é importante garantir que o servidor no outro extremo da comunicação é realmente quem diz ser, e não algum sistema se fazendo passar pelo gateway VPN. Assim, o cliente exige autenticação no nível de máquina por parte do servidor. Isto pode ser diretamente obtido através dos mecanismos oferecidos pelo IKE no IPSec. Além disto, este tipo de autenticação tende a persistir com o tempo, ainda que a duração dessa persistência dependa do mecanismo escolhido.

Enquanto uma autenticação no nível de máquina por parte do servidor é suficiente, o mesmo não acontece para o cliente. No caso da autenticação do cliente é importante saber se a entidade no outro extremo da conexão é uma pessoa com acesso autorizado aos recursos da rede privada, e não alguém que de alguma forma teve acesso a um sistema autorizado, ou um cavalo de tróia (*Trojan Horse*) instalado no sistema do usuário, ou alguma outra entidade não autorizada. A autenticação do usuário apresenta diferentes requisitos em relação à autenticação da máquina do usuário, sendo necessária alguma forma de entrada do usuário, devendo a autenticação ser periodicamente renovada.

Em situações onde um alto nível de segurança física não existe, é comum exigir um segredo fornecido pelo usuário como parte do processo de autenticação, e então periodicamente renovar a autenticação. Além disso, dado que sobre tais circunstâncias pode existir a possibilidade da presença de um cavalo de tróia no sistema do cliente, mecanismos de senhas de uma via (one-time passwords) são freqüentemente aconselháveis. Escolher um mecanismo de senha e intervalos de renovação que provêem um nível aceitável de risco, mas que não aborreça o usuário em excesso, pode ser um desafio. É claro que até mesmo esta abordagem oferece garantias limitadas em muitos casos.

Claramente, existem vários níveis possíveis de garantia que serão atingidos com a utilização de várias técnicas de autenticação, e nenhuma das técnicas discutidas oferece garantias absolutas. Também, existem variações nos requisitos de autenticação entre diferentes cenários de acesso remoto. Isso significa que não existe uma solução padrão para este problema, e cada cenário em particular deve ser cuidadosamente examinado para se obter seus requisitos específicos.

Compatibilidade com mecanismos de acesso remoto legados

Existem vários mecanismos de acesso remoto que foram criados antes do desenvolvimento do IPSec. Tipicamente, são sistemas que confiam no RADIUS [RRSW00] para autenticação dos usuários e registro de eventos, mas existem também outros mecanismos. Uma solução ideal de acesso remoto IPSec pode utilizar os componentes do sistema já existentes sem modificações. Considerando que isto é possível, esta deveria ser uma meta. No entanto, pode haver casos onde isto simplesmente não pode ser realizado, devido a segurança ou outra consideração qualquer. Em tais casos, o modelo de acesso remoto IPSec deve ser projetado para acomodar a migração entre esses mecanismos da melhor forma possível.

Em geral, os mecanismos de acesso remoto IPSec propostos deveriam atender às seguintes metas:

- prover suporte direto a sistemas legados de autenticação de usuários e registro de eventos;
- encorajar a migração dos sistemas baseados em senhas de baixa entropia para sistemas de autenticação mais seguros;
- se o suporte a autenticação de usuário legada não puder ser provida sem algum tipo de migração, o impacto de tal migração deve ser minimizado;
- informações de autenticação de usuários devem ser protegidas contra eavesdropping (escuta clandestina) e ataques de replay (incluindo a identidade do usuário).

4.1.2 Configuração do sistema remoto

A configuração do sistema remoto esta relacioanda à configuração dos parâmetros de rede do sistema cliente. Essa configuração pode ser fixa ou dinâmica. Ela pode ser provida completamente pelo administrador da rede onde o usuário remoto está situado, como por exemplo, o Provedor de Acesso à Internet (*Internet Service Provider* – ISP), ou pode ser provido parcialmente por este administrator, com o restante das configurações providas por uma entidade na rede remota da corporação que o cliente está acessando. Em geral, esta configuração pode incluir vários itens, como por exemplo:

- Endereço(s) IP(s)
- Máscara de rede
- Endereço de broadcast

- Nome da máquina
- Relógio (Time offset)
- Servidores (por exemplo SMTP, POP, DNS/NIS, WINS, NTP, etc)
- Roteadores
- Opções de router discovery
- Rotas estáticas
- MTU (Unidade máxima de transferência)
- TTL default
- Opções de source routing
- Ligamento/Desligamento do repasse de pacotes (IP Forwarding)
- Opções de Path MTU
- Timeout do cache ARP
- Opções de X Windows
- Opções do NIS
- Opções do NetBIOS

Por exemplo, em alguns casos pode ser atribuído ao cliente um "endereço virtual", dando a aparência de que ele reside na rede privada que está sendo acessada, como mostrado na Figura 4.2.

Neste caso, o sistema cliente inicia a conexão utilizando um endereço válido de Internet. Um endereço adicional da rede privada é atribuído a esse cliente, e pacotes contendo esse endereço que foi atribuído são encapsulados, com os cabeçalhos externos contendo o endereço válido do cliente, e repassados para o servidor através do túnel. Isto provê ao cliente uma presença virtual na rede privada através do túnel IPSec. Note que o cliente agora tem dois endereços ativos: o endereço atribuído pelo provedor de acesso à Internet (ISP) e o endereço IP virtual (*Virtual IP* – VIP).

Após obter essa presença virtual na rede da corporação, o cliente pode agora requisitar outros tipos de configuração relacionados à topologia, por exemplo, roteadores padrão, servidores de DNS, além de outros parâmetros, da mesma forma que uma máquina configurada dinamicamente situada fisicamente na rede privada.

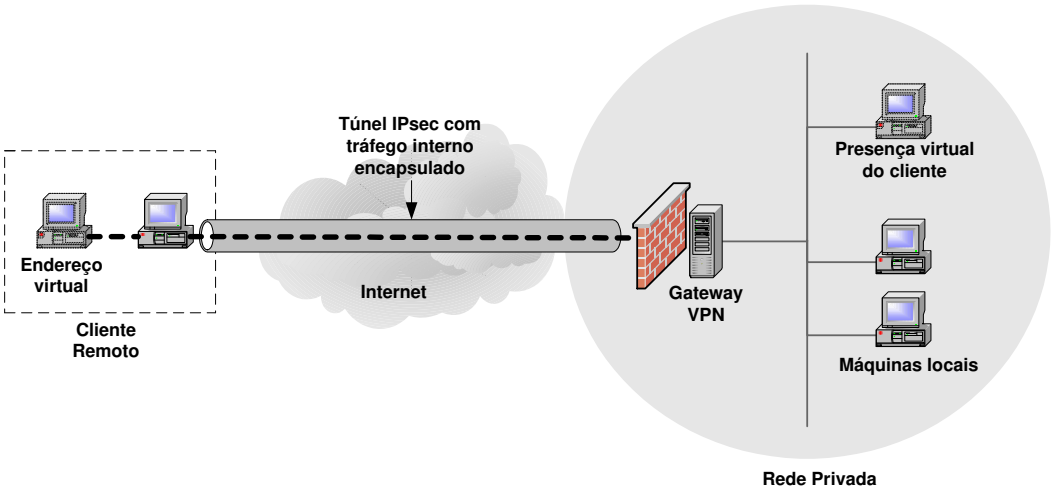


Figura 4.2: Atribuição de endereço IP virtual

4.1.3 Configuração da política de segurança

A configuração da política de segurança está relacionada às políticas de acesso para ambos, cliente remoto e gateway VPN. Em alguns cenários, pode ser necessário configurar as políticas de acesso nos sistemas clientes conectados, protegendo assim a rede privada. Por exemplo, como o cliente tem acesso à Internet, através de seu endereço válido, outros sistemas na Internet também têm algum nível de acesso recíproco ao cliente. Em alguns casos, pode ser desejável bloquear este acesso à Internet, ou forçá-lo a passar pelo túnel IPSec, enquanto o cliente possuir uma conexão tunelada com a rede privada. Esta é uma forma de configuração da política de segurança no cliente.

Para o gateway VPN, também pode ser necessário ajustar dinamicamente suas políticas baseado no usuário com o qual a conexão foi estabelecida. Por exemplo, digamos que existam dois usuários remotos A e B. Deseja-se proporcionar ao usuário A um acesso irrestrito à rede privada, enquanto que se deseja restringir o acesso do usuário B a segmentos de rede específicos. Uma forma de realizar isso seria atribuir estaticamente um "endereço virtual" interno para cada usuário, de forma que cada um sempre terá o mesmo endereço. Então, um acesso de um usuário em particular pode ser controlado através das políticas baseadas naquele endereço em particular. Contudo, esta não seria uma solução escalável.

Uma solução escalável para o controle de acesso de clientes remotos seria atribuir dinamicamente endereços IP de uma faixa específica baseado na identidade do cliente autenticado, com acesso aos recursos específicos controlado por políticas baseadas em endereços no gateway VPN. Isto é bastante similar ao mapeamento estático descrito anteriormente, exceto pelo fato de que um grupo de usuários, com controle de acesso idêntico, compartilharia uma determinada faixa de endereços IP, que garantem o acesso exigido, ao invés de

um determinado usuário sempre mapeado a um determinado endereço. Entretanto, esta solução também possui problemas de escalabilidade, porém não tão consideráveis quanto no mapeamento estático.

Alternativamente, um endereço arbitrário pode ser atribuído ao usuário, com a política de segurança do gateway VPN sendo dinamicamente atualizada baseada na identidade do cliente remoto e seu endereço IP virtual atribuído, para permitir acesso a recursos particulares. Nestes casos, a configuração relevante das políticas de segurança é específica para o gateway VPN, e não para o cliente. Tanto a configuração das políticas de segurança do servidor quanto do cliente são abrangidas por esta categoria de requisitos.

4.1.4 Auditoria

O termo auditoria é usado aqui para se referir à coleta e apresentação de informações sobre o estado da conexão pelo servidor de acesso remoto IPSec, com a finalidade de manter a segurança e a integridade da rede protegida pelo servidor. Para o acesso remoto, as seguintes informações de auditoria são úteis do ponto de vista da segurança:

- horário de início da conexão
- horário de fim da conexão

Note que os requisitos para o atributo "horário de fim da conexão" implicam na necessidade de algum tipo de mecanismo de conexão com verificação freqüente, com o qual o servidor possa determinar precisamente esse valor em casos onde o cliente não encerra a conexão explicitamente.

Em alguns casos, essa freqüência de verificação pode influenciar negativamente em uma conexão. Por exemplo, se o intervalo de freqüência é muito curto, e a conexão é encerrada após a perda de poucos pacotes de verificação, há a possibilidade de que um congestionamento na rede possa conduzir a resets desnecessários. O intervalo de freqüência de verificação e o limiar dos resets devem ser escolhidos tendo este fato em mente, e deve ser possível ajustar estes valores através de configuração ou negociação.

4.1.5 Passagem por intermediário

Passagem por intermediário é usado aqui para se referir à passagem de um fluxo de dados seguro através de um intermediário tal como um firewall ou um dispositivo de Tradução de Endereços de Rede (*Network Address Translation* – NAT). No caso dos firewalls, vários produtos desenvolvidos não reconhecem a família de protocolos IPSec, tornando difícil, ou às vezes impossível, obter uma configuração para atravessá-lo. Em

tais casos, um mecanismo é necessário para fazer com que o fluxo de dados pareça ser de um outro tipo que o firewall seja capaz de gerenciar.

No caso de dispositivos de NAT, existem vários problemas com a tentativa de se passar um fluxo de dados cifrado ou autenticado. Por exemplo, dispositivos de tradução de endereços de rede com multiplexação de porta (*Network Address Port Translation* – NAPT) normalmente modificam o endereço IP e a porta TCP/UDP de origem dos pacotes de saída, e o endereço IP e a porta TCP/UDP de destino dos pacotes de chegada, e em alguns casos, eles modificam campos adicionais na porção de dados dos pacotes. Tais modificações tornam impossível o uso do protocolo AH. No caso do ESP, os campos de porta TCP/UDP são algumas vezes ilegíveis e sempre imodificáveis, tornando as traduções significativas dos dispositivos de NAPT impossíveis. Existem várias outras combinações de campos de protocolos que sofrem com esse problema.

4.2 Cenários

Existem inúmeros cenários de acesso remoto possíveis utilizando IPSec. Esta seção contém um breve resumo destes cenários, seguido por uma subseção dedicada a cada um, que explora os vários requisitos de acordo com as categorias definidas anteriormente.

4.2.1 Usuários dial-up/DSL/cablemodem

Este é um dos cenários mais comuns de acesso remoto. A conveniência e a alta disponibilidade do acesso à Internet fazem com que esta seja uma opção atraente em muitas circunstâncias. Usuários podem acessar a Internet do conforto de sua casa ou quarto de hotel, e usando esta conexão com a Internet, podem acessar os recursos de uma rede privada. Em alguns casos, são usadas contas dial-up para prover o acesso inicial à Internet, enquanto em outros casos algum tipo de conexão permanente, como DSL ou cablemodem, é utilizada.

Os casos de conexão dial-up e conexões permanentes são bem parecidos, com duas diferenças significativas: o mecanismo de atribuição de endereço e a duração da conexão. Em muitas casos de conexão dial-up, o endereço IP do cliente é atribuído dinamicamente como parte da configuração da conexão, e com probabilidade bastante alta de ser diferente para cada conexão do cliente. Usuários DSL, por outro lado, freqüentemente têm endereços IP estáticos atribuídos a eles, embora a atribuição dinâmica esteja crescendo. Em relação à duração da conexão, o acesso remoto dial-up possui normalmente um tempo de vida curto, enquanto que conexões permanentes podem manter conexões de acesso remoto por períodos de tempo significativamente mais longos.

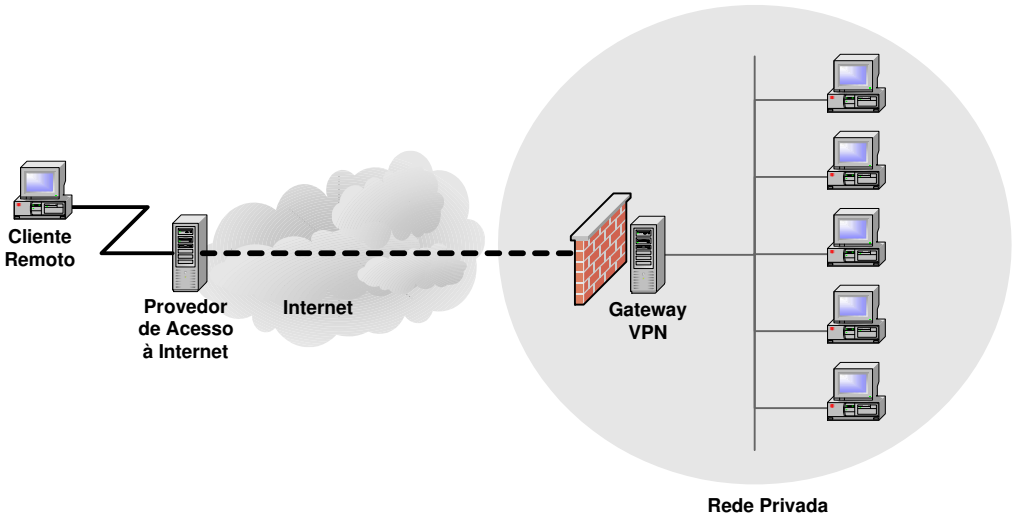


Figura 4.3: Usuários dial-up/DSL/cablemodem

A configuração geral, em ambos os casos, é semelhante ao cenário mostrado na Figura 4.3.

Uma alternativa para esta configuração seria colocar um gateway VPN entre o sistema do usuário e o modem, caso no qual este gateway VPN adicionado se tornaria o cliente de acesso remoto IPSec. Isto é atualmente muito comum em casos onde conexões DSL/cablemodem são utilizadas.

Requisitos de autenticação dos extremos do túnel

Os requisitos de autenticação desse cenário dependem em parte dos requisitos gerais de segurança da rede à qual o acesso está sendo provido. Assumindo que o gateway VPN é fisicamente seguro, uma autenticação de máquina para este servidor é suficiente.

Para o cliente, existem várias ameaças à integridade do processo de autenticação do usuário. Devido à natureza desprotegida dos sistemas operacionais mais comuns, é bastante difícil se proteger contra algumas dessas ameaças. Por exemplo, é muito difícil afirmar, com qualquer nível de certeza, que um sistema de usuário que permite o download e a execução de aplicações arbitrárias da Internet não esteja comprometido, e que uma aplicação oculta não esteja monitorando e interagindo com os dados do usuário.

Porém, existem duas ameaças gerais para as quais poderíamos lidar com os mecanismos de autenticação apropriados se pudermos assumir que o sistema não esteja comprometido. Primeiro, existe a possibilidade de que uma conexão segura seja estabelecida com um usuário particular, mas que alguém diferente do usuário planejado esteja usando esta conexão. Segundo, há a possibilidade de que as credenciais do usuário tenha sido

comprometida de alguma maneira, e esteja sendo usada por alguém diferente do usuário autorizado para obter acesso à rede privada.

Para minimizar a primeira ameaça, a possibilidade de alguém diferente do usuário autorizado estar utilizando a conexão, é necessária uma renovação periódica da autenticação do usuário. Deve ficar claro que uma autenticação de máquina não é suficiente neste caso, e que requisitar periodicamente a reentrada de uma senha inalterada limitará a eficácia da solução. A verificação convincente da presença do usuário autorizado, em muitos casos, requer a aplicação periódica de uma credencial que varia com o tempo.

Minimizar a segunda ameaça, o comprometimento da credencial, é difícil, e depende de vários fatores. Se o sistema cliente estiver executando um sistema operacional altamente seguro, então uma credencial que varia com o tempo pode novamente ser interessante. Uma senha estática é claramente deficiente neste cenário, já que ela pode estar sujeita a ataques de adivinhação online ou offline, e eventualmente ser comprometida, que é justamente a ameaça que estamos tentando minimizar. Contudo, se o sistema operacional do cliente não é seguro, o uso de uma credencial que varia com o tempo só será eficaz se o acesso simultâneo de mais de um local for proibido, e se o mecanismo gerador de credenciais não é facilmente comprometido.

Uma segunda abordagem para o problema do comprometimento da credencial seria o uso de uma credencial baseada em uma Infra-estrutura de Chaves Públicas (ICP) que é de alguma forma armazenada em um dispositivo seguro, e que requer alguma interação com o usuário antes da operação, como por exemplo, um smartcard. Se uma dada credencial requer uma interação periódica com o usuário para continuar operando, como por exemplo, um número de identificação pessoal (*Personal Identification Number* – PIN) com reentrada, isto pode ajudar a limitar o acesso de um usuário não autorizado. Porém, escolher um intervalo de renovação aceitável é um grande problema, e se o PIN não variar com o tempo, ele fornecerá uma garantia adicional limitada.

Requisitos de configuração do sistema remoto

Existem duas possibilidades para a configuração do sistema remoto neste cenário: o acesso à rede privada é permitido para os endereços nativos atribuídos pelo provedor de acesso à Internet utilizado pelo sistema do cliente remoto, ou então é atribuído ao sistema do cliente um endereço virtual do espaço de endereçamento da rede privada. No primeiro caso, não há requisitos de configuração do sistema remoto que não seja satisfeito pelo ISP. Porém, este caso é a exceção, e não a regra.

O segundo caso é mais comum, devido aos inúmeros benefícios proporcionados pela presença virtual do sistema cliente na rede privada. A presença virtual permite que o cliente receba broadcasts de rede, permitindo assim que ele faça uso do protocolo WINS, geralmente usado em redes Windows, na rede privada. Além disso, se o cliente tunela

todo o tráfego para a rede privada, então algumas políticas da rede privada podem ser aplicadas ao tráfego de Internet de e para o sistema cliente.

Neste caso, como requisitos de configuração do cliente, temos no mínimo a atribuição de um endereço IP da rede privada. Tipicamente, o sistema cliente requer várias outras informações de configuração, dependendo do nível de complexidade da topologia da rede corporativa.

Requisitos de configuração da política de segurança

Em relação à configuração das políticas de segurança no cliente, o assunto mais importante é se o cliente pode ter acesso direto à Internet ao mesmo tempo em que está conectado à rede destino. Isto é importante devido ao fato de que se o cliente tem acesso a sites na Internet, os sites possuem o mesmo nível de acesso recíproco ao cliente. Pode ser desejável eliminar completamente este tipo de acesso enquanto o túnel estiver ativo.

Alternativamente, os riscos podem ser minimizados forçando todo o tráfego para a Internet gerado pelo cliente a passar pelo túnel com a rede privada, onde ele pode estar sujeito às políticas da rede. Um segunda abordagem que acarretaria uma menor sobrecarga na comunicação seria modificar a configuração das políticas no próprio sistema cliente refletindo assim as políticas da rede privada enquanto o cliente estiver conectado. Neste caso, o tráfego não é forçado a passar pela rede destino antes de sair ou entrar no cliente. Isto requer alguma forma de download ou modificação das políticas como parte do processo de estabelecimento da associação de segurança (SA). Uma terceira abordagem seria prover uma configuração variável para o cliente que permita especificações do tipo "tunele tudo", ou "bloqueie todo o tráfego que não seja destinado à rede privada enquanto a SA estiver ativa".

Em relação à configuração do servidor, pode ser necessário atualizar dinamicamente a base de dados de políticas de segurança (*Security Policy Database* – SPD) do IPSec quando o usuário remoto se conectar. Isto porque os seletores de tráfego podem ser baseados nos parâmetros de endereço de rede, e este pode não ser conhecido a priori no caso do acesso remoto. Isto pode ser evitado por meio de um mecanismo que permita a atribuição de endereço baseado na identidade que foi autenticada.

Requisitos de auditoria

Para sessões de usuários dial-up/DSL/cablemodem, os horários de início e término da sessão devem ser coletados. A obtenção confiável do horário de fim da sessão requer que o cliente de alguma forma anuncie que a conexão permanece ativa. Isto fica implícito se o servidor receber dados do cliente através da conexão, mas em casos onde nenhum dado é enviado por algum período de tempo, é necessário um mecanismo de sinalização através

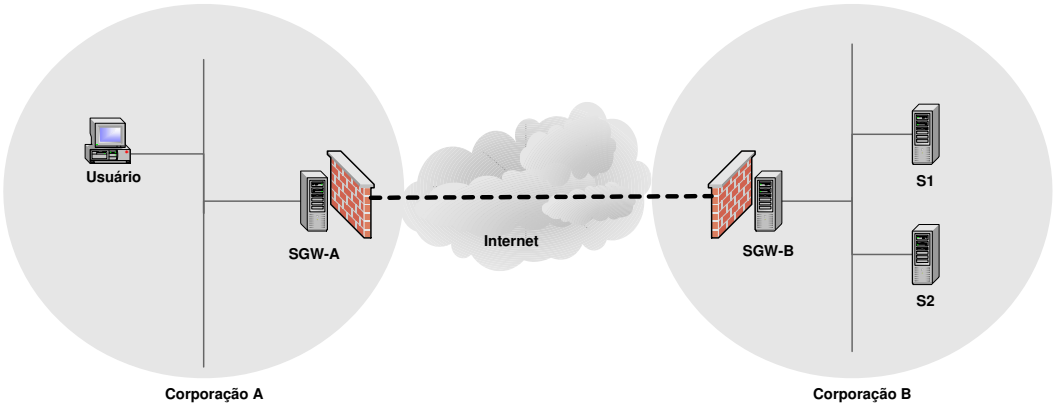


Figura 4.4: Ambiente corporativo para Extranets

do qual o cliente indica que a conexão permanece em uso.

Requisitos de passagem por intermediário

Se o endereço atribuído ao cliente pelo provedor é um endereço público [RMK+94], e não há dispositivos intermediários entre o cliente e o servidor de acesso remoto realizando operações de tradução de endereços com multiplexação de porta (NAPT) no fluxo de dados, então não existem requisitos adicionais. Se operações de NAPT são realizadas no fluxo de dados, algum mecanismo deve ser provido para tornar estas modificações transparentes à implementação IPSec.

4.2.2 Ambiente corporativo para Extranets

Neste cenário, um usuário situado fisicamente em um ambiente corporativo utiliza um sistema local para acessar recursos na rede de outra corporação. Tipicamente, estas empresas possuem algum nível de cooperação entre si, mas não em um grau no qual a falta de controle de acesso entre as duas redes seja aceitável. Conseqüentemente, este cenário é caracterizado pelo acesso limitado. A aparência deste cenário é semelhante ao apresentado na Figura 4.4.

Esta topologia é propositadamente simplificada para ilustrar algumas características básicas sem aprofundar nos detalhes. Na extremidade de cada rede há um dispositivo que é a combinação de um gateway VPN e firewall. Eles serão chamados de SGW-A e SGW-B. Neste diagrama, a corporação B deseja prover ao usuário da corporação A o acesso aos servidores S1 e S2. Isto pode ser realizado de várias formas diferentes:

(1) Uma associação de segurança (SA) fim-a-fim é estabelecida entre o usuário e S1 ou S2.

(2) Uma associação de segurança (SA) em modo túnel é estabelecida entre SGW-A e SGW-B que permite somente tráfego entre S1/S2 e o usuário.

(3) Uma associação de segurança (SA) em modo túnel é estabelecida entre o usuário e SGW-B que permite somente tráfego entre S1/S2 e o usuário.

Estes vários casos serão individualmente discutidos em relação a cada categoria de requisitos a seguir.

Requisitos de autenticação

Para o cenário de uma corporação externa (*extranet*), os requisitos de autenticação podem variar ligeiramente dependendo da maneira como a conexão é realizada. Se é permitido que somente um usuário em particular tenha acesso a S1/S2, então é necessária uma autenticação em nível de usuário. Se as conexões forem dos tipos (1) ou (3), elas podem então ser tratadas da mesma forma que conexões de usuários dial-up. Se as conexões forem do tipo (2), então ou SGW-A provê algum mecanismo local para autenticar o usuário e SGW-B deve confiar neste mecanismo, ou SGW-B deve ter algum mecanismo para autenticar o usuário que seja independente de SGW-A.

Se o acesso é permitido a qualquer pessoa dentro da corporação A então uma autenticação de máquina será suficiente. Porém, isto é altamente improvável. Uma situação um pouco mais provável seria aquela onde o acesso é permitido para qualquer pessoa dentro de uma unidade organizacional em particular na corporação A. Este caso é bem parecido com o caso de uma único usuário discutido anteriormente, e essencialmente tem as mesmas exigências em termos de mecanismos necessários para SGW-A, embora a autenticação de máquina possa ser suficiente se a unidade organizacional a qual é permitido o acesso tenha um nível suficiente de segurança física. Novamente, isto requer que a corporação B confie na corporação A.

Requisitos de configuração do sistema remoto

É possível que a corporação B queira atribuir um endereço virtual para o sistema do usuário durante sua conexão. O único modo disso se realizar seria se o usuário fosse um dos extremos do túnel, como nos casos (1) e (3).

Requisitos de configuração da política de segurança

Qualquer um dos casos discutidos anteriormente poderia apresentar alguma exigência de configuração de uma política estática. O caso (1) pode exigir que SGW-A e SGW-B permitam o tráfego IPSec entre o usuário e S1/S2. O caso (3) possui requisitos parecidos,

com a diferença de que o tráfego IPSec deve ser entre o usuário e SGW-B. O caso (2) pode exigir que o tráfego apropriado seja protegido entre o usuário e S1/S2.

Nenhum desses casos requer uma configuração dinâmica de políticas de segurança.

Requisitos de auditoria

Para os casos (1) e (3), os horários de início e término das sessões devem ser coletados. A obtenção confiável do horário de fim da sessão requer que o cliente de alguma forma anuncie que a conexão permanece ativa. Isto fica implícito se o servidor receber dados do cliente através da conexão, mas em casos onde nenhum dado é enviado por algum período de tempo, é necessário um mecanismo de sinalização através do qual o cliente indica que a conexão permanece em uso.

Para o caso (2), o tipo de auditoria de dados exigida iria depender se o tráfego de múltiplos usuários seria agregado dentro de um único túnel ou não. Neste caso, a noção de tempo de início e fim de conexões individuais seria perdida. Se tais medidas são desejadas, é necessário que sejam criados túneis para cada usuário entre SGW-A e SGW-B, e que alguma forma de timeout seja usada para causar a finalização do túnel quando o tráfego não ocorrer por algum intervalo de tempo.

Requisito de passagem por intermediário

Se o endereço atribuído ao sistema cliente pela rede hospedeira (*extranet*) é um endereço público [RMK+94], e não há dispositivos intermediários entre o cliente e o servidor realizando operações de tradução de endereços com multiplexação de porta (NAPT) no fluxo de dados, então não há requisitos adicionais a este respeito. Se operações de NAPT são realizadas no fluxo de dados, algum mecanismo deve ser utilizado para tornar estas modificações transparentes à implementação IPSec.

Se um firewall situado na borda da rede hospedeira não puder ser configurado para permitir a passagem de protocolos IPSec, então algum mecanismo deve ser utilizado para converter o fluxo de dados em algum tipo que o firewall esteja configurado para permitir a passagem. Se o firewall pode ser configurado para permitir a passagem de protocolos IPSec, então isto deve ser realizado antes do estabelecimento da conexão.

4.2.3 Notebook em uma extranet para rede interna da corporação

O uso de um notebook durante uma visita a outras corporações representa outro cenário de extranet que tem se tornado bastante comum. Neste caso, um usuário trabalha temporariamente dentro de outra corporação, por exemplo, como parte de algum tipo de

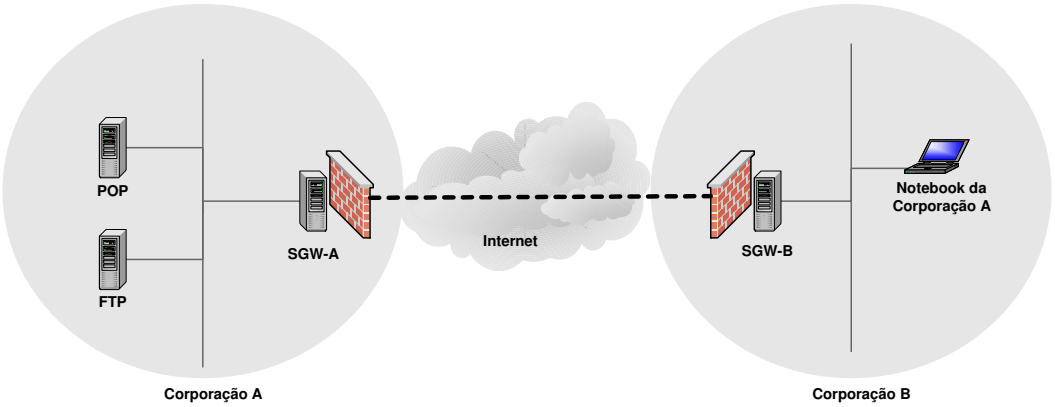


Figura 4.5: Notebook em uma extranet para rede interna da corporação

contrato de serviço. O usuário traz consigo um laptop da corporação A que recebe um endereço da corporação B estática ou dinamicamente, e o usuário deseja acessar recursos na rede da corporação A de forma segura usando este laptop. Este cenário seria semelhante ao apresentado na Figura 4.5.

Este é um cenário bastante parecido com o cenário de um usuário dial-up, mas ele difere em vários aspectos importantes. Em primeiro lugar, neste caso, há freqüentemente um gateway VPN e um firewall do lado da corporação B. Em segundo lugar, há um risco significativamente maior de que uma conexão de maior duração fique acessível a alguém diferente do usuário planejado.

Requisitos de autenticação

Na maioria dos casos, as únicas conexões aceitáveis do ponto de vista da corporação A são entre o notebook e o SGW-A ou entre o notebook e os servidores que ele deseja acessar. A maioria das considerações feitas aos usuários dial-up também se aplicam a este cenário, e uma autenticação no nível de usuário é necessária para prover garantias de que o usuário que iniciou a conexão é o mesmo que permanece ativo. Como uma precaução adicional, uma combinação de autenticação no nível de usuário e autenticação no nível de máquina pode ser justificável em alguns casos. Além disso, esta autenticação deve ser renovada freqüentemente.

Requisitos de configuração do sistema remoto

Os requisitos de configuração do sistema remoto neste cenário são os mesmos para o cenário de um usuário dial-up, isto é, o notebook pode ter uma presença virtual na rede da corporação, e nesse caso, ser necessária uma infra-estrutura completa de configuração.

Requisitos de configuração da política de segurança

As exigências de configuração de políticas neste cenário diferem do caso dos usuários dial-up, pois ao laptop não pode ser atribuída uma política que exige que todo o tráfego seja repassado para a corporação A através do túnel. Isto devido ao fato de que o laptop possui um endereço da corporação B, e como tal, pode gerar tráfego destinado à corporação B. Se este tráfego for tunelado para a corporação A, pode não haver nenhum caminho de retorno para a corporação B exceto através do próprio laptop. Por outro lado, o tráfego relacionado à Internet pode estar sujeito a esta restrição se desejado, e todo o tráfego que não seja entre a corporação A e o laptop pode ser bloqueado durante a conexão.

Requisitos de auditoria

Os requisitos de auditoria neste cenário são os mesmos do cenário de usuários dial-up. Os horários de início e término das sessões devem ser coletados. A obtenção confiável do horário de fim da sessão requer que o cliente de alguma forma anuncie que a conexão permanece ativa. Isto fica implícito se o servidor receber dados do cliente através da conexão, mas em casos onde nenhum dado é enviado por algum período de tempo, é necessário um mecanismo de sinalização através do qual o cliente indica que a conexão permanece em uso.

Requisito de passagem por intermediário

Se o endereço atribuído ao sistema cliente pela rede hospedeira (extranet) é um endereço público [RMK+94] e não há dispositivos intermediários entre o cliente e o servidor realizando operações de tradução de endereços com multiplexação de porta (NAPT) no fluxo de dados, então não há requisitos adicionais a este respeito. Se operações de NAPT são realizadas no fluxo de dados, algum mecanismo deve ser utilizado para tornar estas modificações transparentes à implementação IPSec.

Se um firewall situado na borda da rede hospedeira não puder ser configurado para permitir a passagem de protocolos IPSec, então algum mecanismo deve ser utilizado para converter o fluxo de dados em algum tipo que o firewall esteja configurado para permitir a passagem. Se o firewall pode ser configurado para permitir a passagem de protocolos IPSec, então isto deve ser realizado antes do estabelecimento da conexão.

4.2.4 Desktop em uma extranet para rede interna da corporação

Este cenário é bastante parecido com o cenário de um laptop em uma extranet discutido anteriormente, exceto pelo fato de que um grau de confiança maior é exigido pela

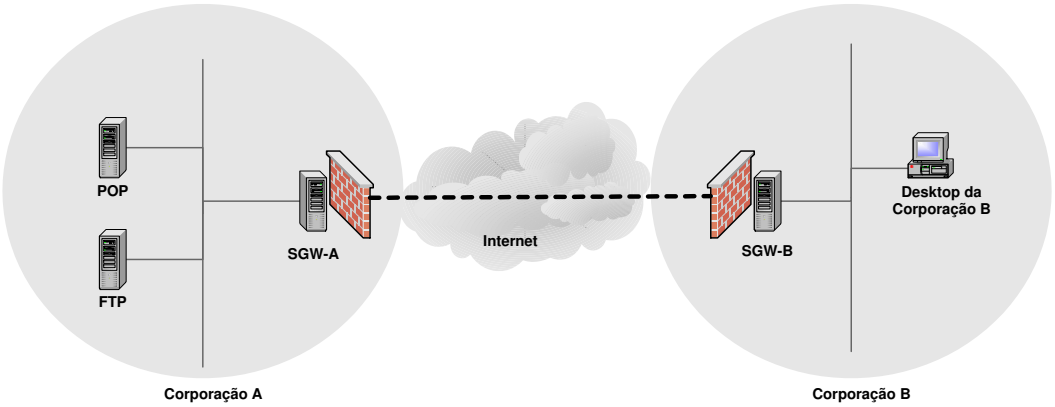


Figura 4.6: Desktop em uma extranet para rede interna da corporação

corporação A para a corporação B. Este cenário é apresentado na Figura 4.6.

Requisitos de autenticação

Os requisitos de autenticação para o cenário de um computador em uma extranet são muito parecidos com os discutidos anteriormente para o cenário de um laptop em uma extranet. A principal diferença está no tipo de autenticação utilizado. No caso do laptop, a corporação A possui alguma garantia de que a conexão esteja vindo de um dos sistemas da própria corporação A, se uma credencial de máquina for utilizada pelo laptop. No caso do desktop isto não é possível, já que a corporação A não é a proprietária do sistema cliente.

Requisitos de configuração do sistema remoto

Os requisitos de configuração do sistema remoto neste cenário são os mesmos do cenário do laptop em uma extranet, isto é, ao sistema desktop pode ser atribuída uma presença virtual na rede da corporação, e nesse caso, pode ser necessária uma infra-estrutura completa de configuração. Contudo, isto parece menos provável do que no cenário do laptop, dada a ausência de controle da corporação A sobre o software de configuração do sistema desktop da corporação B.

Requisitos de configuração da política de segurança

Os requisitos de configuração de política são bastante semelhantes aos do cenário do laptop em uma extranet, exceto pelo fato de que neste cenário há bem menos controle sobre o desktop da corporação B do que sobre o laptop. Isto significa que pode não ser possível restringir o tráfego no sistema desktop.

Requisitos de auditoria

Os requisitos de auditoria neste cenário são os mesmos do cenário de usuários dial-up. Os horários de início e término das sessões devem ser coletados. A obtenção confiável do horário de fim da sessão requer que o cliente de alguma forma anuncie que a conexão permanece ativa. Isto fica implícito se o servidor receber dados do cliente através da conexão, mas em casos onde nenhum dado é enviado por algum período de tempo, é necessário um mecanismo de sinalização através do qual o cliente indica que a conexão permanece em uso.

Requisito de passagem por intermediário

Se o endereço atribuído ao sistema cliente pela rede hospedeira (extranet) é um endereço público [RMK+94] e não há dispositivos intermediários entre o cliente e o servidor realizando operações de tradução de endereços com multiplexação de porta (NAPT) no fluxo de dados, então não há requisitos adicionais a este respeito. Se operações de NAPT são realizadas no fluxo de dados, algum mecanismo deve ser utilizado para tornar estas modificações transparentes à implementação IPSec.

Se um firewall situado na borda da rede hospedeira não puder ser configurado para permitir a passagem de protocolos IPSec, então algum mecanismo deve ser utilizado para converter o fluxo de dados em algum tipo que o firewall esteja configurado para permitir a passagem. Se o firewall pode ser configurado para permitir a passagem de protocolos IPSec, então isto deve ser realizado antes do estabelecimento da conexão.

4.2.5 Sistema público para rede privada

Este cenário se refere ao caso de um usuário em viagem se conectando a uma rede destino utilizando um sistema público de outro proprietário qualquer. Um exemplo comum poderia ser um quiosque de aeroporto. Este cenário é semelhante ao cenário de um desktop em uma extranet, exceto pelo fato de que no cenário da extranet, a corporação A pode ter uma relação de confiança com a corporação B, enquanto que neste cenário, a corporação A pode não confiar em um sistema publicamente acessível. Note que uma relação de confiança entre a corporação A e o proprietário do sistema publicamente acessível pode existir, mas na maioria da vezes não existirá.

Requisitos de autenticação

Há duas variações para este cenário. Na primeira, não existe uma relação de confiança entre a rede destino e o sistema público utilizado. Na segunda, existe uma relação de confiança. No caso onde não existe uma relação de confiança, a autenticação de máquina

está fora de cogitação, pois não faz sentido neste contexto. Além disso, como este sistema pode facilmente capturar uma senha, o uso de uma senha estática em tal sistema é fortemente desaconselhável.

Se uma senha de uso único (*one-time password*) fosse usada, isto poderia reduzir o risco de uma captura de senha por um sistema público. Por outro lado, se esta captura é uma ameaça real, ou seja, o sistema é malicioso, então qualquer dado transmitido e recebido através da sessão resultante não deve ser confidencial ou confiável, e não se pode garantir que este sistema esteja de fato desconectado quando o usuário encerrar o seu uso. Isto significa que acessar informações sensíveis através de tais sistemas é uma atitude no mínimo imprudente.

Outra opção de autenticação de usuário possível seria um smartcard. Contudo, muitos *smartcards* exigem um número de identificação pessoal (PIN) ou senha para destravá-los, o que requer algum nível de confiança no quiosque para não manter de alguma forma esta senha. Conseqüentemente, esta abordagem sofre de desvantagens semelhantes às das considerações de senhas estáticas. A principal diferença seria que o PIN/senha não poderia ser utilizado sozinho para acesso sem o smartcard.

Em casos onde existe uma relação de confiança com o proprietário do sistema público, o nível de confiança se adaptaria ao nível de risco discutido anteriormente. Se existe um nível de confiança suficiente no proprietário do sistema, o uso de senhas estáticas pode não apresentar maiores riscos do que se este fosse permitido a um sistema cujo proprietário é a própria rede acessada. No entanto, o principal benefício de tal relacionamento de confiança seria a habilidade de autenticar as máquinas das quais o usuário está tentando realizar o acesso.

Uma política de segurança exigindo que o acesso remoto somente fosse permitido com a combinação de autenticação usuário/máquina poderia ser efetuada, com controle adicional relacionado a quais máquinas estão autorizadas.

Uma característica adicional que pode ser negociada em qualquer um dos casos está ligada à verificação da identidade do servidor. Se o cliente for de alguma forma enganado, um ataque de man-in-the-middle [NdG02] pode ser realizado, com a senha obtida do usuário sendo então usada para acessos maliciosos ao verdadeiro servidor. Note que até mesmo um mecanismo de senha de uso único oferece pouca proteção neste caso. Para evitar tal ataque, o cliente deve possuir algum conhecimento certificado ou secreto do servidor antes de tentar se conectar. Note que no caso onde não existe uma relação de confiança, isto não é possível.

Requisitos de configuração do sistema remoto

Não há requisitos de configuração do sistema remoto neste caso.

Requisitos de configuração da política de segurança

Não há requisitos de configuração da política de segurança neste caso.

Requisitos de auditoria

Os requisitos de auditoria neste cenário são os mesmo do cenário de usuários dial-up. Os horários de início e término das sessões devem ser coletados. A obtenção confiável do horário de fim da sessão requer que o cliente de alguma forma anuncie que a conexão permanece ativa. Isto fica implícito se o servidor receber dados do cliente através da conexão, mas em casos onde nenhum dado é enviado por algum período de tempo, é necessário um mecanismo de sinalização através do qual o cliente indica que a conexão permanece em uso.

Requisito de passagem por intermediário

Se o endereço atribuído ao sistema cliente pela rede hospedeira (extranet) é um endereço público [RMK+94] e não há dispositivos intermediários entre o cliente e o servidor realizando operações de tradução de endereços com multiplexação de porta (NAPT) no fluxo de dados, então não há requisitos adicionais a este respeito. Se operações de NAPT são realizadas no fluxo de dados, algum mecanismo deve ser utilizado para tornar estas modificações transparentes à implementação IPSec.

4.3 Conclusão

Através da apresentação dos cenários mais comuns de acesso remoto, foi possível identificar um conjunto geral de requisitos necessários na maioria dos casos.

Em relação à autenticação, foi possível identificar que a autenticação de máquina para o servidor é necessária em todos os cenários, a fim de evitar ataques de man-in-the-middle, onde o cliente remoto se conecta a um falso servidor. O suporte à autenticação de usuário também é necessário em praticamente todos os cenários, pois é difícil garantir um nível aceitável de segurança física em relação ao sistema cliente. A autenticação de máquina para o cliente geralmente só é útil se combinada com autenticação de usuário, podendo tal combinação ser um opção interessante em alguns cenários.

Um mecanismo para prover a configuração do sistema cliente é necessário na maioria dos cenários e tal mecanismo deve ser extensível, de forma a oferecer suporte a diversos parâmetros de configuração.

A configuração dinâmica da política de segurança no cliente é útil em vários cenários, já que tal sistema não possui garantias de segurança física e está suscetível a diversas

ameaças quando utilizado fora do escopo do acesso remoto. Em alguns cenários também é interessante a configuração de políticas dinâmicas no servidor, permitindo que este adapte suas políticas de segurança aos usuários conectados em um determinado instante.

A maioria dos cenários necessita de auditoria dos horários de início e término de sessão, e de algum mecanismo que garanta uma certa precisão destes horários.

Um mecanismo de passagem por intermediário pode ser necessário em qualquer um dos cenários, sendo que tal mecanismo deve ser capaz de tornar as modificações realizadas por esses intermediários transparentes à implementação IPSec, sem no entanto exigir modificação na configuração dos dispositivos intermediários.

Capítulo 5

Análise das soluções existentes

Após a análise de alguns dos cenários mais comuns de acesso remoto, ficou evidente a existência de requisitos importantes que devem ser satisfeitos para a completa viabilidade de uma solução de acesso remoto VPN.

No entanto, apesar do IPSec ser uma solução amplamente difundida para VPNs e possuir mecanismos de segurança bastante capazes, muitos dos requisitos apresentados anteriormente não são atendidos pelos mecanismos nativos do IPSec. Como conseqüência disso, diversos mecanismos proprietários foram sendo desenvolvidos para viabilizar o acesso remoto utilizando IPSec. Contudo, a existência de diferentes soluções gerou um grande problema de interoperabilidade, já que a inexistência de um padrão fez com que muitos fabricantes de produtos VPN desenvolvessem soluções que na grande maioria das vezes são compatíveis apenas com seus próprios produtos.

Com o objetivo de criar uma solução padrão para os problemas envolvendo o uso do IPSec em um ambiente de acesso remoto, várias propostas têm sido apresentadas e amplamente discutidas pelo *IPSec Remote Access Working Group* (IPSRA), contudo poucos resultados concretos foram alcançados até o momento.

É importante ressaltar que um dos requisitos apresentados pelo IETF para a padronização de uma solução é não exigir modificações nos protocolos AH, ESP e IKE que compõem o IPSec. Tal opção é justificável pelo fato deste requisito facilitar bastante a implementação e o desenvolvimento dos mecanismos que constituem uma solução, além de manter a compatibilidade com implementações anteriores e não adicionar complexidade e conseqüentemente potenciais problemas de segurança aos protocolos já existentes.

Neste capítulo serão discutidas algumas das soluções existentes para cada um dos requisitos dos cenários de acesso remoto VPN. O objetivo é obter um conjunto de mecanismos que viabilizem o acesso remoto VPN utilizando IPSec, avaliando suas vantagens e desvantagens, a fim de obter uma solução geral que atenda a todos os requisitos da melhor forma possível.

5.1 Autenticação

O IKE [HC98] provê mecanismos criptográficos para a realização de associações de segurança entre pares IP. Contudo, para isto o IKE exige que esses pares possuam fortes chaves criptográficas (simétrica ou assimétrica). Por esse motivo, o IKE não acomoda cenários onde a autenticação é realizada com uma senha de usuário ou outro material de natureza semelhante. Como esta última forma de autenticação é algo que muitas aplicações comerciais ainda requerem, o IPSRA foi incumbido da tarefa de desenvolver mecanismos criptográficos que complementem o IKE permitindo a realização de associações de segurança IPSec baseadas em métodos de autenticação legada de usuários.

Quatro métodos de autenticação estão atualmente definidos dentro do IKE [HC98]. Um dos métodos, denominado método de chaves pré-compartilhadas, usa um segredo que é compartilhado pelas entidades que estão se autenticando. O uso de chaves pré-compartilhadas é pessimamente escalável, exigindo o gerenciamento de $O(n^2)$ chaves para garantir uma segurança efetiva. Os outros três métodos são todos baseados no uso de tecnologias de chaves públicas, exigindo que, pelo menos em algum grau, a organização esteja envolvida no desenvolvimento ou uso de uma infra-estrutura de chaves públicas, para garantir uma solução escalável. Sistemas de autenticação legada, tais como o SecurID da SEcurity Dynamics, o OmniGuard/Defender da Axent, e até mesmo o RADIUS, um padrão do próprio IETF para autenticação legada, não são tratados neste padrão atual do IKE.

Os métodos de autenticação do IKE atualmente definidos compartilham duas propriedades: a autenticação é mútua (ambos os participantes autenticam um ao outro); e simétrica (ambos os participantes usam o mesmo método para autenticação). A autenticação mútua é importante não somente para mera identificação, mas também para prevenir ataques de man-in-the-middle [NdG02].

Em implementações cliente/servidor como a do IKE, quando um dos participantes no IKE é um usuário, enquanto o outro é um equipamento, como por exemplo um gateway ou um firewall, nem sempre é possível preservar a autenticação simétrica. Por exemplo, um usuário pode usar um token OmniGuard/Defender para responder a um desafio de autenticação, mas não podemos lançar um desafio OmniGuard/Defender para o firewall, já que não se pode checar a resposta do mesmo.

Diversos sistemas de autenticação já estão implantados em muitas organizações, e possivelmente grande parte dessas organizações não planejam desenvolver uma infra-estrutura de chaves públicas em um futuro próximo. Além disto, mesmo se uma organização decidir desenvolver uma infra-estrutura de chaves públicas, esse desenvolvimento pode levar um tempo considerável. Dentro deste período de transição, organizações podem desejar continuar usando seus sistemas legados de autenticação.

Durante o projeto de um método de autenticação do IKE que atenda a sistemas de autenticação legada, é necessário preservar a propriedade de autenticação mútua do IKE, apesar desta natureza simétrica poder ser violada.

A seguir serão apresentadas as características básicas de alguns dos principais mecanismos criados para prover a autenticação legada em conjunto com o atual padrão do protocolo IKE.

5.1.1 IKE Extended Authentication (XAUTH)

O IKE Extended Authentication (XAUTH) [PB99] é um mecanismo proposto ao IETF que se baseia no protocolo IKE, originalmente desenvolvido pela antiga empresa Timestep, hoje Alcatel. Ele descreve um método para utilizar os mecanismos de autenticação unidirecional existentes, tais como RADIUS, SecurID, e OTP (*One Time Password*), dentro do protocolo ISAKMP do IPSec. O propósito deste mecanismo não é substituir ou reforçar os mecanismos de autenticação existentes descritos no IKE [HC98], e sim permitir que eles possam ser estendidos usando mecanismos de autenticação legados.

O XAUTH permite ao protocolo ISAKMP/Oakley do IPSec suportar mecanismos de autenticação estendidos como autenticação de dois fatores (*two-factor authentication*), desafio/resposta (*challenge/response*) e outros métodos de autenticação unidirecional do acesso remoto.

A autenticação de dois fatores e o esquema de desafio/resposta, como SecurID e RADIUS, são formas de autenticação que permitem a um gateway VPN delegar a administração e autenticação de usuários a um servidor central de gerenciamento. Como esses métodos são todos métodos de autenticação unidirecional, ou seja, um cliente se autenticando perante um gateway, eles não podem ser utilizados isoladamente, devendo sempre ser utilizados em conjunto com outros métodos de autenticação do padrão ISAKMP.

A técnica utilizada pelo XAUTH usa o ISAKMP para transferir as informações de autenticação do usuário, tais como nome e senha, ao gateway VPN em uma mensagem ISAKMP protegida. Esse dispositivo pode então usar o protocolo apropriado (RADIUS, SecurID ou OTP) para autenticar o usuário. Isto permite que o servidor de autenticação esteja situado dentro da rede privada protegida pelo gateway VPN.

Método de autenticação estendida

Este mecanismo permite o uso de autenticação estendida, permitindo ao gateway VPN requisitar uma autenticação estendida de um cliente remoto, forçando este cliente a responder com suas credenciais de autenticação estendida. O gateway VPN pode então responder com uma mensagem de falha ou permissão.

Quando o gateway VPN requisita uma autenticação estendida, ele especifica o tipo de autenticação extra exigida e quais os parâmetros necessários para tal. Esses parâmetros podem ser os atributos necessários para realizar a autenticação ou podem ser uma informação necessária para a resposta do cliente, como por exemplo, um desafio.

A última mensagem enviada pelo gateway VPN é simplesmente uma mensagem informando a falha ou o sucesso da operação. A resposta pode conter alguma informação textual descrevendo a razão para a falha ou o sucesso. O gateway VPN podem também requisitar em seguida outra forma de autenticação, caso seja necessário.

Assim como o *PPP Challenge Handshake Authentication Protocol* (CHAP) [Sim96a], este protocolo também pode ser usado para autenticar periodicamente o usuário durante o tempo de vida da associação de segurança.

Se a máquina cliente não possui suporte ao método de autenticação requisitado pelo gateway VPN, então ela enviará de volta uma resposta com um atributo de status informando uma falha, falhando assim a autenticação, mas completando a transação.

O mecanismo de autenticação estendida não substitui os mecanismos de autenticação da Fase 1 do IKE. Eles simplesmente o estendem para permitir aos dispositivos realizar dois esquemas diferentes de autenticação. Ambos os pontos devem ainda autenticar um ao outro através dos métodos de autenticação descritos no IKE [HC98].

Como exemplos de autenticação estendida suportados pelo XAUTH podemos citar:

- **Autenticação simples:** Onde um nome de usuário e senha são requisitados para autenticação.
- **Desafio/Resposta:** Onde um desafio do gateway VPN deve ser incorporado com a resposta. Isto torna cada resposta diferente.
- **Autenticação de dois fatores (*Two-Factor Authentication*):** Este método de autenticação combina algo que o usuário conhece (sua senha) e algo que o usuário possui (um cartão).
- **Senha de uso único (*One-Time Password*):** Semelhante ao método de desafio/resposta, este método garante que a autenticação seja protegida contra ataques passivos baseados no reenvio de senhas capturadas, conhecidos como ataques de replay [NdG02].
- **Usuário autenticado previamente:** Podem ocorrer algumas situações onde o gateway VPN já tenha autenticado o cliente e nenhuma nova autenticação é necessária. Isto pode acontecer durante a renovação da chave de uma associação de segurança já existente (Fase 1 do IKE). Em tais cenários este método pode ser usado para evitar incomodar o usuário.

Extensões do Mode-Config

Para executar sua transação de autenticação, o XAUTH utiliza os mecanismos do Mode-Config [PAP99], descritos na Seção 5.2.1.

Todas as mensagens do Mode-Config em uma transação de autenticação estendida devem conter o identificador de transação do Mode-Config. O identificador da mensagem no cabeçalho ISAKMP também segue as regras definidas pelo protocolo Mode-Config.

Este protocolo pode então ser usado em conjunto com qualquer método de autenticação básico do IKE [HC98]. Se a autenticação mútua não é necessária, então a negociação da Fase 1 do IKE pode usar um método de autenticação de pré-segredo compartilhado e utilizar este segredo pré-compartilhado como nulo. Contudo, isto é fortemente desaconcelhável, já que dessa forma o gateway VPN não será autenticado.

Esta autenticação deve ser usada após a troca da Fase 1 ter sido completada e antes de qualquer outra troca, com exceção das trocas do modo Info [HC98], que são apenas mensagens informacionais. Se a autenticação estendida falhar, então a associação de segurança da Fase 1 deve ser imediatamente encerrada. O gateway VPN pode requisitar novamente uma autenticação estendida do usuário, com a restrição de que isso deve ser feito na mesma transação Mode-Config.

A autenticação estendida pode ser iniciada pelo gateway VPN a qualquer momento após a troca de autenticação inicial. Um servidor RADIUS, por exemplo, pode especificar que um usuário seja autenticado somente por um certo período de tempo. Uma vez que este período de tempo tenha se esgotado, o gateway VPN pode requisitar uma nova troca XAUTH. Se essa troca de autenticação estendida falhar, o gateway VPN deve encerrar todas as associações de segurança da Fase 1 e da Fase 2 associadas a este usuário.

Considerações de segurança

O uso do XAUTH não elimina a necessidade de autenticação da Fase 1 do IKE, que oferecem um alto nível de autenticação ao assinar os pacotes ISAKMP. Já a autenticação estendida não provê este serviço. A remoção ou o enfraquecimento da autenticação na Fase 1 torna a sessão IPSec suscetível a ataques de man-in-the-middle e ataques de spoofing [NdG02]. Por isso, quando o XAUTH for utilizado com chaves pré-compartilhadas, é vital que essa chave seja bem escolhida e protegida.

Além disso, quando o XAUTH for utilizado com chaves pré-compartilhadas em cenários onde o sistema do cliente remoto possui um endereço IP dinâmico, o *Main Mode* do IKE não pode ser utilizado, causando uma diminuição no nível de segurança desta solução. Neste cenário em particular, o gateway VPN não tem como estabelecer uma ligação entre o endereço IP do cliente e sua chave pré-compartilhada correspondente. Esse fato limita então a solução à utilização de uma única chave pré-compartilhada para todos os clien-

tes remotos, o que torna essa chave fortemente suscetível a ataques de engenharia social [NdG02].

5.1.2 Autenticação Híbrida

A Autenticação Híbrida (*Hybrid Authentication*) [LSZ00] é uma proposta apresentada ao IETF que define um conjunto de novos métodos de autenticação para serem usados dentro da Fase 1 do IKE, originalmente concebida pela empresa Check Point. Os novos métodos propostos assumem uma assimetria entre as entidades que estão se autenticando.

Uma entidade, tipicamente um gateway VPN, autentica-se através de técnicas padrões de chaves públicas, enquanto a outra entidade, tipicamente um usuário remoto, autentica-se utilizando técnicas de desafio/resposta. Estes métodos de autenticação são usados para estabelecer ao final da Fase 1 do IKE, uma associação de segurança IKE (IKE SA) que é unidirecionalmente autenticada. Para tornar esta autenticação bidirecional, esta Fase 1 é imediatamente seguida por uma troca XAUTH [PB99]. A troca XAUTH é usada para autenticar o usuário remoto. O uso destes métodos de autenticação é chamado de modo de Autenticação Híbrida.

Esta proposta foi projetada como uma solução para ambientes onde existe um sistema de autenticação legada, e uma infra-estrutura de chaves públicas ainda não foi desenvolvida.

Todos os métodos de autenticação atualmente definidos no IKE usam uma troca de seis pacotes para o *Main Mode*, e uma troca de três pacotes para o *Aggressive Mode*. Durante a definição de um novo método de autenticação, que é baseado em autenticação de desafio/resposta, não é possível impor uma limitação no número de pacotes que devem ser trocados para autenticar o usuário. Usualmente, um protocolo de autenticação simples consiste de três mensagens: um desafio do gateway VPN; uma resposta do usuário; e uma mensagem de status, indicando o sucesso ou falha na autenticação, enviada pelo gateway VPN. Contudo, em muitos casos o protocolo consiste em mais do que um simples desafio/resposta.

Devido a estas limitações, o processo de autenticação foi dividido em dois estágios. No primeiro estágio, uma troca da Fase 1 é utilizada para autenticar o gateway VPN e para estabelecer uma associação de segurança IKE (IKE SA). No segundo estágio, uma troca de transação do Mode-Config [PAP99], com os mecanismos descritos pelo XAUTH [PB99] é usada para autenticar o cliente. Mesmo que os dois estágios possam ser integrados em uma troca simples, essa separação, sendo baseada em trocas existentes sem a modificação das mesmas, é mais fácil de ser implementada.

Esta proposta é adequada para ambientes onde um sistema de autenticação legada é utilizado, mas mesmo assim criptossistemas de chaves públicas podem ser usados pelo

gateway VPN. Neste caso, a situação se parece com a autenticação que é implementada na World Wide Web usando o SSL. Os servidores usam técnicas de chave pública para se autenticar para o usuário, e estabelecer uma conexão criptografada. O usuário pode então se autenticar, ou enviar outra informação de identificação, tal como um número de cartão de crédito. A suposição neste modo é que distribuir chaves públicas para um pequeno número de entidades, como servidores web ou gateways VPN, é possível sem o desenvolvimento de uma infra-estrutura de chaves públicas completa.

Em alguns cenários, a política de segurança no gateway VPN pode exigir a autenticação tanto do usuário quanto da máquina utilizada pelo mesmo. Em tais casos os métodos de autenticação da Fase 1 descritos pelo XAUTH [PB99] devem ser usados.

O modo de autenticação híbrida como uma proteção

Os participantes do modo de autenticação híbrida são tipicamente um usuário e um gateway VPN. Eles iniciam uma negociação usando o *Main Mode* ou o *Aggressive Mode*, criando uma associação de segurança (SA) na qual o método de autenticação é de um novo tipo, indicando ser um método de autenticação híbrida. Ao final da Fase 1, a associação de segurança IKE (IKE SA) estabelecida é usada pelo gateway VPN para iniciar uma troca de transação do Mode-Config [PAP99] afim de autenticar o usuário. Após a conclusão bem sucedida da troca os participantes podem prosseguir usando a IKE SA para outros propósitos, como por exemplo um subseqüente *Quick Mode*.

Descrição do modo de Autenticação Híbrida

O modo de autenticação híbrida é dividido em dois estágios. O primeiro estágio é uma troca da Fase 1 usada para autenticar o gateway VPN. A troca segue a mesma estrutura e regras descritas pelo IKE [HC98] com algumas exceções, como será descrito nas subseções seguintes. A troca da Fase 1 usa tanto o *Aggressive Mode* como o *Main Mode*. O iniciador da Fase 1 pode ser tanto o cliente quanto o gateway VPN. Já o iniciador da troca de transação do Mode-Config que se segue deve ser sempre o gateway VPN.

A Fase 1 deve ser imediatamente seguida por uma troca de transação cujo iniciador é o gateway VPN. A troca de transação deve ser protegida pela IKE SA negociada na Fase 1 precedente. Esta IKE SA não deve ser usada por nenhuma outra troca antes da troca de transação terminar com sucesso e , conseqüentemente, o usuário ser autenticado. Se a autenticação do usuário falhar a IKE SA deve ser encerrada.

Há duas características que identificam unicamente um método de autenticação híbrida. A primeira é a direção da autenticação. A segunda determina o método de autenticação usado para autenticar o gateway VPN.

Considerações de segurança

O nível de segurança provido por esse protocolo, conta entre outras coisas, com a força do mecanismo de autenticação usado para autenticar o cliente.

Apesar da autenticação por chave pré-compartilhada para usuários móveis poder ser feita somente no *Aggressive Mode*, revelando assim a identidade do usuário, estes métodos propostos provêem, quando usados em conjunto com o *Aggressive Mode*, proteção da identidade do usuário e quando usados em conjunto com o *Main Mode*, provêem proteção da identidade de ambas as partes.

Apesar do uso de senhas fixas ser uma prática altamente desencorajada, estes métodos possuem uma vantagem sobre o método de chave pré-compartilhada, pois a senha não tende a sofrer ataques de dicionário offline, já que ela é cifrada usando uma derivação da chave compartilhada Diffie-Hellman, e somente os participantes do protocolo IKE conhecem essa chave.

Quando se usa os métodos padrões de autenticação do IKE, ambas as partes podem e devem detectar ataques de man-in-the-middle. Quando se usa autenticação híbrida para estabelecer uma IKE SA com autenticação unidirecional, somente o cliente pode e deve detectar este tipo de ataque.

O método de autenticação híbrida não provê proteção contra ataques de negação de serviço nos quais um atacante, personificando um usuário, repetidamente tenta se autenticar, eventualmente causando a revogação da conta do usuário. Apesar de tudo, este tipo de vulnerabilidade é inerente à técnica de desafio/resposta e não deve ser considerada uma falha deste protocolo e sim do método de autenticação utilizado.

5.1.3 IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK)

O IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) [HKP99] é um mecanismo proposto ao IETF que descreve uma nova troca baseada no IKE, originalmente concebido pela antiga empresa Network Alchemy, hoje Nokia. Tal troca tem como objetivo prover autenticação quando um dos lados da comunicação está utilizando uma técnica de autenticação unidirecional como o RADIUS, SecurID ou OTP (*One-Time Password*), comumente chamados de métodos de autenticação legada.

O protocolo CRACK deve ser usado como uma troca da Fase 1 do IKE, onde o resultado desta troca é uma associação de segurança IKE mutuamente autenticada. As chaves resultantes desta SA também são mutuamente autenticadas, o que estende essa propriedade a qualquer SA criada a partir dela para qualquer outro serviço de segurança, como o IPSec [Pip98].

Novos Payloads

A especificação do protocolo CRACK define dois novos payloads para transportar as informações de autenticação. O primeiro, denominado "Raw Public Key Payload", é usado para transportar uma chave pública não autenticada. Já o segundo, chamado "Challenge/Response Payload", é usado para transportar um desafio do gateway para o cliente e também é usado pelo cliente para responder ao desafio do gateway. O Challenge/Response Payload contém atributos denotando informações específicas enviadas do cliente para o gateway VPN e vice-versa. O método de autenticação legada escolhido determinará o conteúdo específico deste payload. Cada um desses payloads é constituído pelo cabeçalho genérico ISAKMP [MMS98] e por um payload específico cujo tamanho não é fixo.

Considerações de segurança

O canal resultante da troca das primeiras duas mensagens pode ser considerado seguro devido ao fato do gateway VPN assinar sua chave pública Diffie-Hellman. O cliente, no entanto, não assina sua chave pública Diffie-Hellman. Assim, do ponto de vista do cliente o canal está protegido porque ele tem certeza de que o gateway VPN é o proprietário da chave pública Diffie-Hellman recebida. Do ponto de vista do gateway VPN, o canal está protegido porque o cliente não enviará informações sensíveis caso um ataque de man-in-the-middle seja detectado.

5.1.4 Pre-IKE Credential Provisioning Protocol (PIC)

O Pre-IKE Credentials Provisioning Protocol (PIC) [SKA02] é um método proposto ao IETF com o objetivo de fornecer autenticação IPSec através de um Servidor de Autenticação (*Authentication Server* - AS) e usar mecanismos de autenticação legada.

O PIC é realizado em uma etapa anterior à execução do IKE, onde a máquina cliente se comunica com um servidor de autenticação (AS) usando um protocolo de troca de chaves onde somente o servidor é autenticado, e as chaves derivadas são usadas para proteger a autenticação do usuário. Após o usuário ter se autenticado, a máquina cliente obtém do AS credenciais, que podem ser mais tarde usadas para autenticar o cliente em uma troca IKE padrão, sem a intervenção do usuário. A troca de chaves proposta é baseada no ISAKMP, semelhante a uma troca IKE simplificada e a autenticação do usuário é suportada através do uso do *PPP Extensible Authentication Protocol* (EAP)[1] [BV98].

[1]O EAP é um protocolo de autenticação geral, projetado para permitir múltiplas formas de autenticação. Ele permite que um servidor qualquer repasse mensagens de autenticação para um servidor de autenticação, agindo como um proxy, e também possibilita que aquele servidor analise os pacotes para determinar se a autenticação foi bem sucedida.

Uma nova abordagem

Existem várias propostas com o objetivo de integrar a autenticação legada diretamente no IKE, tais como o XAUTH [PB99], a Autenticação Híbrida [LSZ00], e o CRACK [HKP99]. No entanto, esses mecanismos definem novos modos de autenticação para o IKE, uma abordagem que é evitada pelo IPSRA Working Group.

Recentemente, Bellovin e Moskowitz [BM00] propuseram uma abordagem alternativa, que realiza a tarefa de autenticação legada em um servidor separado, chamado um Servidor de Autenticação (*Authentication Server* - AS), e que, após a autenticação do usuário, fornece à máquina cliente credenciais que permitem a autenticação IKE padrão. Tal processo consiste de uma primeira fase onde a máquina cliente entra em contato com o AS para receber credenciais aceitáveis pelo IKE, como um certificado de chave pública ou uma chave compartilhada, e uma segunda fase na qual a máquina cliente entra em contato com o gateway VPN e usa estas credenciais em uma execução normal do IKE para estabelecer uma associação de segurança.

Apesar dessa abordagem necessitar de um grande número de trocas de mensagens antes de uma associação IPSec ser estabelecida por envolver a interação com o AS em adição à interação normal sobre o IKE, ela é a solução mais viável para os requisitos do IPSRA de não alterar o IKE e não adicionar novos modos a ele.

Esta abordagem baseada em um AS separado traz vários benefícios:

- O gateway VPN pode implementar somente o IPSec/IKE, sem se preocupar com a autenticação do usuário. Isso possibilita que o mesmo gateway seja utilizado tanto em organizações baseadas em ICP quanto em organizações baseadas em mecanismos de autenticação legada.

- A transição das soluções implementadas baseadas em métodos legados, através de um AS separado, para uma autenticação mais escalável baseada em ICP suportada pelo IKE é direta, bastando eliminar a fase do AS.

- Um ataque de negação de serviço no AS não pode comprometer conexões existentes do gateway VPN, minimizando assim os danos causados por esses ataques.

- O AS pode ou não ser colocado na mesma máquina que o gateway VPN. Um AS separado alivia a carga do gateway VPN mas pode envolver um custo adicional.

O protocolo PIC se baseia nesta abordagem e a protege usando mecanismos simplificados do ISAKMP e do IKE. O protocolo introduz mensagens EAP (*Extensible Authentication Protocol*) [BV98] em payloads ISAKMP para suportar múltiplas formas de autenticação de usuário. Uma vez que a autenticação do usuário tenha sido bem sucedida, a

máquina cliente obtém do servidor de autenticação (AS) credenciais que podem ser usadas mais tarde pelo cliente para realizar uma autenticação IKE regular com um gateway VPN. A especificação do protocolo PIC define várias formas de credenciais e pode ser estendido para suportar outras.

É importante enfatizar que o PIC não requer modificações no IKE, ao contrário dos demais mecanismos apresentados nas seções anteriores. Ao invés disso ele usa elementos simplificados do ISAKMP e do IKE para atingir um objetivo muito menos ambicioso do que o objetivo do IKE, o provimento de credenciais para usuários autenticados com sucesso. O uso direto do IKE reduz a complexidade e contribui para a eficiência do protocolo.

Visão geral do Protocolo PIC

Os quatro estágios principais do protocolo PIC são:

1. Uma etapa opcional de mensagens provê proteção parcial do AS a ataques de negação de serviço (DoS), verificando se o iniciador da troca é alcançável pelo endereço IP de origem apresentado. Isto é feito antes de qualquer consumo significativo dos recursos de CPU ou memória do AS.

2. O protocolo estabelece um canal de autenticação do cliente para o AS, no qual somente o servidor é autenticado.

3. A autenticação do usuário é realizada sobre este canal seguro. As informações de autenticação do usuário são transportadas usando o EAP [BV98] tunelado dentro do ISAKMP.

4. O AS envia ao cliente um credencial, geralmente de curto prazo, que pode ser usada em trocas IKE subseqüentes. Esta credencial pode ser vista como um certificado, ou uma chave privada gerada ou armazenada pelo AS e acompanhada pelo certificado correspondente. Pode ser também uma chave simétrica, ou uma informação para a derivação de tal chave.

Para minimizar o número de mensagens trocadas no PIC, os diferentes estágios compartilham mensagens, e o protocolo toma o cuidado de garantir a segurança do quarto estágio, mesmo que ele seja iniciado quando o cliente ainda não tenha sido autenticado.

PIC e ISAKMP

O PIC é baseado no ISAKMP [MMS98] e no ISAKMP IPSec DOI [Pip98], com algumas pequenas adições.

A SA criada durante a primeira troca do PIC não deve ser usada para qualquer outra mensagem que não seja as próprias mensagens deste protocolo, e deve ser destruída após a conclusão do mesmo.

Considerações de segurança

O protocolo PIC autentica o usuário, e não a máquina da qual o usuário está se conectando. Assim o AS é incapaz de tomar decisões de política referentes à segurança da máquina cliente.

O PIC consiste em quatro estágios lógicos. O primeiro estágio tem por objetivo prover alguma proteção contra ataques DoS. Ele utiliza uma abordagem adaptativa sugerida no Oakley [Orm98] onde a aplicação deste mecanismo é deixada a critério do servidor.

Uma vez completado o segundo estágio do protocolo, o cliente autenticou o AS e tem total confiança no mesmo, para os propósitos de provimento de credenciais. Assim não é necessário validar as credenciais recebidas.

Dado que a troca no segundo estágio é protegida com Perfect Forward Secrecy[2] (PFS), via Diffie-Hellman, todos os dados cifrados no protocolo, incluindo os dados de autenticação do usuário, estão protegidos contra o comprometimento da chave tão logo esta chave, e suas chaves derivadas, tenham sido seguramente apagadas da memória do computador.

5.1.5 Conclusão

Existem diversas propostas com o objetivo de integrar a autenticação legada diretamente no IKE, tais como o XAUTH, a Autenticação Híbrida, e o CRACK.

O XAUTH provê apenas autenticação unidirecional, sendo portanto extremamente dependente dos mecanismos de autenticação bidirecional da Fase 1 do IKE. A remoção ou o enfraquecimento da autenticação na Fase 1 torna a sessão IPSec suscetível a ataques de man-in-he-middle e ataques de spoofing.

Além disso, quando utilizado com chaves pré-compartilhadas, em cenários onde o sistema do cliente remoto possui um endereço IP dinâmico, o *Main Mode* do IKE não pode ser utilizado, diminuindo significativamente o nível de segurança desta solução. Tal solução também é limitada à utilização de uma única chave pré-compartilhada para todos os clientes remotos, o que torna essa chave fortemente suscetível a ataques de engenharia social.

[2]O termo Perfect Forward Secrecy (PFS) se refere à propriedade de garantir que o comprometimento de uma única chave permitirá acesso somente aos dados protegidos por aquela chave. Para a existência de PFS a chave usada para proteger uma transmissão de dados não deve ser usada para derivar qualquer chave adicional.

A Autenticação Híbrida é um mecanismo que combina o XAUTH com os mecanismos existentes do IKE, a fim de prover uma autenticação bidirecional, porém assimétrica. Isto é feito através da inserção de um novo método de autenticação no IKE, onde em uma etapa inicial, durante a Fase 1 do IKE o gateway VPN se autentica perante o cliente remoto, e em uma etapa seguinte, após a conclusão da Fase 1, o XAUTH é utilizado para autenticar o cliente perante o gateway VPN.

O CRACK é um mecanismo que provê a mesma funcionalidade da autenticação híbrida, através da inserção de um novo método de autenticação no IKE. A principal diferença entre esses dois mecanismos é que, no CRACK, todas as etapas da autenticação, tanto do gateway VPN quanto do cliente, são realizadas durante a Fase 1 do IKE. Como conseqüência, a IKE SA estabelecida por ele ao final da Fase 1 possui autenticação bidirecional, enquanto que na autenticação híbrida ela é apenas unidirecional, dependendo ainda de uma autenticação unidirecional provida pelo XAUTH para prover bidirecionalidade na autenticação.

Esses mecanismos, no entanto, definem novos modos de autenticação para o IKE, uma abordagem que é evitada pelo *IPSRA Working Group*. Além disso, eles implicam, mesmo que em um grau reduzido, em uma complexidade adicional agregada a este protocolo.

O protocolo PIC, ao contrário dos demais, provê a mesma funcionalidade que a autenticação híbrida e o CRACK, sem no entanto requerer modificações no IKE. Tal fato o coloca em uma posição privilegiada em relação às exigências impostas pelo IPSRA Working Group, para prover interoperabilidade com os mecanismos de autenticação legada existentes, mostrando ser esta a solução mais adequada para atender a este requisito.

5.2 Configuração do sistema remoto

Em muitos cenários de acesso remoto VPN, a presença virtual da máquina remota na rede privada, proporcionada pela atribuição de um "endereço IP virtual" ao sistema remoto, pode trazer uma série de vantagens em relação ao controle de acesso e a implementação das políticas de segurança sobre o tráfego originado pelos clientes VPN.

Essa presença virtual pode ser conseguida através do provimento de parâmetros de configuração de rede, como endereço IP, servidores DNS, servidores WINS, além de outros, ao sistema remoto, realizando em seguida o tunelamento de todo o tráfego desse sistema até o gateway VPN através do IPSec.

A seguir serão apresentadas e discutidas as principais soluções para a configuração do sistema remoto em ambientes de acesso remoto VPN.

5.2.1 ISAKMP Configuration Method (Mode-Config)

O ISAKMP Configuration Method [PAP99], também conhecido como Mode-Config, é um mecanismo proposto ao IETF que se baseia no protocolo ISAKMP. Sua função é prover, durante o estabelecimento de uma ISAKMP SA, informações necessárias à configuração do outro extremo do túnel IPSec.

Tendo sido originalmente desenvolvido pela Cisco e posteriormente proposto ao IETF, rapidamente se tornou uma solução popular de mercado incorporada a diversos produtos VPN. Apesar de não atender perfeitamente aos requisitos do *IPSRA Working Group*, pelo fato de exigir modificações no atual padrão do IKE, suas características têm conduzido à sua inclusão oficial na proposta do protocolo IKEv2 [Kau03] sendo especificado atualmente pelo *IPSec Working Group* do IETF, para ser o substituto do atual protocolo.

A especificação do Mode-Config define um novo modo de troca incorporado ao protocolo ISAKMP. É baseado nesta nova troca, denominada "*Transaction Exchange*", que se realiza todo o processo de configuração.

Transaction Exchange

A *Transaction Exchange* é semelhante à "*Information Exchange*" descrita na especificação dos protocolos ISAKMP [MMS98] e IKE [HC98], porém permite uma transação multi-troca ao invés de uma transmissão de informação de forma única.

Uma *Transaction Exchange* é definida como duas trocas de configuração, a primeira sendo ou um `Set` ou um `Request` e a segunda sendo ou um `Acknowledge` ou um `Reply`, respectivamente.

Existem dois paradigmas a serem seguidos para este método:

- `Request/Replay:` permite a uma máquina requisitar informação de um gerenciador de configuração. Se os atributos na mensagem `Request` não são vazios, então eles são tidos como uma sugestão. A mensagem de `Replay` pode escolher tais valores, ou retornar novos valores. Ela pode também adicionar novos atributos e não incluir algum anteriormente requisitado.

  Um `Reply` deve sempre ser enviado quando um `Request` for recebido, mesmo que seja um Replay vazio ou que haja atributos esperados no `Request`. Isto significa meramente que os atributos requisitados não estavam disponíveis ou eram desconhecidos.

- `Set/Acknowledge:` permite a um gerenciador de configuração, tipicamente uma máquina que deseja enviar informação para outra máquina, iniciar a transação de configuração. O código `Set` envia atributos que se deseja alterar no outro extremo da comunicação. O código `Acknowledge` deve retornar atributos de comprimento

zero indicando que os aceitou. Aqueles atributos que não foram aceitos não serão enviados de volta na mensagem de `Acknowledge`.

As transações são completadas uma vez que o código `Replay` ou o `Acknowledge` tenha sido recebido. Caso ele não seja recebido, a implementação pode desejar retransmitir a troca original.

O *initiator* e o *responder* não são necessariamente os mesmos *initiator* e *responder* da troca ISAKMP.

Requisitando um endereço interno

Esse mecanismo provê a alocação de um endereço para um sistema remoto tentando estabelecer um túnel com uma rede privada através de um gateway VPN. A máquina remota requisita um endereço e opcionalmente outras informações a respeito da rede privada. O gateway VPN obtém um endereço da rede interna para a máquina remota de uma fonte qualquer, como um servidor DHCP ou de sua própria faixa de endereços reservados para este propósito.

Todos os valores retornados serão dependentes da implementação. O gateway VPN pode também enviar outros atributos que não foram incluídos no `Request` e pode ignorar os atributos que ele não suporta.

Esta *Transaction Exchange* deve ocorrer após o estabelecimento da Fase 1 do IKE e antes de uma Fase 2 ter sido iniciada, já que esta última negociação requer um endereço interno.

Requisições de endereço subseqüentes podem ser feitas sem a negociação da Fase 1, quando já existir uma ISAKMP SA estabelecida.

Considerações sobre o gerenciamento de endereços

O método definido pelo Mode-Config não deve ser usado para o gerenciamento em larga escala. Seu principal objetivo é prover um mecanismo próprio para troca de informação dentro do IPSec. Apesar de poder ser útil utilizar tal mecanismo de troca de informação para alguma redes pequenas e máquinas fora do escopo do IPSec, os protocolos de gerenciamento existentes tais como DHCP [Dro97], RADIUS [RRSW97], SNMP ou LDAP [WHK97] devem ser considerados para o gerenciamento de endereços de redes bem como para as trocas de informação subseqüentes.

5.2.2 DHCP sobre IPSec

O protocolo DHCP sobre IPSec [PAKG03] é uma solução recentemente padronizada pelo IETF, que se utiliza das funcionalidades do protocolo DHCP (*Dynamic Host Confi-*

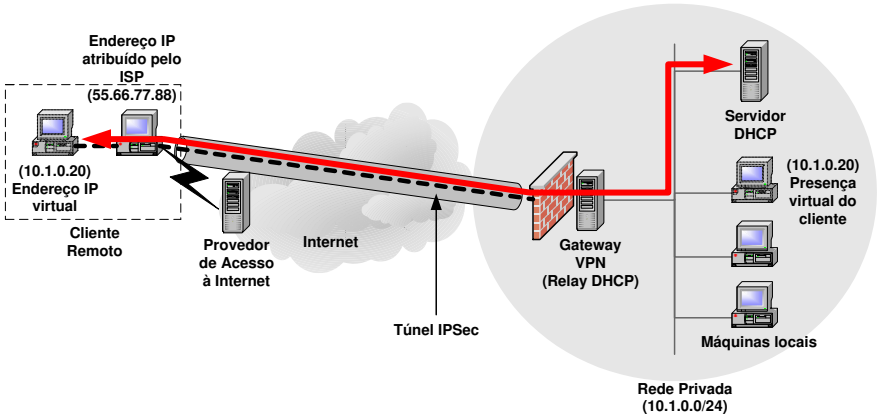


Figura 5.1: DHCP utilizado sobre o túnel IPSec

guration Protocol) [Dro97] para prover as configurações necessárias a um sistema remoto através de um túnel IPSec [KA98c], sem no entanto exigir quaisquer modificações nos protocolos existentes.

Este processo é realizado em várias etapas. Inicialmente um máquina remota na Internet estabelece um túnel IPSec com o gateway VPN. A máquina remota, então, interage através do túnel IPSec com um servidor DHCP, que provê ao sistema remoto um endereço pertencente ao espaço de endereçamento da rede interna, como mostrado na Figura 5.1. A partir deste ponto, ela usa o endereço recebido como endereço de origem para todas as interações com os recursos da rede privada. Isto significa que o gateway VPN continua a reconhecer a legitimidade da máquina e seu endereço IP público, atribuído pelo provedor de acesso à Internet (ISP) ou obtido de qualquer outra forma, como o ponto final do túnel. Do ponto de vista da rede privada, a identidade virtual assumida pela máquina remota aparece como se este sistema estivesse situado atrás de uma outra máquina, que age como um gateway VPN, cujo endereço é o endereço IP público originalmente atribuído pelo ISP. Assim, todo o tráfego entre a máquina remota e a rede privada será transportado sobre o túnel IPSec criado.

Uma configuração típica da máquina remota para esse tipo de utilização seria usar dois endereços: uma interface para conexão com a Internet, e uma interface virtual para conexão com a rede privada. O endereço IP da interface de Internet e da interface virtual são usados no cabeçalho externo e interno do modo túnel IPSec, respectivamente.

Processo de configuração

A configuração da interface virtual da máquina remota é realizada nas seguintes etapas:

1. A máquina remota estabelece uma associação de segurança IKE com o gateway

VPN através do *Main Mode* ou do *Aggressive Mode*. Esta ISAKMP SA então serve para proteger as IPSec SAs adicionais que serão criadas através do *Quick Mode*.

2. A máquina remota estabelece uma DHCP SA com o gateway VPN através do *Quick Mode*. A DHCP SA é uma IPSec SA em modo túnel estabelecida para proteger o tráfego DHCP inicial entre o gateway VPN e a máquina remota. A DHCP SA deve ser utilizada somente para o tráfego DHCP.

3. Mensagens DHCP são trocadas entre a máquina remota e o servidor DHCP, protegidas pela DHCP SA estabelecida na etapa anterior entre a máquina remota e o gateway VPN. Após a negociação DHCP se completar, a interface virtual da máquina remota obtém um endereço IP, bem como outros parâmetros de configuração necessários.

4. A máquina remota pode requisitar o encerramento da DHCP SA, já que as futuras mensagens DHCP serão transportadas sobre um novo túnel IPSec, estabelecido na etapa seguinte. Alternativamente, a máquina remota e o gateway VPN podem continuar a usar a mesma SA para todo o tráfego subseqüente adicionando seletores SPD temporários.

5. Se um novo túnel IPSec for necessário, a máquina remota estabelece uma IPSec SA em modo túnel com o gateway VPN através do *Quick Mode*. Neste caso, o novo endereço atribuído através do DHCP deve ser usado no *Quick Mode*.

Ao fim da última etapa, a máquina remota está pronta para se comunicar com a rede privada usando um túnel IPSec. Todo o tráfego IP, incluindo futuras mensagens DHCP, serão agora tunelados sobre esta IPSec SA em modo túnel.

Processamento das mensagens DHCP

O processo de configuração da interface virtual se inicia com o envio de uma mensagem DHCPDISCOVER, que é tunelada para o gateway VPN usando a DHCP SA, onde a máquina remota procura descobrir quais são os servidores DHCP disponíveis.

Em seguida, o servidor DHCP envia uma mensagem de DHCPOFFER, em resposta ao DHCPDISCOVER, contendo uma oferta dos parâmetros de configuração.

Após a interface de Internet ter recebido a mensagem DHCPOFFER, ela a repassa para a interface virtual, após o processamento IPSec. A interface virtual responde com uma mensagem DHCPREQUEST, requisitando os parâmetros oferecidos pelo servidor.

O servidor DHCP então responde com uma mensagem DHCPACK, em caso de sucesso, ou DHCPNAK, em caso de falha, que é encaminhada pelo gateway VPN através da DHCP

SA. A interface de Internet da máquina remota encaminha a mensagem DHCPACK ou DHCPNACK para a interface virtual após o processamento IPSec.

Após o recebimento do DHCPACK, a interface virtual estará configurada e a interface de Internet pode agora estabelecer uma nova IPSec SA em modo túnel com gateway VPN, utilizando o novo endereço recebido. A máquina remota pode também encerrar a DHCP SA, pois todas as futuras mensagens DHCP enviadas pelo cliente, incluindo as mensagens DHCPREQUEST, DHCPINFORM, DHCPDECLINE, e DHCPRELEASE, usarão o nova SA estabelecida. Similarmente, todas as mensagens DHCP subseqüentes enviadas pelo servidor DHCP serão encaminhadas pelo gateway VPN, agindo como um Relay DHCP, através da IPSec SA em modo túnel, incluindo as mensagens DHCPOFFER, DHCPACK e DHCPNAK.

Comportamento do Relay DHCP

Apesar de outras configurações serem possíveis, o servidor DHCP tipicamente não reside na mesma máquina que o gateway VPN, que deverá então agir como um Relay DHCP. Neste caso, o gateway VPN repassa pacotes entre o cliente e o servidor DHCP, mas não requisita ou renova endereços em nome do cliente.

Como os Relays DHCP não mantêm estados, o gateway VPN deve inserir informações apropriadas na mensagem DHCP antes de repassar a um ou mais servidores DHCP. Isto permite ao gateway VPN rotear a mensagem de DHCOFFER correspondente, de volta à máquina remota, no túnel IPSec correto, sem ter de manter em uma tabela a informação de estado obtida na mensagem DISCOVER.

Considerações de segurança

Este protocolo é protegido usando os mecanismos de segurança do IPSec, e como resultado os pacotes DHCP trocados entre a máquina remota e o gateway de segurança possuem proteção em relação à confidencialidade, autenticação e à integridade.

Contudo, como o gateway VPN age como um Relay DHCP, nenhuma proteção é aplicada aos pacotes DHCP no caminho entre o gateway VPN e o servidor DHCP, a menos que seja usada a autenticação do próprio DHCP [DA01]. Contudo, a autenticação DHCP não pode ser usada como um mecanismo de controle de acesso eficaz, pois se baseia em informações presentes nos datagramas IP que podem ser facilmente modificadas com o uso de técnicas de spoofing.

Como resultado, a segurança não deve depender da atribuição de endereço. Ao invés disso, o gateway VPN pode usar outras técnicas tais como a instanciação de filtros de pacotes ou seletores *Quick Mode* em um controle por túnel.

Diversos problemas podem surgir durante o repasse de requisições de clientes DHCP

de fontes não confiáveis. Isto inclui os ataques de exaustão DHCP, e spoofing das opções `client identifier` ou `client MAC address`. Estes problemas podem ser parcialmente tratados através do uso da opção `DHCP Relay Agent Information` [Pat01b].

Deve ser possível configurar a máquina remota para encaminhar todo o tráfego de Internet através do túnel. Apesar disto adicionar um atraso de comunicação entre a máquina remota e a Internet, também provê alguma segurança adicional, de forma que o firewall pode agora filtrar o tráfego proveniente da máquina remota como se ela estivesse fisicamente localizada na rede interna.

5.2.3 Conclusão

Dentre os mecanismos propostos para realizar a configuração do sistema remoto em cenários de acesso remoto VPN, dois merecem atenção especial: o Mode-Config e o DHCP sobre IPSec.

O Mode-Config define uma nova troca incorporada ao protocolo ISAKMP através da qual se realiza todo o processo de configuração. O fato de adicionar extensões ao protocolo ISAKMP, e conseqüentemente exigir modificações no atual padrão do IKE, faz com que esta solução conflite com os requisitos apresentados pelo *IPSRA Working Group* para a adoção de um mecanismo padrão.

Além disso, a adição de novas funcionalidades a um protocolo de segurança como o IKE, pode aumentar consideravelmente a complexidade deste protocolo, podendo eventualmente afetar o nível de segurança oferecido por ele, além de trazer problemas de incompatibilidade entre diferentes implementações.

Contudo, suas características o tornam um forte candidato à inclusão na proposta do protocolo IKEv2, sendo atualmente especificado pelo IETF.

Já o DHCP sobre IPSec, um mecanismo que se baseia no uso do protocolo DHCP sobre túneis IPSec, não exige quaisquer modificações no atual padrão do IKE, atendendo perfeitamente aos requisitos do *IPSRA Working Group*. Isto fez com que ele se torna-se recentemente o mecanismo padrão do IETF para a configuração de sistema remotos.

Outra vantagem deste mecanismo em relação ao Mode-Config, é a flexibilidade que ele oferece em relação aos parâmetros de configuração. Experiências anteriores com mecanismos de configuração similares como o PPP IPCP (*PPP Internet Protocol Control Protocol*) [McG92] mostraram que não é viável suportar meramente um conjunto mínimo de configurações.

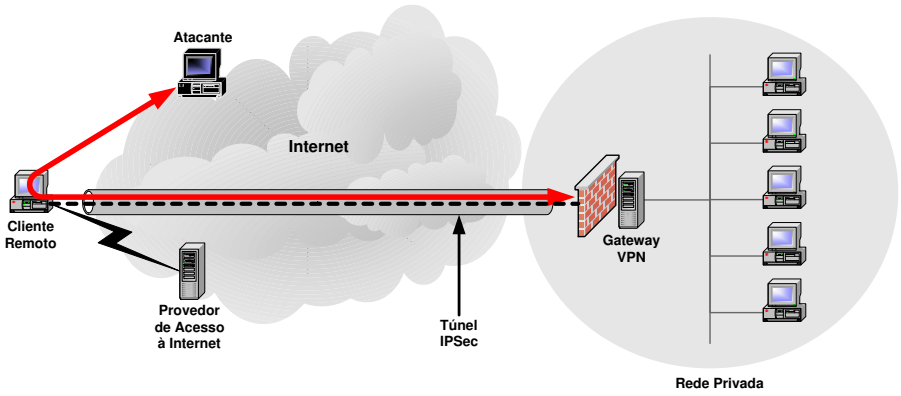


Figura 5.2: Cliente remoto como ponte para a rede privada

5.3 Configuração da política de segurança

Uma preocupação existente durante o planejamento do acesso remoto VPN é a extensão do perímetro de segurança da rede privada. Ao permitir acesso à rede interna através da VPN, uma máquina potencialmente não-confiável estará ganhando acesso à rede protegida.

É importante ressaltar que a VPN oferece uma conectividade segura entre a máquina do cliente e a rede corporativa, não oferecendo características pessoais de segurança ao sistema cliente, ou proteção contra ataques de fontes externas como a Internet. A conexão VPN existe para fornecer a confidencialidade e a integridade dos dados bem como serviços de autenticação.

Sendo assim, o comprometimento da máquina remota pode permitir que um atacante utilize esse sistema como meio de entrada para a rede corporativa. Neste caso, a segurança da rede privada dependerá de se evitar que o sistema remoto sirva como ponte para um ataque vindo da Internet, como ilustrado na Figura 5.2. Tal ataque pode ser ao vivo, com a conexão ao gateway VPN estabelecida, ou mesmo off-line, após contaminação da máquina remota por um vírus, worm ou cavalo-de-tróia (*trojan horse*) [NdG02] adequado para os fins do ataque.

Como muitos, se não a maioria dos usuários, tomam poucas medidas de segurança, quando conectados à Internet eles se tornam um alvo muito mais fácil do que a rede privada. Um computador desprotegido pode estar vulnerável a diversas ameaças, como coleta de senhas, infecção por vírus ou worms, e até desconhecidamente servir como ponto para um ataque de negação de serviço distribuído (DDoS), que poderia ter efeitos adversos se introduzido na rede privada através da conexão VPN.

Para reduzir a exposição da rede privada, diversas precauções e imposições devem estar presentes na política de segurança da organização. A política de segurança deve

abordar por exemplo o tempo máximo permitido para uma sessão VPN, e garantir que uma sessão seja encerrada após um período prescrito de tempo inativo decorrido. Isto seria particularmente interessante para os casos de usuários remotos com acesso de banda larga à Internet, devido à natureza permanente da conexão.

A fim de diminuir a exposição da rede corporativa às ameaças de origem externa, um grande número de questões devem ser consideradas, em torno das quais a política de segurança deve se basear. As áreas de interesse em relação ao cliente VPN que devem ser abrangidas incluem: os perigos potenciais da natureza permanente das conexões Internet de banda larga, a instalação de firewalls pessoais e softwares anti-vírus, e até o próprio equipamento do usuário remoto.

5.3.1 O cliente VPN e a política de segurança

A análise do aspectos de segurança envolvendo o cliente VPN começa com as considerações feitas ao próprio equipamento utilizado pelo usuário remoto.

Devido às dificuldades de se garantir algum nível de segurança física razoável em relação a esses equipamentos, é recomendável que a política de segurança estabeleça que a máquina cliente seja um equipamento de propriedade da própria organização, preferencialmente em relação a equipamentos de propriedade pessoal dos usuários. Isto minimiza os problemas associados à utilização do equipamento para fins pessoais, resultando possivelmente em uma maior exposição deste sistema. Assim é mais fácil garantir que o usuário cumpra a política de segurança, eventualmente restringindo que o equipamento seja usado somente para fins profissionais.

Caso o equipamento seja de propriedade da companhia, é possível também garantir que os usuários não tenham privilégios de super-usuário, ou administrador, em suas máquinas. Controlar a atividade do usuário, além de verificar e manter a integridade do sistema operacional é uma tarefa muito difícil, se não impossível, quando os usuários possuem o controle total sobre os privilégios de super-usuário. Isto também serve para minimizar as tarefas de gerenciamento, pois a configuração do sistema deve permanecer relativamente estática, sem instalações de software não autorizado, mudanças de configuração do usuário ou conflitos de dispositivos.

Um outro item de extrema importância que deve ser abordado pela política de segurança é a instalação e revisão periódica das atualizações de segurança apropriadas no sistema remoto. Isto porque grande parte dos ataques realizados atualmente são baseados na exploração de vulnerabilidades específicas em aplicativos, sistemas operacionais e protocolos, no nível de aplicação [NdG02].

5.3.2 Anti-vírus e firewall pessoal

A fim de garantir a integridade do sistema remoto, a política de segurança deve estabelecer o uso obrigatório de um software anti-vírus e um firewall pessoal neste sistema, operando e usando os arquivos de configuração mais atuais.

A solução ideal deve se basear em pacotes de anti-vírus gerenciáveis, reduzindo assim a responsabilidade do usuário remoto. Existem diversas soluções comerciais que atendem a esses requisitos, desenvolvidas pelos principais fabricantes de anti-vírus do mercado como McAfee, Symantec e Trend Micro, entre outros.

O uso de uma solução de anti-vírus gerenciável permite a existência de um único ponto de administração e monitoração, possibilitando um gerenciamento mais eficiente dos clientes remotos. Nesses produtos, um console central permite que o administrador controle políticas e mantenha os usuários e as estações de trabalho atualizados e configurados corretamente.

Um produto de anti-vírus gerenciável permite também que o administrador proteja as configurações do cliente para impedir que os usuários modifiquem a configuração prescrita. Caso seja detectada a presença de um vírus no sistema remoto, ele será automaticamente reparado e o console central alertado.

A política de segurança também deve exigir o uso de um firewall pessoal, em adição a um produto de anti-vírus. Tal como os softwares anti-vírus, vários produtos de firewall pessoal de qualidade estão disponíveis no mercado, desenvolvidos por empresas como a Zone Labs, Sygate e Symantec, entre outros. Apesar da maioria dos softwares anti-vírus reduzirem problemas relacionados a presença de vírus e worms no cliente, eles não protegem contra ameaças desconhecidas ou atacantes habilidosos.

O uso de um firewall pessoal permite o acesso somente aos recursos necessários, bloqueando tentativas de acesso não autorizadas. Alguns produtos de firewall pessoal monitoram também o tráfego de saída baseado no processo que o originou, permitindo que somente aplicações confiáveis acessem a Internet. Este tipo de software constitui uma excelente opção para as exigências da política de segurança.

É importante evidenciar que a ausência de um firewall pessoal no cliente VPN, expõe não somente as informações armazenadas no próprio cliente, como toda a estrutura de segurança da rede privada. Isto porque durante a existência de um túnel VPN com a rede privada, o cliente remoto passa a ser um prolongamento da rede lógica da organização.

Tal como os produtos de anti-vírus, existem também diversas opções de firewalls pessoais gerenciáveis, sendo a adoção destes altamente recomendada para uma solução ideal.

Um bom exemplo de firewall pessoal gerenciável é o Zone Labs Integrity, desenvolvido pela empresa Zone Labs. O Zone Labs Integrity consiste em um agente que reside na máquina do cliente, e um servidor, um ponto central de gerência que permite que o administrador crie, monitore e reforce a política de segurança a partir de um console

central. Além de servir como um firewall pessoal, este software serve para reforçar a segurança da rede se comunicando com um equipamento Cisco VPN 3000 Concentrator, um gateway VPN fabricado pela Cisco, para garantir que somente clientes VPN dentro dos padrões de segurança sejam autenticados e tenham acesso permitido à rede corporativa.

5.3.3 Conexões de banda larga

O tipo de conexão com a Internet utilizado pelo clientes VPN é um fator importante a ser considerado na criação de uma política de segurança. Como a disponibilidade do acesso de banda larga à Internet é crescente e os preços tornam-se cada vez mais competitivos, é normal que um grande número de usuários utilizem cada vez mais conexões de banda larga para o acesso remoto à rede da corporação.

A maior largura de banda disponível, unido ao fato do cliente de banda larga possuir uma conexão permanente e um endereço IP estático, ou que mude com pouca freqüência, fazem com que ele esteja mais exposto a ataques do que um cliente dial-up. Por isso, é imperativo ao cliente de banda larga ter um software anti-vírus e um firewall pessoal atualizados e executando todo o tempo.

Devido à natureza permanente do acesso de banda larga, a política de segurança pode também estabelecer que os clientes desliguem suas máquinas quando não estiverem em uso. Não exclusivo ao acesso de banda larga, a política de segurança deve também limitar o tempo de inatividade de uma sessão VPN. Isto serve para impedir que o usuário VPN se conecte à rede corporativa e deixe a sessão aberta e desacompanhada por um período de tempo prolongado.

Por fim, é importante que existam também formas de reforçar a política de segurança, devendo ser esta uma consideração preliminar durante todas as fases da pesquisa, do teste e da execução de qualquer tecnologia de segurança. A pesquisa cuidadosa, a revisão da documentação dos softwares utilizados e o teste da tecnologia podem servir para elaborar esses critérios. Sem um método de reforço, a eficácia da política de segurança é questionável.

A auditoria de rastros, a análise do equipamento e os registros de segurança devem ser revistos regularmente. Isto é um processo de tempo intensivo, porém é o único alerta sobre as violações e ameaças de segurança ocorridas. Sem os meios de reforço, a segurança da rede corporativa estará sendo colocada em risco, ao confiar que os usuários remotos voluntariamente cumprirão a política estabelecida. Como o perímetro de segurança da rede está sendo estendido para abranger o cliente VPN, a política de segurança deve ser reforçada em tempo real para proteger a integridade tanto do cliente VPN quanto da rede corporativa.

5.4 Passagem por intermediário

Em diversos cenários de acesso remoto VPN, é comum a existência de mecanismos de Tradução de Endereços de Rede (*Network Address Translation* – NAT) situados em uma posição intermediária entre o cliente remoto e o gateway VPN. Tais mecanismos inviabilizam o uso tradicional do protocolo IPSec nesses cenários, ao efetuarem alterações significativas no tráfego entre os extremos do túnel. Como conseqüência, as incompatibilidades entre NAT e IPSec têm constituído uma enorme barreira para o desenvolvimento do IPSec em uma de suas principais funcionalidades.

Nesta seção serão detalhados os problemas originados pela passagem de tráfego IPSec por um dispositivo intermediário de NAT, apresentando também uma solução que atende aos requisitos especificados pelo *IPSRA Working Group*, denominada NAT Traversal.

5.4.1 NAT Traversal (NAT-T)

O NAT Traversal (NAT-T) [KSHV03] é um mecanismo proposto ao IETF com o objetivo de solucionar os problemas surgidos em cenários onde um tráfego IPSec passa por um dispositivo de NAT. Esse mecanismo surgiu da combinação de dois trabalhos propostos por grupos distintos. Um preparado pela empresa SSH Communications, e o outro resultado de uma união de empresas como F-Secure, Microsoft, Cisco e Nortel. As duas propostas foram unidas para formar uma solução única após um encontro em março de 2001, pelo fato de ambas apresentarem muitos pontos em comum.

O NAT e o IPSec são extremamente problemáticos quando utilizados em conjunto sem uma forma padrão que ofereça um gerenciamento e interoperabilidade simples. O NAT-T é uma solução promissora, que apesar de introduzir novos conceitos, já é utilizada por muitos fabricantes de soluções VPN em seus produtos.

Tradução de Endereços de Rede (NAT)

A Tradução de Endereços de Rede (*Network Address Translation* – NAT) [EF94] é basicamente uma conversão aplicada aos endereços IP de origem e destino de um pacote IP.

Devido a uma possível escassez de endereços IPv4, este mecanismo foi desenvolvido para permitir que gateways, roteadores, firewalls, ou dispositivos intermediários em geral, pudessem realizar modificações nos datagramas IP em trânsito, substituindo endereços IPs privados [RMK+94] por endereços IP públicos [RMK+94] e vice-versa. Assim, toda uma rede com endereços IP privados pode acessar a Internet, desde que o endereço IP de origem dos pacotes de saída seja substituído pelo dispositivo de NAT por um endereço público, de forma que os pacotes modificados possam ser roteados apropriadamente. Da

mesma forma, o endereço IP de destino dos pacotes de chegada correspondentes deve ser substituído pelo endereço do destino final na rede privada.

Existem basicamente dois tipos de NAT: o NAT estático (*Static NAT*) e a Tradução de Endereço de Porta (*Port Address Translation* – PAT). Este último algumas vezes é chamado de Tradução de Endereço de Rede com multiplexação de Porta (*Network Address Port Translation* – NAPT).

O NAT estático é simplesmente a conversão direta, onde cada endereço IP privado é mapeado em um endereço IP público.

Já o NAPT provê um mapeamento de múltiplos endereços IP privados para um único endereço IP público. A porta de origem dos pacotes de saída é mapeada dinamicamente para uma porta disponível. Com isso, toda uma rede fica oculta atrás de um único endereço IP.

Alguns fabricantes também desenvolveram um terceiro método chamado *Pooled NAT*. Neste método o endereço IP privado é mapeado para um endereço pertencente a uma faixa de endereços IP pré-alocados. O dispositivo de NAT mantém uma tabela de tradução onde ele registra o endereço IP de origem e a porta de origem de um pacote de saída. Em seguida ele os substitui por um endereço IP e porta novos, e esses valores também são registrados nesta tabela. O pacote de retorno é comparado com esta tabela a fim de encontrar alguma entrada correspondente, e o endereço IP e o número da porta de destino são então substituídos apropriadamente.

Definição do problema

Um dos principais objetivos do IPSec é garantir a integridade dos pacotes, tentando prevenir qualquer modificação nos mesmos. No entanto, o mecanismo de NAT realiza modificações significativas no cabeçalho IP.

Tanto no modo transporte quanto no modo túnel, o AH autentica todo o datagrama IP. Ao contrário da autenticação do ESP, o AH também autentica o cabeçalho IP que o precede. Quando o NAT modifica o cabeçalho IP, o IPSec interpreta como uma violação de integridade e descarta o pacote. Dessa forma, o AH e o NAT não podem ser utilizados em conjunto, restando assim duas possibilidades de uso do IPSec: ESP no modo transporte e ESP no modo túnel.

O ESP no modo transporte protege o cabeçalho TCP/UDP, mas não protege os endereços IP de origem e destino. Assim, a modificação do endereço IP não afeta sua checagem de integridade. Contudo, se o pacote for um pacote TCP ou UDP, o NAT modifica o checksum que é protegido pelo ESP, o que causa uma falha na checagem de integridade.

A única solução viável, portanto, é o uso do cabeçalho ESP no modo túnel. Ainda sim podem existir alguns problemas que afetam o IKE, como por exemplo, no uso de

chaves pré-compartilhadas para a autenticação durante o *Main Mode*. Como o *Main Mode* requer autenticação dos pares da comunicação, e a autenticação do IKE com chaves pré-compartilhadas se baseia no endereço IP da máquina para a seleção da chave pré-compartilhada utilizada, um dispositivo intermediário de NAT causará a falha desta autenticação.

Funcionamento do NAT-T

O NAT Traversal é projetado como uma solução simples, que não requer nenhuma modificação nos dispositivos intermediários e nos protocolo existentes. O único requisito é o suporte ao NAT Traversal nos extremos do túnel IPSec. Ele também provê uma forma automatizada de suportar os procedimentos de NAT Traversal, minimizando assim a intervenção do usuário.

O primeiro passo é determinar se as partes comunicantes suportam ou não o NAT Traversal. Isto é feito na Fase 1 do IKE, pelo envio de um campo *vendor ID string* especial, preenchido com o valor "`4485152d 18b6bbcd 0be8a846 9579ddcc`", que é o hash MD5 de "`draft-ietf-ipsec-nat-t-ike-00`". Uma troca bem sucedida indica que ambos os lados suportam o NAT Traversal.

Após a verificação do suporte ao NAT-T por ambas as partes, o segundo passo é descobrir se existe algum dispositivo intermediário de NAT. Essa etapa é denominada NAT Discovery (NAT-D). O NAT Discovery é também usado para determinar qual dos extremos do túnel está localizado atrás do dispositivo de NAT, de forma que somente este lado deverá enviar mensagens de *keep-alive*. O NAT-D nada mais é do que um procedimento para determinar se o endereço IP ou a porta transmitidos no datagrama IP são alterados ao longo do caminho. Para realizar isto ambos os lados calculam e enviam os hashes dos endereços IP e portas de origem e destino para o outro lado. Ambos comparam estes valores e julgam que há um dispositivo de NAT entre eles, caso o hash não coincida. Estes hashes são enviados nos payloads NAT-D. Os payloads NAT-D são inseridos na terceira e quarta mensagens no *Main Mode*, e segunda e terceira mensagens no *Aggressive Mode*.

Quando um dispositivo intermediário de NAT é descoberto, a negociação e posterior decisão de usar o NAT-T são realizadas no *Quick Mode*. A negociação NAT-T decide qual modo de encapsulamento será usado, de forma que um encapsulamento UDP em modo túnel e um encapsulamento UDP em modo transporte são usados em substituição aos modos túnel e transporte tradicionais, respectivamente. Os pares também enviam seus endereços IP originais se necessário. No modo transporte, o envio dos endereços IP e portas originais é obrigatório, enquanto que no modo túnel esse envio é opcional, já que os endereços estão incluídos no datagrama IP interno transportado pelo ESP.

Dessa forma, o tráfego IPSec entre as máquinas é encapsulado em um datagrama UDP

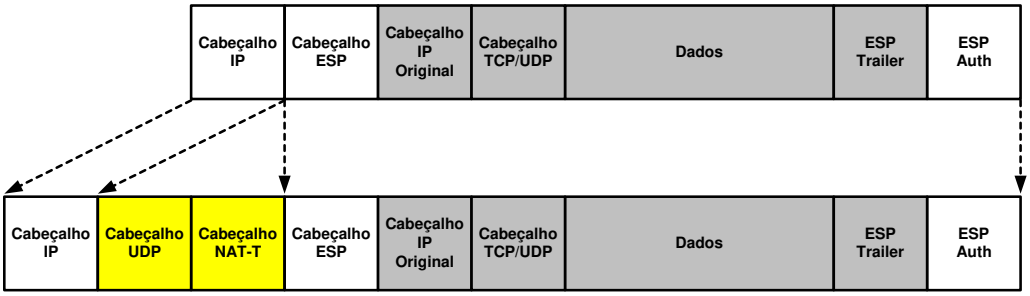


Figura 5.3: Encapsulamento UDP em modo túnel

destinado à porta do IKE. Assim, os pacotes encapsulados seguem a mesma rota que os pacotes IKE. Isto evita modificações nos firewalls e garante que os dispositivos de NAT modifiquem os pacotes NAT-T da mesma forma que eles modificam os pacotes IKE.

Este encapsulamento é feito através da inserção de um cabeçalho UDP à direita do cabeçalho IP externo, como mostrado na Figura 5.3. A porta UDP de destino utilizada é a porta 500, também utilizada pelo IKE. Este cabeçalho UDP sobrescreve os 8 bits do campo `IKE-initiator-cookie` com zeros, o que não é permitido normalmente. Isto provê a habilidade de diferenciar o tráfego normal IKE do tráfego NAT-T. O tamanho e o tipo de protocolo do cabeçalho IP original são armazenados no cabeçalho NAT-T. Por fim, o tamanho do cabeçalho IP é preenchido com o valor 20, ou seja 20 bytes, e o protocolo é preenchido como UDP.

O desencapsulamento é feito da forma reversa. Os pacotes que chegam são checados para identificar se são ou não pacotes NAT-T. Isto é feito procurando-se pelas seguintes condições: tipo de protocolo UDP, porta de destino 500 (IKE) e campo `IKE-initiator-cookie` zerado. Em seguida, é checado se o datagrama IP que chegou faz parte de alguma associação de segurança (SA) previamente negociada. Os endereços IP são substituídos pelos dos pares IPSec, informações adicionais do cabeçalho IP são extraídas do cabeçalho NAT-T, e os cabeçalhos UDP e NAT-T são removidas do pacote.

Mesmo com o encapsulamento UDP funcionando perfeitamente, um outro problema pode surgir quando os dispositivos de NAT, após um período de inatividade, encerram uma associação de NAT sendo que a sessão NAT-T ainda se mantém ativa. Quando um novo pacote chega após um certo período de inatividade, o dispositivo de NAT pode atribuir uma nova porta dinâmica de origem a este pacote, o que causa uma falha na fase de checagem do desencapsulamento. Para evitar tal problema, pacotes de *keep-alive* devem ser enviados pelo extremo do túnel que se encontra atrás do dispositivo de NAT. O intervalo entre os pacotes de *keep-alive* proposto na especificação é de 9 segundos. Se nenhum pacote deste tipo é recebido por um certo período de tempo, a SA é encerrada prematuramente.

Obviamente todo esse processo implica em um overhead considerável. Este overhead é de cerca de 200 bytes para a Fase 1 do IKE e de 20 bytes para cada pacote. O tempo de processamento também pode ser considerado uma desvantagem. Em adição a isso, há o overhead dos pacotes de *keep-alive*, que são enviados a cada 9 segundos. Contudo, se comparados à simplicidade e funcionalidade providas pelo NAT-T, esses atrasos e overheads podem ser considerados insignificantes, ou pelo menos toleráveis.

Uma deficiência mais séria desse mecanismo é o fato da negociação NAT-T não autenticar as máquinas envolvidas. Isto pode expor o gateway VPN a ataques de negação de serviço (DoS), já que um atacante pode iniciar uma negociação utilizando cada uma de suas 65535 portas, o que pode facilmente sobrecarregar o servidor. Um atacante pode também conseguir informações sobre endereços IP internos, já que o hash dos endereços IP é negociado e não é necessário nenhum esforço significativo para varrer toda uma faixa de endereços de 32 bits, resultando em no máximo 2^{32} possibilidades.

Além disso, o NAT-T não pode ser utilizado com protocolos como o FTP e o LDAP, pois estes e alguns outros protocolos incluem os endereços IP da máquinas que estão se comunicando no nível de aplicação dos pacotes. Normalmente esta parte do payload é cifrada e não há formas do NAT-T modificar seu conteúdo, por isso precauções devem ser tomadas para evitar esse tipo de problema.

Capítulo 6

Implementação do Acesso Remoto VPN

Os cenários de acesso remoto VPN se caracterizam basicamente por um usuário remoto que deseja acessar uma rede privada de forma segura de um ponto qualquer na Internet.

Isto significa que o endereço de origem externo do túnel IPSec, será atribuído dinamicamente pelo Provedor de Acesso à Internet (ISP). O mesmo é válido para muitos usuários remotos que acessam a Internet de suas casas através de uma conexão permanente DSL ou cablemodem, onde freqüentemente uma mudança de endereço IP diária é forçada pelo operador da rede. De uma forma geral, na maioria dos cenários possíveis de acesso remoto, mesmo que o endereço IP do sistema cliente não seja totalmente dinâmico, raramente o cliente poderá garantir a utilização de um endereço IP fixo ou previamente conhecido.

Baseado nessas características, foi possível identificar algumas das áreas, no contexto do acesso remoto VPN utilizando IPSec em modo túnel, que devem ser tratadas prioritariamente para o desenvolvimento de uma solução segura e funcional, como:

- Autenticação dos extremos do túnel
- Configuração do sistema remoto
- Configuração da política de segurança
- Passagem por intermediário

Como o objetivo deste trabalho é desenvolver uma solução de acesso remoto VPN segura e viável, uma das decisões de implementação foi a opção pelo uso do software FreeS/WAN[1], uma implementação Open Source do protocolo IPSec baseada em Linux,

[1]Disponível em: <http://www.freeswan.org>.

desenvolvida pelo *FreeS/WAN Project*. Além de ser uma alternativa de baixo custo, o FreeS/WAN é uma das implementações IPSec mais populares para plataformas Linux, que conta com a contribuição de desenvolvedores e grupos de pesquisa de diversos países, em um esforço conjunto visando agregar novas funcionalidades a este produto.

Isto não significa, no entanto, que o suporte à clientes remotos baseados em sistemas Windows ou outros sistemas operacionais não seja suportado. Gateways VPN utilizando FreeS/WAN possuem compatibilidade conhecidamente testada com clientes FreeS/WAN, PGPnet, SafeNet/Soft-PK, SafeNet/SoftRemote, SSH Sentinel, Microsoft Windows 2000 e Windows XP [Ste03b].

Neste capítulo serão detalhadas as decisões de implementação e alguns dos aspectos específicos da configuração de uma solução de acesso remoto VPN baseada em FreeS/WAN. Devido à expressiva parcela de mercado ocupada por produtos Microsoft, serão abordadas também algumas soluções de clientes VPN baseados em Windows, principalmente nos sistemas Windows 2000 e Windows XP, devido à presença de suporte nativo ao IPSec nestes produtos.

Alguns exemplos de arquivos de configuração e um detalhamento maior dos parâmetros utilizados na implementação do acesso remoto VPN utilizando FreeS/WAN serão apresentados no Apêndice A.

6.1 Autenticação dos extremos do túnel

As características dinâmicas dos cenários de acesso remoto impedem que o gateway VPN, que protege o acesso à rede da organização, identifique o cliente de acesso remoto com base no seu endereço IP de origem. Isto impossibilita o uso de segredos pré-compartilhados como forma de autenticação durante o *Main Mode* do IKE, já que a chave de sessão usada para cifrar a identidade na mensagem 5 do IKE, mostrada na Figura 6.1, depende também do segredo pré-compartilhado. Sem o conhecimento a priori da identidade do cliente que inicia uma conexão, o gateway VPN não pode selecionar o segredo pré-compartilhado correto para decifrar a mensagem 5 do IKE que contém por sua vez a informação necessária para identificar o cliente.

Como uma alternativa, o *Aggressive Mode* é freqüentemente usado em soluções VPN, sendo a identidade do cliente enviada em claro. Infelizmente o hash da identidade também é transmitido em claro, o que cria uma potencial brecha de segurança possibilitando um ataque de dicionário off-line sobre o segredo pré-compartilhado que foi usado para assinar o hash.

Assim, para evitar esta potencial fraqueza do *Aggressive Mode* e também proteger a identidade dos clientes de acesso remoto, deve ser usado o *Main Mode* do IKE com assinaturas e certificados digitais, como mostrado na Figura 6.2.

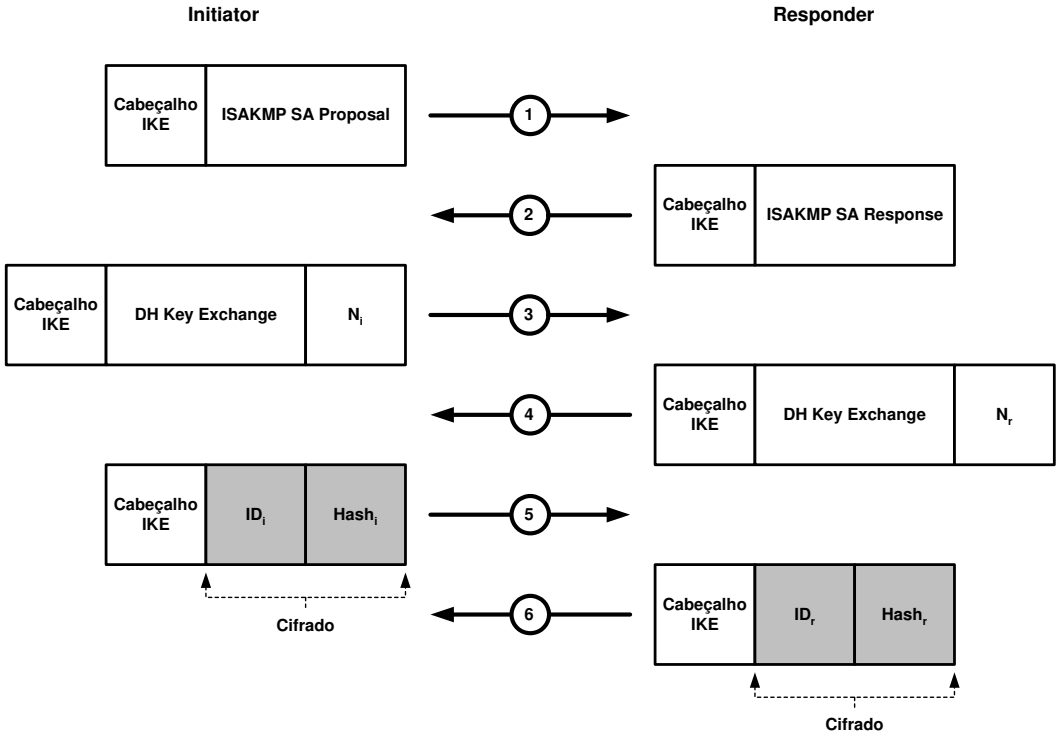


Figura 6.1: *Main Mode* do IKE usando chaves pré-compartilhadas

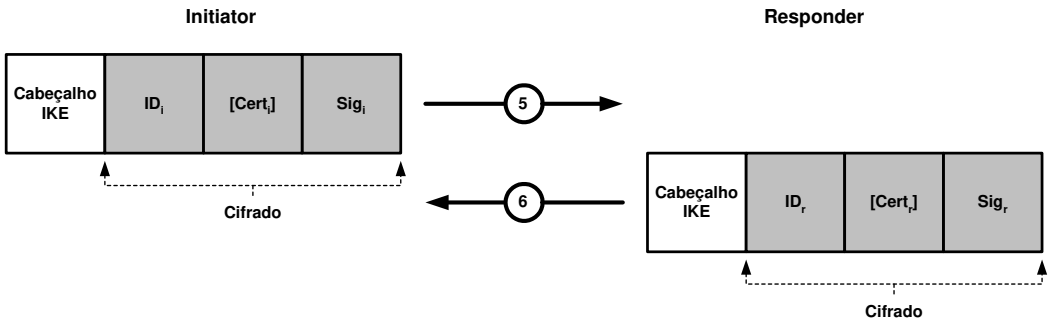


Figura 6.2: *Main Mode* do IKE usando certificados

Neste cenário de chave pública, a chave de sessão simétrica que cifra a troca IKE iniciada com a mensagem 5 depende somente do segredo Diffie-Hellman estabelecido pelas mensagens 3 e 4. Isso possibilita que o receptor extraia a identidade cifrada, que desta forma pode ser usada para selecionar a chave pública correta necessária para verificar a assinatura. Como uma conveniência, a maioria das implementações VPN envia junto um certificado X.509 contendo a chave pública exigida, de forma que não seja necessário obtê-la por outros meios, como por exemplo, uma requisição a um servidor LDAP.

O uso de certificados X.509 normalmente requer a existência de uma Infra-estrutura de Chaves Públicas (ICP) baseada em uma Autoridade Certificadora (AC) que emite e eventualmente revoga certificados de usuários e máquinas. A AC pode também ser executada dentro da empresa ou opcionalmente ser utilizado um centro de confiança oficial. Esta sobrecarga adicional impõe um fardo considerável no desenvolvimento inicial de uma solução VPN. Contudo, esse investimento é compensador, pois o gerenciamento de usuários baseado em certificados é mais escalável em relação a um número crescente de clientes VPN. O uso de certificados de usuário fornece a base ideal para um esquema de controle de acesso sofisticado.

Em ambientes onde existe um sistema de autenticação legada em uso e a organização não planeja desenvolver uma infra-estrutura de chaves públicas em um futuro próximo, deve ser utilizado algum dos mecanismos legados de autenticação descritos na Seção 5.1.

6.1.1 Certificados digitais

No desenvolvimento de VPNs em larga escala, uma maneira viável de realizar a autenticação mútua de ambos os pontos da VPN de uma forma segura e eficiente é usando esquemas baseados em criptografia de chave pública, utilizando certificados digitais. Nestes casos, cada extremo da VPN deve possuir um certificado de usuário ou um certificado de máquina que é enviado ao outro extremo como parte do processo de autenticação no *Main Mode* do IKE. Esta autenticação é baseada em uma assinatura digital gerada cifrando um valor de hash com a chave privada de um dos extremos da VPN. A outra ponta pode então facilmente verificar a assinatura decifrando-a com a chave pública contida no certificado e, em seguida, comparando os hashes.

Para que este processo de autenticação seja seguro, é crucial que exista uma confiança total no certificado da outra ponta. Isto pode ser feito através da inclusão do certificado da AC raiz que emitiu os certificados de usuário e máquina em cada extremo da VPN. A confiança é então transferida para o certificado da AC. Se autoridades certificadoras multi-nível são usadas, então toda a cadeia de certificação deve estar disponível para cada cliente VPN. Os certificados de ACs intermediárias podem ser carregados estaticamente ou ficarem disponíveis através do *Main Mode*.

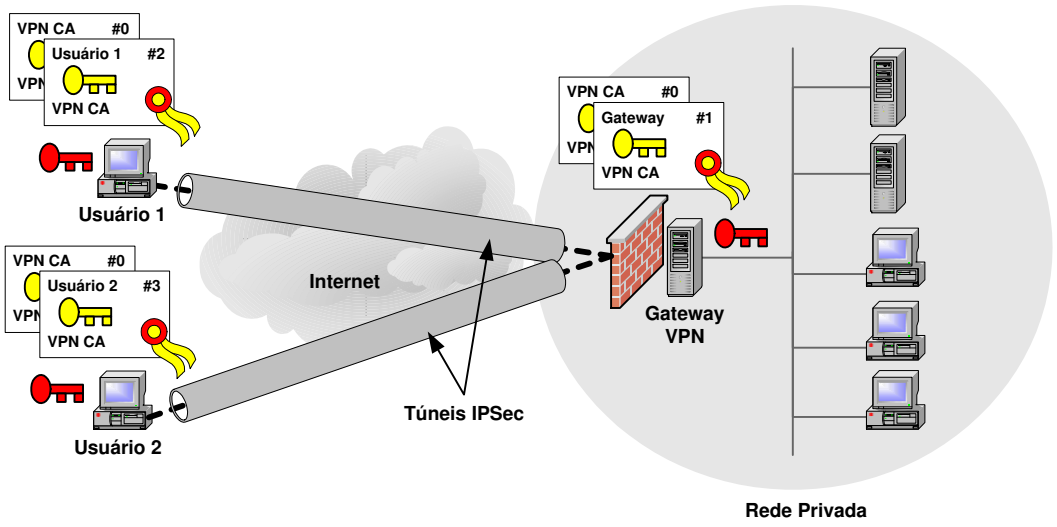


Figura 6.3: Autenticação baseada em certificados X.509

O FreeS/WAN suporta o uso de certificados X.509 a partir de sua versão 1.99, através da instalação de um patch[2] desenvolvido pelo *Security Group of the Zurich University of Applied Sciences*.

No exemplo apresentado na Figura 6.3, todos os certificados finais foram emitidos pela autoridade certificadora VPN CA. O certificado da VPN CA deve ser instalado em cada ponto final da VPN para que se estabeleça uma relação de confiança no certificado recebido da outra ponta. Dessa forma, o gateway VPN aceitará qualquer cliente remoto que apresente um certificado de usuário válido emitido pela VPN CA.

6.1.2 Identidades Coringa

De acordo com as especificações do IETF [Pip98], [KR03b], os seguintes tipos de identidade podem ser usados na autenticação do *Main Mode* baseada no uso de certificados X.509:

- `ID_IPV4_ADDR / ID_IPV6_ADDR`: Endereço IPv4 ou IPv6
- `ID_FQDN`: Nome de domínio da máquina (*Fully Qualified Domain Name*)
- `ID_USER_FQDN`: Identificador de usuário (*Fully Qualified Username*)
- `ID_DER_ASN1_DN`: X.500 *Distinguished Name*

[2]Disponível em: <http://www.strongsec.com/freeswan/>

Para clientes VPN com endereços de rede dinâmicos não faz muito sentido usar um endereço IP com identificador, portanto, somente os três últimos tipos de identidade são relevantes.

Identidades enviadas como parte das mensagens 5 e 6 do *Main Mode* devem estar presentes nos campos correspondentes do certificado X.509, já que a identidade deve estar vinculada a uma chave pública que pode ser usada para checar a assinatura. Se a identidade utilizada for do tipo `ID_DER_ASN1_DN`, ela deve estar contida no campo *subject distinguished name* (`DN`) do certificado, enquanto que identidades do tipo `ID_FQDN ou ID_USER_FQDN` devem estar contidas no campo *subjectAltName*, uma extensão do X.509v3.

Os exemplos a seguir mostram como identidades coringa, representadas pelo caracter "∗", podem ser utilizadas para especificar políticas de controle de acesso mais detalhadas:

```
conn IC
    right=%any
    rightid="C=BR,O=UNICAMP,OU=IC,CN=*"              /* ID_DER_ASN1_DN */
    leftsubnet=10.1.1.0/24

conn DCC
    right=%any
    rightid=*@dcc.unicamp.br                         /* ID_USER_FQDN */
    leftsubnet=10.1.2.0/24

conn LAS
    right=%any
    rightid=@*.las.ic.unicamp.br                     /* ID_FQDN */
    leftsubnet=10.1.3.4/32
```

A primeira definição de conexão (`conn IC`) restringe o acesso à sub-rede `10.1.1.0/24` a qualquer usuário (`CN=`∗) pertencente ao Instituto de Computação (`OU=IC`).

A segunda conexão (`conn DCC`) permite o acesso à sub-rede `10.1.2.0/24`, a todos os usuários que possuem e-mail no domínio `dcc.unicamp.br` através do uso de um caracter coringa no endereço de e-mail (∗`@dcc.unicamp.br`).

A terceira definição (`conn LAS`) permite o acesso ao servidor `10.1.3.4` somente às máquinas que fazem parte do subdomínio atribuído ao Laboratório de Administração e Segurança de Sistemas (∗`.las.ic.unicamp.br`).

O FreeS/WAN também suporta caracteres coringa nos campos *relative distinguished name* (`C=`, `O=`, `OU=`, `CN=`, etc.) das identidades do tipo `ID_DER_ASN1_DN`.

6.1.3 Listas de Certificados Revogados (LCR)

Confiar em um certificado de uma AC raiz significa confiar automaticamente em todos os certificados emitidos por essa AC. Assim, é de extrema importância que uma Lista de Certificados Revogados (LCR) seja mantida pela AC ou por uma entidade delgada para tal, que gerenciará então uma lista dos números de série de todos os certificados que tenham sido revogados.

A freqüência com que uma LCR atualizada é emitida pela AC depende do que foi definido na política de segurança, de forma que os intervalos de emissão podem variar de acordo com a maior ou menor necessidade de impedir o acesso de usuários ou máquinas não-autorizados. O gateway e o cliente VPN devem periodicamente atualizar sua cópia local da LCR de acordo com os intervalos de emissão, carregando-os de um servidor HTTP ou LDAP.

Um ou vários pontos de distribuição de LCRs (`crlDistributionPoints`) podem ser inseridos como uma extensão em certificados X.509v3 para cada um dos certificados utilizados. Um `crlDistributionPoint` usualmente tem a forma de uma URI (*Uniform Resource Indicator*), e pode ser usado para obter automaticamente uma LCR de um servidor HTTP ou LDAP.

Um exemplo de uma URI HTTP na notação do OpenSSL, seria:

```
crlDistributionPoints=URI:http://www.vpnca.org/ca/cert.crl
```

A obtenção automática de LCRs baseadas em `crlDistributionPoints` é suportada a partir da versão 2.00 do Linux FreeS/WAN. Os certificados de máquina e usuário necessários podem ser gerados usando o pacote OpenSSL, através da definição de um ou mais `crlDistributionPoints` no arquivo de configuração `openssl.cnf`.

6.1.4 Protocolo Online de Estado de Certificado (OCSP)

Com um crescente número de usuários e a revogação freqüente de certificados, os intervalos de emissão de LCRs podem se tornar inadequados para garantir que certificados recentemente revogados sejam rejeitados. Uma alternativa viável para complementar ou mesmo substituir as listas de certificados revogados pode ser o uso do Protocolo Online de Estado de Certificados (*Online Certificate Status Protocol* – OCSP) [MAM+99].

Quando o OCSP é utilizado, um ponto da VPN envia uma requisição contendo o número de série do certificado da outra ponta para ser verificado por um servidor OCSP, que retorna uma resposta assinada contendo um dos indicadores: bom (*good*), revogado (*revoked*) ou desconhecido (*unknown*). A chave privada usada para assinar a resposta deve pertencer: à AC que emitiu o certificado em questão; a um *Trusted Responder* cuja chave pública é confiável; ou a uma *CA Designated Responder*, também denominada *Authorized*

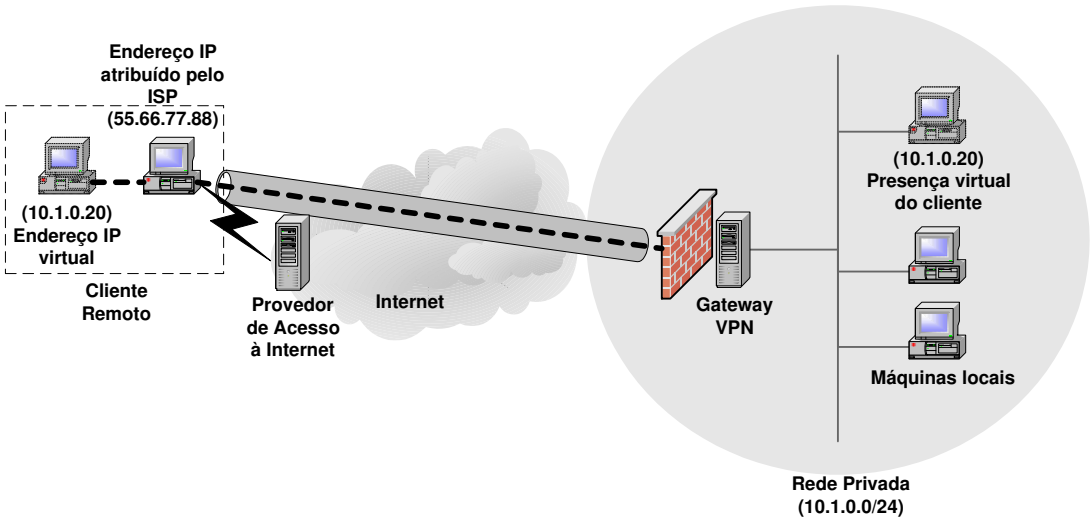


Figura 6.4: Atribuição de Endereço IP Virtual (VIP)

Responder, que possui um certificado especial emitido diretamente pela AC, indicando a permissão para emitir respostas OCSP em nome da AC.

Foi incorporado recentemente, na versão 1.5 do patch X.509, o suporte à verificação de certificados baseada em OCSP para o daemon IKE do FreeS/WAN, denominado Pluto. Um servidor OCSP também já está sendo disponibilizado a partir da versão 0.9.7 do pacote OpenSSL.

6.2 Configuração do sistema remoto

Como os sistemas dos clientes remotos carregam um endereço IP de origem externo dinâmico atribuído a eles por seus ISPs, é bastante desejável que seus endereços IP de origem internos pertençam a um segmento de rede especial da faixa de endereços da rede privada, constituindo assim o que geralmente é denominado de "*extruded net*". Isto pode ser conseguido atribuindo um IP Virtual (*Virtual IP* - VIP) ao cliente remoto estática ou dinamicamente como mostrado na Figura 6.4.

O uso do endereço IP virtual facilita tanto a filtragem de pacotes IP que saem do túnel IPSec pelo gateway VPN, quanto o roteamento dos pacotes de retorno das máquinas da rede privada para os clientes remotos.

Devido ao grande sucesso do protocolo PPP (*Point-to-Point Protocol*) e seus auxiliares, como o protocolo IPCP (*IP Control Protocol*), que permite a atribuição automática de um endereço IP ao cliente e também a especificação de servidores DNS e WINS, estes princípios foram prontamente herdados pelo protocolo L2TP (Layer 2 Tunneling Protocol)

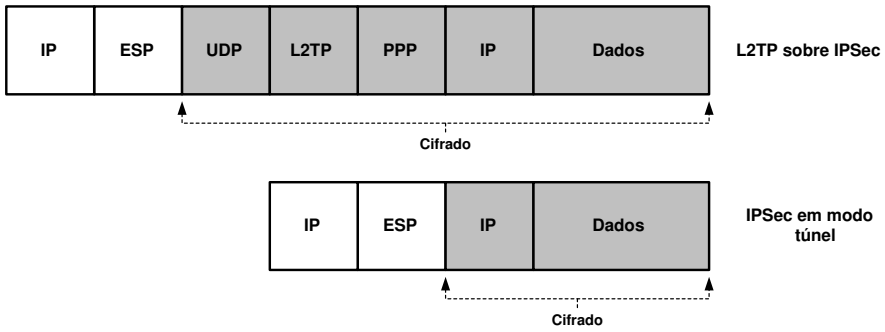


Figura 6.5: L2TP sobre IPSec vs. IPSec em modo túnel

que encapsula quadros PPP em datagramas UDP para tunelá-los sobre a Internet, criando assim uma conexão virtual.

Pelo fato das funcionalidades do IPCP não serem diretamente suportadas pelo protocolo IKE, soluções baseadas no L2TP são freqüentemente adotadas em cenários de acesso remoto. Para suprir a necessidade de segurança criptográfica deste protocolo, o L2TP deve ser adicionalmente protegido pelo IPSec, como mostrado na parte superior da Figura 6.5. Esta é exatamente a abordagem escolhida pela Microsoft para sua solução de acesso remoto nos sistemas operacionais Windows 2000 e XP.

Apesar desta ser uma solução aparentemente viável, na prática ela apresenta diversos problemas causados pelo overhead de cabeçalhos na comunicação e pela própria natureza do protocolo PPP, como discutido no Capítulo 3. A utilização de túneis IPSec, como mostrado na parte inferior da Figura 6.5, constitui uma excelente alternativa ao uso do L2TP, contanto que a atribuição dinâmica de endereços IP virtuais e servidores de informação DNS/WINS possa ser de alguma forma solucionada.

Uma abordagem proprietária chamada Mode-Config [PAP99], apresentada na Seção 5.2.1, introduz mensagens específicas proprietárias no protocolo IKE. Este conceito tem algumas vantagens convincentes quando informações de usuário, incluindo o endereço IP virtual que será atribuído, estão armazenadas em um servidor centralizado LDAP ou RADIUS. O gateway VPN pode então obter diretamente as informações de usuário do servidor de diretórios e encaminhar a informação para o cliente graças ao canal de comunicação IKE. Este argumento a favor do Mode-Config tem conduzido à sua inclusão oficial na proposta do protocolo IKEv2 [Kau03] sendo especificado atualmente pelo *IPSec Working Group* do IETF.

Contudo, a necessidade de inclusão de novas mensagens no atual padrão do IKE em uso, faz com que essa abordagem seja radicalmente evitada pelo *IPSRA Working Group* do IETF. Uma solução alternativa, recentemente padronizada pelo IETF, é o uso do protocolo DHCP sobre IPSec [PAKG03].

6.2.1 DHCP sobre IPSec

Geralmente um ou mais servidores DHCP são responsáveis pela atribuição dinâmica de endereços IP e de informações auxiliares para máquinas de uma rede privada. Vários aspectos importantes como uma renovação periódica dos empréstimos (*leases*) de endereços, o gerenciamento eficiente dos endereços disponíveis e a reação apropriada aos timeouts podem ser tratados por servidores DHCP de forma estável e confiável.

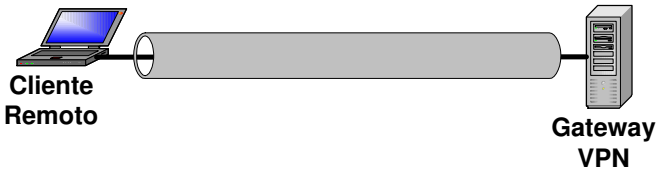
Um cliente remoto acessando uma rede privada através de um túnel IPSec necessita do mesmo tipo de informação para a configuração de sua interface IP virtual. Dessa forma, um servidor DHCP pode ser utilizado para prover esses serviços, enquanto que o gateway VPN se restringirá somente ao repasse de informações DHCP sobre o canal IPSec.

A Figura 6.6 mostra como um esquema de atribuição dinâmica de endereço IP pode ser realizado usando o protocolo DHCP sobre IPSec:

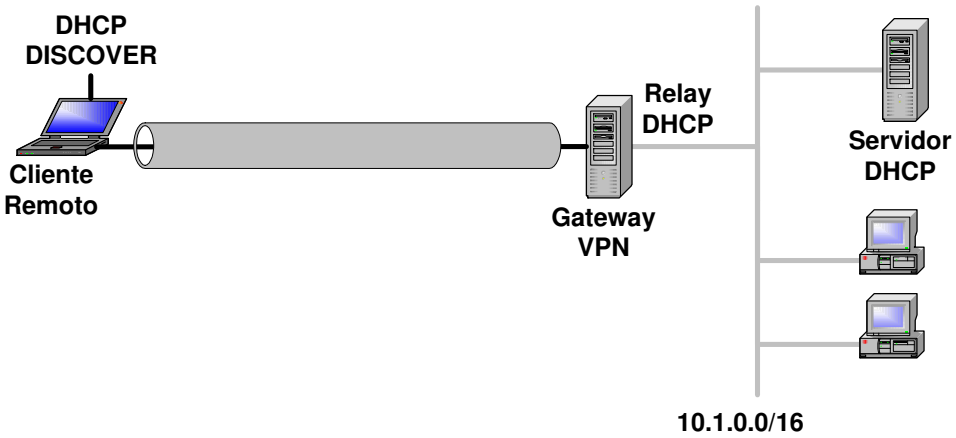
a) Na primeira fase uma negociação *Main Mode* do IKE é usada para criar uma associação de segurança ISAKMP (ISAKMP SA) estabelecendo uma relação de confiança entre o cliente remoto e o gateway VPN através de autenticação mútua. Esta ISAKMP SA é então a base para todas as IPSec SAs subseqüentes que serão negociadas pelos extremos do túnel.

b) Em seguida uma negociação *Quick Mode* do IKE configura uma IPSec SA com uma máscara de rede igual a 0.0.0.0/0, denominada DHCP SA, para que seja possível tunelar a mensagem broadcast DHCP DISCOVER subseqüente originada pelo cliente remoto. Como tal máscara de rede global poderia implicar em um potencial risco de segurança, esta DHCP SA é restrita ao tráfego entre as portas UDP/bootpc e UDP/bootps, nos lados cliente e servidor respectivamente. Pelo fato do servidor DHCP de uma corporação usualmente não estar localizado na mesma rede que o gateway VPN, um relay DHCP é necessário no gateway para encaminhar a mensagem de DHCP DISCOVER ao servidor DHCP localizado em algum lugar na rede privada. Como uma medida adicional de segurança, o tempo de vida da DHCP SA será configurado como o mínimo de tempo absolutamente necessário para tratar a troca composta pelo broadcast DHCP DISCOVER inicial e pela mensagem de DHCP REPLY de retorno.

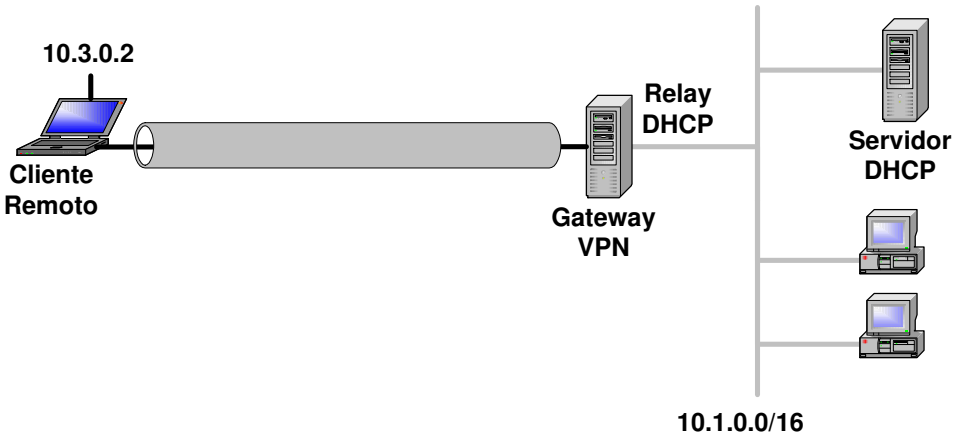
c) Assim que o cliente remoto obtiver o endereço IP interno, uma negociação normal *Quick Mode* é iniciada, conectando o endereço IP interno virtual do cliente VPN à rede privada através do túnel IPSec. Freqüentemente, quando o empréstimo DHCP (*DHCP lease*) requisitar uma renovação, a mensagem unicast DHCP REQUEST correspondente poderá ser tunelada para o gateway VPN usando a IPSec SA estabelecida, de forma que uma DHCP SA separada não tenha mais que ser configurada.



a) ISAKMP SA (Main Mode)
Cliente Remoto <=> Gateway VPN



b) DHCP SA (Quick Mode, curto tempo de vida)
Cliente Remoto : UDP/bootpc <=> Gateway VPN : UDP/bootps --- 0.0.0.0/0



c) IPSec SA (Quick Mode)
10.3.0.2 --- Cliente Remoto <=> Gateway VPN --- 10.1.0.0/16

Figura 6.6: DHCP sobre IPSec

6.2.2 Servidor DHCP

Uma funcionalidade importante que deve ser provida pelo servidor DHCP é a diferenciação no tratamento das requisições feitas pelos clientes VPN e pelas demais máquinas da rede privada.

Para que isso se torne possível, é necessário que sejam levados em consideração parâmetros da requisição, como o *DHCP Relay Agent Information Option* ou o *Gateway Address*. O primeiro parâmetro contém o nome do dispositivo IPSec de onde se originou a requisição, neste caso, uma interface virtual `ipsec0` criada pelo FreeS/WAN. O segundo parâmetro contém o endereço IP do gateway VPN. O exemplo a seguir ilustra a configuração de um servidor DHCP utilizando o primeiro parâmetro [Str03]:

```
# Classe de clientes VPN
class "vpn-clients" {
    match if option agent.circuit-id = "ipsec0";
}

subnet ... {
    ...

    # Demais máquinas da rede privada
    pool {
        deny members of "vpn-clients";
        ...
    }

    # Clientes VPN
    pool {
        allow members of "vpn-clients";
        ...
    }
}
```

6.2.3 Relay DHCP

Por razões de funcionalidade, o servidor DHCP de uma organização geralmente fica situado em sua rede privada. Já o gateway VPN, normalmente se encontra em uma interface de rede dedicada do firewall, ou em muitos cenários em conjunto com o próprio firewall. O fato de ambos não estarem executando na mesma máquina, exige que o

gateway VPN realize a função de Relay DHCP, encaminhando as mensagens de DHCP DISCOVER enviadas pelos clientes remotos ao servidor DHCP localizado em algum lugar na rede privada.

O Relay DHCP[3] desenvolvido por Mario Strasser [Str03], utilizado em conjunto com o FreeS/WAN, permite a integração das funcionalidades de gateway VPN e Relay DHCP em um único equipamento, realizando todos os procedimentos descritos anteriormente. O arquivo de configuração do Relay DHCP contém quatro ítens:

- LOGFILE: define o arquivo de log utilizado.
- DEVICES: contém uma lista das interfaces IPSec onde o Relay DHCP estará aguardando por requisições.
- SERVERDEVICE: define a interface que leva ao Servidor DHCP.
- DHCPSERVER: define o nome de máquina ou o endereço IP do Servidor DHCP. Se nenhum nome ou endereço forem fornecidos, os pacotes serão enviados em broadcast.

No exemplo a seguir é ilustrada a configuração de um Relay DHCP, realizando o repasse das mensagens DHCP que chegam pela interface ipsec0 ao servidor 10.1.1.3 acessível através da interface de rede eth1:

```
# Arquivo de configuração do Relay DHCP

# Localização dos arquivos de log
LOGFILE="/var/log/relaydhcp.log"

# Interfaces IPSec
DEVICES="ipsec0"

# Interface que leva ao Servidor DHCP
SERVERDEVICE="eth1"

# Nome de máquina ou endereço IP do Servidor DHCP
DHCPSERVER="10.1.1.3"
```

Proxy ARP

Algumas questões relacionadas à faixa de endereços reservada aos clientes VPN merecem atenção especial. Existem basicamente dois cenários que devem ser considerados.

[3]Disponível em: <http://www.strongsec.com/freeswan/dhcprelay/>

O primeiro é aquele onde clientes VPN recebem um endereço IP virtual de uma sub-rede separada. A principal vantagem desta opção é a facilidade de gerenciamento das políticas de segurança impostas aos clientes, já que estes pertencem a uma sub-rede bem definida. Além disso, o roteamento dos pacotes que retornam aos clientes remotos se torna mais simples.

Um segundo cenário possível é aquele onde são atribuídos aos clientes VPN endereços IP virtuais da mesma sub-rede que as máquinas da rede privada. A grande vantagem deste cenário é a possibilidade do uso de aplicações que eventualmente necessitam enviar pacotes em broadcast para seu perfeito funcionamento. Nestes casos o suporte ao mecanismo de proxy ARP [Ste96] deve estar habilitado e devidamente configurado no gateway VPN, para que este consiga rotear os pacotes endereçados ao cliente apropriadamente.

Nas distribuições Linux mais populares isto pode ser feito através da configuração apropriada das rotas direcionadas ao cliente VPN, o que normalmente é feito automaticamente pelo FreeS/WAN, e da habilitação do suporte de kernel ao mecanismo de proxy ARP na interface de rede adequada, através da execução do comando:

```
echo 1 > /proc/sys/net/ipv4/conf/eth*/proxy_arp
```

6.3 Configuração da política de segurança

Usando informações de identidade do usuário disponíveis em uma negociação IKE bem sucedida, um firewall pode dinamicamente abrir partes selecionadas da rede de acordo com um perfil de usuário pré-definido. Para implementar tal esquema comum, o firewall e o software VPN deveriam idealmente executar no mesmo computador, contudo uma variação onde um gateway VPN separado está conectado ao firewall através de uma interface de rede dedicada também pode ser possível.

A implementação IPSec do FreeS/WAN apresenta uma característica importante, onde há a possibilidade de definir um script qualquer que, imediatamente após a configuração bem sucedida de uma conexão VPN, deverá ser executado. Dessa forma, é possível inserir um conjunto de regras de firewall dinâmicas, possibilitando que ambos, cliente e gateway VPN, se protejam utilizando regras específicas durante a existência de uma determinada conexão VPN. Ao término do túnel VPN, as regras inseridas serão automaticamente removidas e o acesso à rede privada será fechado para aquele usuário específico.

A Figura 6.7 apresenta um cenário onde o firewall/gateway VPN permite a implementação de uma política de segurança comum que abrange a terminação do túnel VPN e o acesso seletivo a diferentes partes da rede privada controlado por regras de firewall dedicadas.

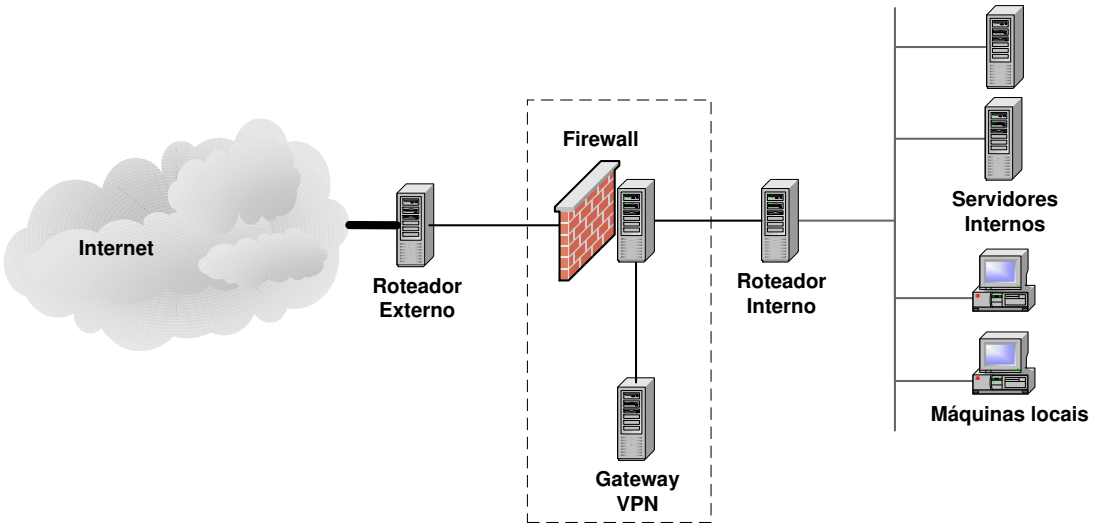


Figura 6.7: Firewall/gateway VPN implementando controle de acesso

Outra forma de implementar uma política de segurança comum é através de um acesso seletivo baseado em identidades coringa, como descrito anteriormente. Tal mecanismo foi recentemente padronizado, através de sua inclusão na especificação de um Modelo de Informação de Configuração de Políticas IPSec [JRV03] desenvolvido pelo *IP Security Policy Working Group* do IETF.

Uma grande vantagem dessa abordagem baseada em identidades coringa é o fato de poder utilizar uma hierarquia de confiança bastante simplificada, sem a necessidade de diferentes níveis de autoridades certificadoras. Por outro lado, requer um planejamento cuidadoso na estrutura dos campos *Distinguished Name* do certificado no caso de identidades `ID_DER_ASN1_DN` ou na estrutura dos sub-domínios se os tipos `ID_FQDN` ou `ID_USER_FQDN` forem utilizados. Uma vez desenvolvido, torna-se extremamente difícil introduzir grandes modificações nesse esquema de controle de acesso sem substituir todos os certificados emitidos.

Alguns trabalhos estão sendo desenvolvidos com o intuito de criar outros métodos de controle de acesso seletivo baseados em aspectos distintos, como autoridades de certificação intermediárias, certificados de atributos, e tickets Kerberos [Ste03a].

6.4 Passagem por intermediário

Em muitos cenários de acesso remoto VPN, é comum a existência de equipamentos que realizam a tradução de endereços de rede (NAT) situados ao longo do caminho entre o cliente e o gateway VPN.

Estes mecanismos interferem no funcionamento normal das VPNs baseadas em IPSec, ao efetuarem modificações nos cabeçalhos dos pacotes que passam por eles, ocasionando falhas na verificação de integridade dos pacotes.

O que agrava a situação é que esses dispositivos de NAT estão amplamente difundidos, sendo necessários ao pleno funcionamento das redes envolvidas, e dificilmente podem ser modificados para a adequação a um tráfego de VPN.

Como alternativa, umas das propostas apresentadas ao *IPSRA Working Group* do IETF, o NAT Traversal (NAT-T), tem se mostrado uma solução promissora para os conflitos existentes entre NAT e IPSec. Esta solução se baseia no encapsulamento do tráfego da VPN em datagramas UDP, permitindo assim que um cliente remoto e um gateway VPN, ambos com suporte ao NAT-T, utilizem um túnel IPSec para o acesso remoto VPN sem serem afetados pelos inconvenientes causados pelo dispositivo de NAT.

O suporte ao mecanismo de NAT-T no FreeS/WAN é feito através da instalação de um patch[4] desenvolvido por Mathieu Lafon da Arkoon Network Security.

Para que o uso do NAT-T seja habilitado, é necessária a inserção de apenas três novos parâmetros no arquivo de configuração `ipsec.conf` do FreeS/WAN, como mostrado no exemplo a seguir:

```
config setup
    ...
    nat_traversal=yes
    virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16

conn AcessoRemoto
    ...
    rightsubnet=vnet:%priv
```

Na seção de definição dos parâmetros de configuração (`config setup`) é habilitado o suporte ao mecanismo de NAT-T (`nat_traversal=yes`), sendo em seguida definida a faixa de endereços privados que será aceita como válida (`virtual_private=`), sendo suportados endereços IPv4 (`%v4:`) ou IPv6 (`%v6:`).

Em seguida, na definição da conexão do acesso remoto (`conn AcessoRemoto`) define-se que qualquer cliente VPN com endereço IP pertencente à faixa de rede privada definida anteriormente terá acesso permitido (`rightsubnet=vnet:%priv`).

O FreeS/WAN também suporta outros tipos de endereço, sendo `vnet` a definição de uma faixa de rede e `vhost` a definição de um endereço de máquina, e também diferentes

[4]Disponível em: <http://open-source.arkoon.net>

métodos, como `%no` indicando que somente endereços IP públicos são aceitos, `%all` indicando que qualquer endereço IP é aceito, `%priv` como mostrado anteriormente, além de outros ainda não implementados na versão mais recente deste patch.

6.5 Suporte a clientes Windows

Todas as decisões de implementação e exemplos de configuração apresentados até o momento se baseiam no uso do software FreeS/WAN em sistemas Linux, tanto no cliente como no gateway VPN.

Contudo, em razão da significativa parcela de mercado ocupada por produtos Microsoft, soluções baseadas na plataforma Windows não podem ser ignoradas. A solução apresentada a seguir é baseada no sistemas operacionais Windows 2000 e Windows XP, devido à presença de suporte nativo ao IPSec nestes produtos e sua maior disseminação em ambientes corporativos.

Tal solução não possui suporte a muitas das funcionalidades descritas anteriormente, como a atribuição de endereços IP virtuais e suporte ao NAT-T. Na verdade, ela se restringe ao uso de alguns recursos nativos desses sistemas Windows para o estabelecimento de um túnel IPSec com um gateway VPN, baseado ou não em FreeS/WAN, utilizando autenticação por certificados digitais.

Apesar de ser uma solução um tanto restrita, apresenta a vantagem de não necessitar de softwares comerciais, com exceção do próprio sistema operacional da Microsoft, sendo portanto uma alternativa de baixo custo para clientes VPN utilizando tal plataforma.

É importante frisar que gateways VPN utilizando FreeS/WAN possuem compatibilidade conhecidamente testada com clientes FreeS/WAN, PGPnet, SafeNet/Soft-PK, SafeNet/SoftRemote, SSH Sentinel, Microsoft Windows 2000 e Windows XP [Ste03b]. Dentre esses clientes VPN, o SSH Sentinel, desenvolvido pela SSH Communications Security, é o que suporta o maior número de funcionalidades, além de ser o único a suportar a atribuição de endereços IP virtuais, constituindo portanto uma excelente opção de software comercial para a plataforma Windows.

6.5.1 Clientes Windows 2000 e Windows XP

Os sistemas operacionais da família Windows, desenvolvidos pela Microsoft, ocupam uma parcela significativa do mercado de sistemas operacionais domésticos. Tal popularidade também se traduz em realidade nos ambientes corporativos, onde grande parte do parque computacional das organizações utiliza os sistemas da Microsoft, especialmente os Windows 2000 e XP, devido à maior disponibilidade de recursos e mecanismos internos de segurança mais capazes.

O suporte nativo ao protocolo IPSec nesses dois sistemas operacionais permite o desenvolvimento de uma solução de baixo custo para o acesso remoto VPN, que apesar de não suportar algumas funcionalidades desejáveis, oferece ao usuário remoto uma conectividade segura com a rede da organização, através de um túnel IPSec, com autenticação baseada em certificados digitais.

Para isso, é necessária a instalação de dois ítens adicionais. O primeiro é a ferramenta `ipsecpol.exe`[5], que faz parte do *Resource Kit* do Windows 2000, ou sua correspondente `ipseccmd.exe` no Windows XP, cuja função é permitir a adição, remoção e alteração de políticas IPSec por meio de linhas de comando, sem a necessidade de uma interação com interfaces gráficas. O segundo item é uma ferramenta desenvolvida por Marcus Müller[6], que permite a utilização de um arquivo de configuração baseado na sintaxe do FreeS/WAN e também o estabelecimento, monitoramento e encerramento do túnel VPN através de linhas de comando.

Um exemplo de configuração para uma conexão de acesso remoto VPN em um cliente Windows utilizando essas ferramentas é mostrado a seguir:

```
conn AcessoRemoto
    left=%any
    right=143.106.60.15
    rightsubnet=10.1.1.0/255.255.255.0
    rightca="C=BR,O=Unicamp,OU=Instituto de Computação,CN=VPN CA"
    network=auto
    auto=start
```

Na definição da conexão de acesso remoto (`conn AcessoRemoto`) um cliente remoto com endereço IP qualquer (`left=%any`) estabelece um túnel IPSec com gateway VPN `143.106.60.15` (`right=`) que permite o acesso à rede privada `10.1.1.0/255.255.255.0` (`rightsubnet=`) com a autenticação sendo feita por certificados emitidos pela autoridade certificadora VPN CA (`rightca=`). Os parâmetros adicionais servem para definir a interface de rede utilizada e a inicialização automática do túnel, respectivamente.

Após a configuração adequada dos parâmetros da conexão VPN e a instalação do certificado do usuário remoto através do *Microsoft Management Console* (MMC) do Windows, basta executar a aplicação `ipsec.exe` para o estabelecimento do túnel IPSec com o gateway VPN informado e o conseqüente acesso aos recursos da rede privada desejada.

[5]Disponível em: <http://www.microsoft.com/>
[6]Disponível em: <http://vpn.ebootis.de/>

Capítulo 7

Considerações Adicionais

Complementando a análise dos aspectos de segurança envolvidos em um ambiente de acesso remoto VPN, é importante que sejam feitas algumas considerações a respeito do posicionamento do gateway VPN na topologia de segurança de uma organização.

A inserção de um gateway VPN em um ambiente de segurança pré-existente é um tópico que merece atenção especial, pois uma escolha inadequada pode não só comprometer a segurança das informações que trafegam através do túnel VPN, como também trazer sérias implicações de segurança para a rede privada da organização.

A seguir será apresentada uma análise do posicionamento do gateway VPN na topologia de segurança de uma organização, baseada em alguns trabalhos correlatos [FdG02], [Kin03].

7.1 Posicionamento do gateway VPN na topologia de segurança

A adição de um gateway VPN à estrutura de segurança já existente de um ambiente corporativo é um assunto bastante delicado. Uma decisão inadequada pode comprometer não só a segurança das informações que trafegam através da VPN, mas também a segurança da rede privada como um todo. Por isso é importante estar atento a todos os aspectos envolvidos nesse processo.

Em geral, algumas premissas básicas sobre o posicionamento do gateway VPN podem ser evidenciadas, como por exemplo:

- Não comprometer a política geral de segurança da rede.
- O gateway VPN não deve constituir um único ponto de falha.
- O gateway VPN deve aceitar de redes não confiáveis somente tráfego cifrado.

- O gateway VPN deve aceitar tanto tráfego cifrado como não cifrado da rede privada.
- O gateway VPN deve estar protegido de ataques originados da Internet.
- O tráfego resultante do deciframento dos dados por parte do gateway VPN deve ser submetido a algum tipo de filtragem.

A construção de uma política de segurança deve se fundamentar em conceitos gerais do que deve ser uma rede segura, como por exemplo, que serviços devem ser protegidos, que serviços internos devem estar disponíveis para os usuários remotos, além de diversos outros aspectos. A partir do estudo desses fatores, deve ser concebida uma topologia de equipamentos de segurança que reflita a política de segurança anteriormente estabelecida.

A colocação de um gateway VPN, em uma estrutura de rede já consolidada, deve implicar em uma revisão da topologia de segurança da rede, com o objetivo de assegurar as premissas da política estabelecida. Para isso devem ser analisadas todas as alterações de tráfego introduzidas com a adição da VPN, efetuando em seguida as alterações de configuração necessárias nos equipamentos.

Como o gateway VPN deve receber somente tráfego proveniente da própria VPN, não há a necessidade de aceitar qualquer outro tipo de tráfego, além daquele de controle, que não seja cifrado. Essa rejeição ou descarte de outros tipos de tráfegos é parte fundamental da política de auto-defesa do próprio gateway VPN. O posicionamento do gateway VPN em relação ao firewall é um ponto crucial, pois os firewalls não podem aplicar regras de filtragem a pacotes cifrados. Tendo em vista as premissas anteriormente descritas, serão analisadas a seguir cada uma das possibilidades de inserção do gateway VPN em uma topologia de rede típica em relação ao firewall.

7.1.1 Em frente ao firewall

A colocação do gateway VPN em frente ao firewall, mostrada na Figura 7.1, implica em um ponto único de falha. Isto significa que um ataque de negação de serviço (DoS) realizado sobre o gateway VPN, que é o ponto de conexão à Internet, pode ter conseqüências desastrosas para a rede da organização, indisponibilizando toda a comunicação com redes externas. Tal implicação é de grande importância, se considerarmos que o software utilizado no gateway VPN pode conter erros de implementação que podem ser explorados por um atacante, ou mesmo se considerarmos um possível ataque de negação de serviço distribuído (DDoS) visando esgotar os recursos do gateway VPN.

Além disso, com essa configuração de equipamentos, o gateway VPN fica completamente exposto a outros tipos de ataque originados da Internet, já que todo o tráfego que chega a ele não é anteriormente submetido a qualquer tipo de análise.

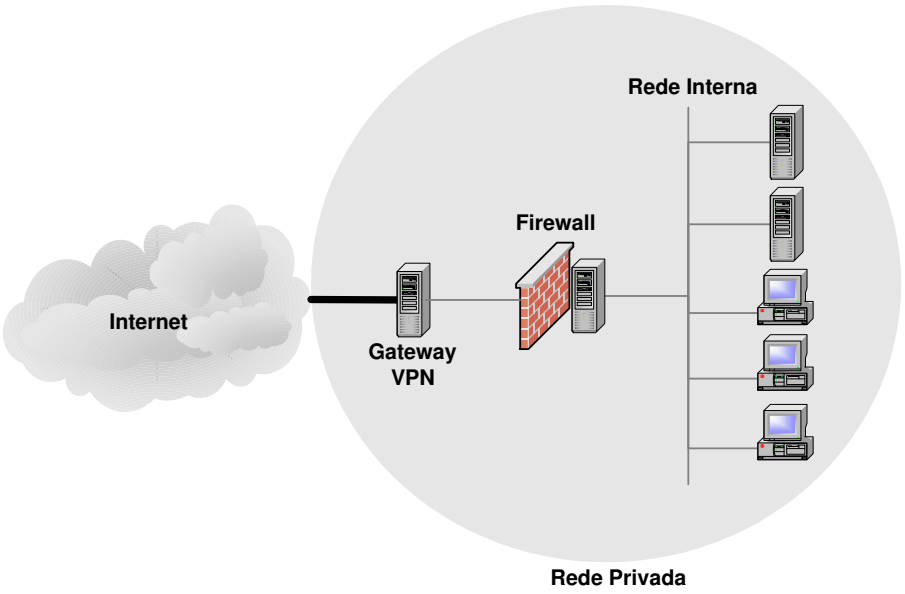


Figura 7.1: Gateway VPN em frente ao Firewall

Outro problema existente neste cenário, é a dificuldade no firewall de diferenciar o tráfego originado por usuários remotos da VPN do tráfego originado de usuários quaisquer da Internet, já que ambos chegam pela mesma interface. Uma simples filtragem baseada em endereços de rede, além de ser complexa em cenários de acesso remoto, pode permitir a um atacante burlar a filtragem do firewall utilizando técnicas triviais de spoofing [NdG02].

7.1.2 Atrás do firewall

Com o gateway VPN situado atrás do firewall, como mostrado na Figura 7.2, é possível que o firewall forneça algum nível de proteção adicional, permitindo que somente pacotes IP do tipo 50 (AH) e 51 (ESP), e pacotes UDP destinados à porta 500 (IKE), cheguem ao gateway VPN.

Contudo, um dos problemas dessa abordagem é que o firewall não consegue efetuar uma filtragem adequada no tráfego endereçado ao gateway VPN, pelo fato dele estar cifrado. Como conseqüência, todo o tráfego VPN, após o deciframento, adentrará a rede interna sem que sobre ele tenha sido aplicado qualquer tipo de controle.

Deve ficar bem claro que o gateway VPN seria, neste caso, o último componente do firewall antes da rede interna. Deste modo, o gateway VPN estaria fornecendo proteção somente ao tráfego entre as extremidades do túnel, deixando fragilizados os recursos da rede interna.

Esta configuração também implica em um único ponto de falha, expondo a rede da

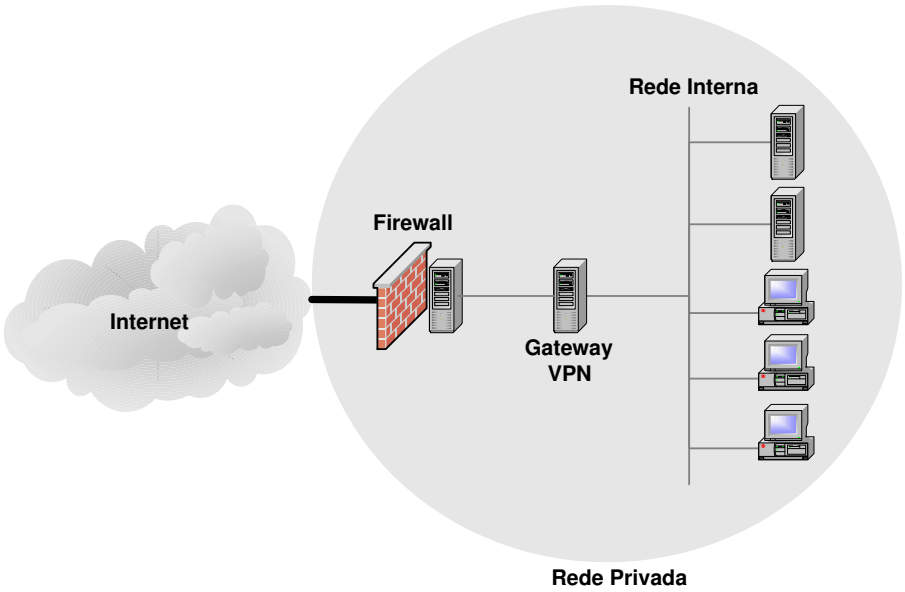


Figura 7.2: Gateway VPN atrás do Firewall

organização às mesmas ameaças descritas anteriormente.

7.1.3 Combinado ao firewall

A combinação de firewall e gateway VPN em um único equipamento, como mostrado na Figura 7.3, é uma alternativa bastante popular recomendada por diversos fabricantes de produtos VPN, que apresenta a vantagem de simplificar a administração e o gerenciamento dos componentes da rede.

A grande desvantagem dessa abordagem é que se exige do equipamento a habilidade de rotear, executar criptografia de chave pública e chavear entre sessões cifradas ao mesmo tempo em que se realiza a filtragem de pacotes e a geração de logs. Isto pode gerar uma sobrecarga considerável no equipamento, dependendo do tipo de tráfego, da quantidade e da complexidade do roteamento e das regras de filtragem.

Porém, o problema crucial nesta solução é que o equipamento constitui num único ponto de falha ainda mais grave do que nos cenários anteriores, pois um ataque ao gateway VPN pode comprometer toda a estrutura do firewall.

7.1.4 Em paralelo ao firewall

Um grande número de fabricantes de produtos VPN sugerem a colocação do gateway VPN em paralelo ao firewall, como mostrado na Figura 7.4, de forma que existam assim duas conexões com a rede externa: uma para o firewall, outra para o gateway VPN.

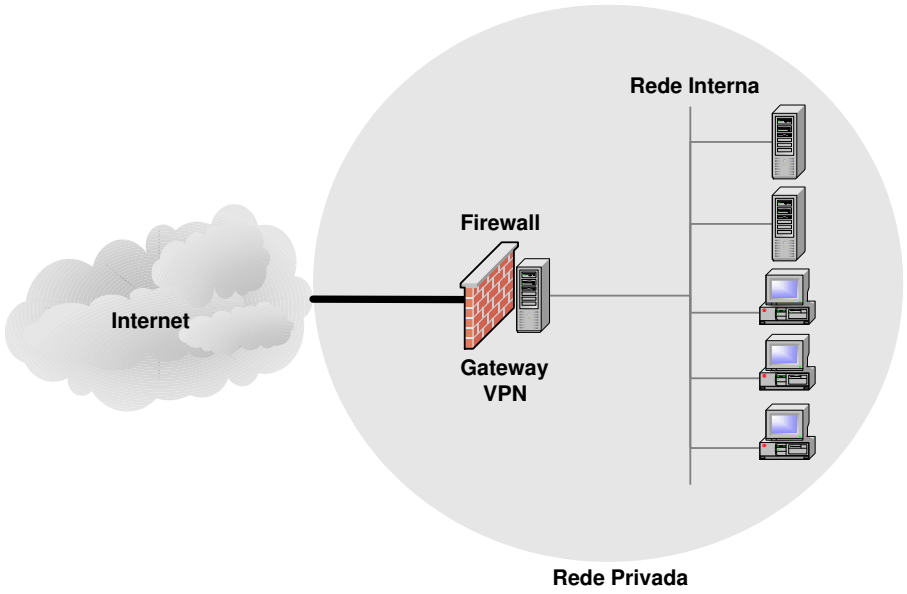


Figura 7.3: Gateway VPN combinado ao Firewall

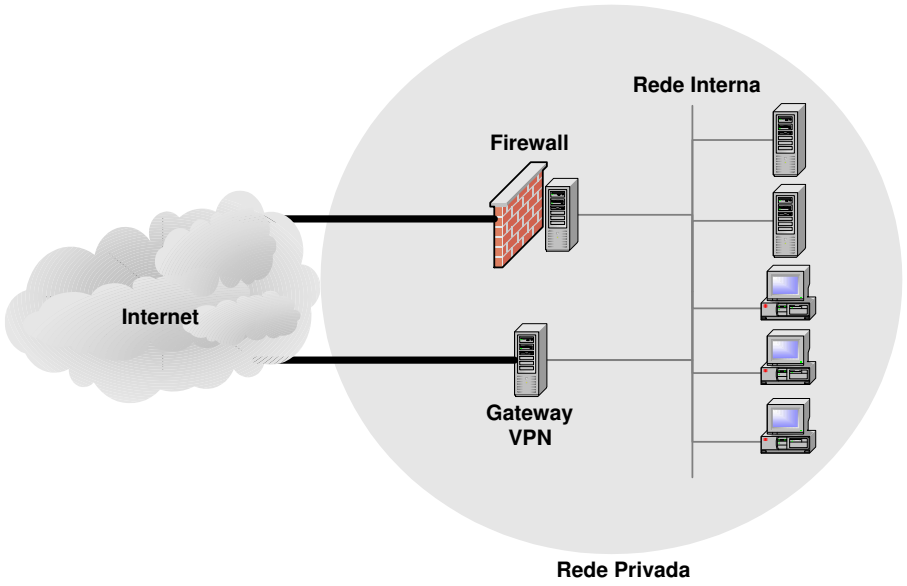


Figura 7.4: Gateway VPN em paralelo ao Firewall

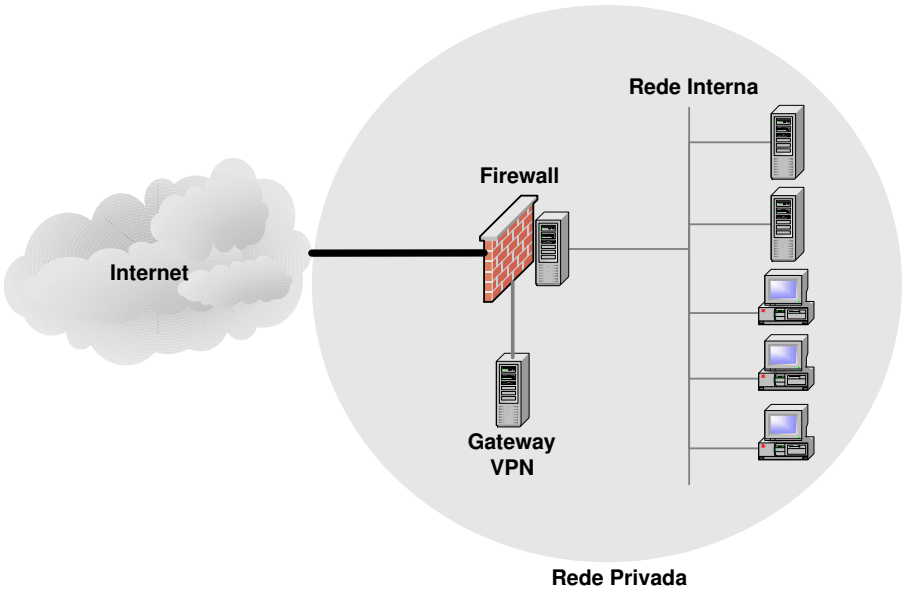


Figura 7.5: Gateway VPN ao lado do Firewall

Nesta estrutura o gateway VPN deve ser configurado para aceitar somente tráfego cifrado. Embora tal arranjo evite a existência de um ponto único de falha, o gateway VPN deve ele próprio se defender de ataques externos. Um problema ainda mais sério é que o tráfego decifrado não é submetido a qualquer controle antes de entrar na rede interna, expondo dessa forma os recursos da organização.

Portanto, não existe uma maneira de se aplicar a política de segurança da corporação à essa conexão. Tal configuração é extremamente perigosa, considerando que o gateway VPN constitui uma entrada alternativa para a rede interna, enfraquecendo o conceito de segurança perimetral introduzido pelo firewall.

7.1.5 Ao lado do firewall

A colocação do gateway VPN em uma interface dedicada do firewall, como ilustrado na Figura 7.5, comumente é referenciada como estando "ao lado do firewall".

Nesta configuração, o tráfego VPN seria tratado da seguinte forma: o firewall repassa o tráfego cifrado ao gateway VPN, que o decifra e o reenvia ao firewall, que por sua vez o analisa e o envia à rede privada.

Este arranjo protege o gateway VPN de ataques originados da Internet e, além disso, filtra todo o tráfego destinado à rede interna. Contudo, é importante observar que ela ocasiona uma pequena sobrecarga ao exigir que toda a comunicação relacionada à VPN passe duas vezes pelo firewall, antes e depois de ser decifrada.

A colocação do gateway VPN em uma interface dedicada do firewall é uma excelente opção, já que em uma configuração deste tipo todos os pacotes que chegam ao gateway VPN passam antes por um filtro de pacotes, o que fornece proteção contra ataques externos. Após passarem pelo gateway VPN, terem os cabeçalhos de tunelamento retirados e serem decifrados, os pacotes originais podem passar agora por um processo de filtragem adequado, o que não podia ser feito anteriormente por estarem completamente cifrados.

No entanto, existem outros detalhes referentes à correta integração do gateway VPN ao firewall. Questões importantes aparecem quando se pensa na adequação das regras do firewall à funcionalidade VPN.

A colocação de um gateway VPN dentro de uma arquitetura de firewall deve levar em conta o possível aumento na complexidade das regras de filtragem, pois muitas vezes é necessário lidar com cenários complexos de acesso de clientes remotos VPN e filiais da própria corporação. Esta complexidade crescente pode comprometer a administração segura dos equipamentos, podendo gerar brechas que facilitem um ataque.

Essa preocupação leva à escolha de um software de filtragem que seja flexível o suficiente para acomodar as novas regras de filtragem do modo mais transparente e simples possível, possibilitando o estabelecimento claro do escopo de cada bloco de regras. Nesse contexto, uma excelente alternativa é o filtro de pacotes IPTables do Linux, que possibilita a separação das regras em listas denominadas "cadeias". Ele possui 3 cadeias básicas: INPUT, que cuida dos pacotes destinados a processos locais; FORWARD, que cuida dos pacotes que transitam entre duas interfaces; e OUTPUT, que cuida dos pacotes originados nos processos locais [NdG02].

Com o uso do IPTables como software de filtragem, é possível construir as regras de modo que todas as filtragens referentes à VPN se localizem em uma única cadeia. Caso a complexidade das regras específicas da VPN seja considerável, é possível quebrar tal cadeia em regras menores, sempre na tentativa de facilitar a administração da segurança.

7.1.6 Gateway VPN na DMZ

A colocação do gateway VPN ao lado do firewall, em uma interface dedicada, é uma opção que oferece uma interessante integração entre os serviços providos pela VPN e as funcionalidades desempenhadas pelo firewall.

No entanto, em um ambiente corporativo é comum que existam diversos outros serviços além da VPN que devem estar acessíveis a usuários externos, como por exemplo, servidores Web, FTP e e-mail. Tais servidores normalmente ficam localizados em uma Zona Desmilitarizada (*Demilitarized Zone* – DMZ) [ZCC00], que pode ser definida como uma pequena sub-rede localizada entre a rede interna, confiável, e a rede externa, não confiável, em uma topologia clássica de ambiente seguro. A própria interface dedicada reservada ao

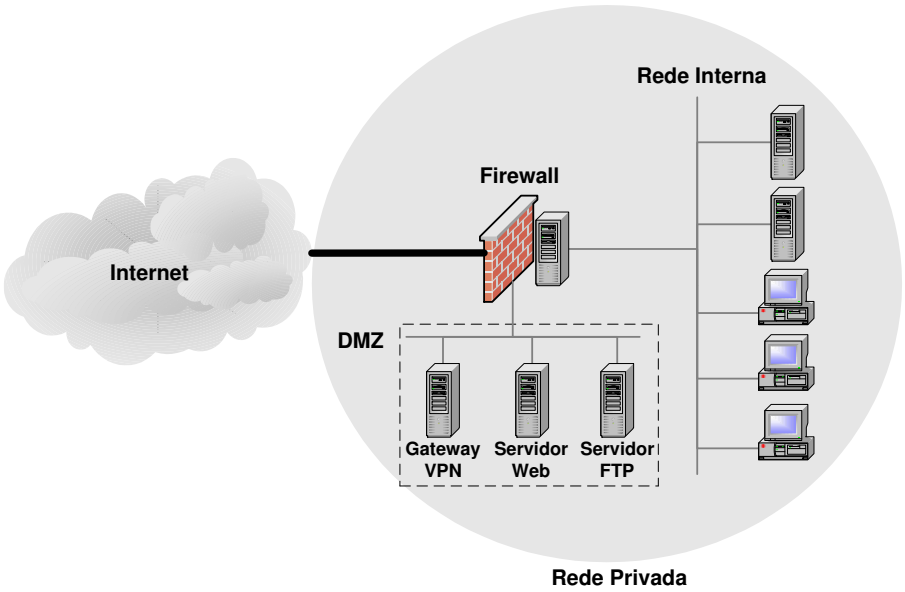


Figura 7.6: Gateway VPN em conjunto com outros equipamentos de uma DMZ

gateway VPN constitui uma DMZ.

Sendo assim, um outro aspecto importante a ser analisado é a correta integração do gateway VPN com os demais serviços existentes na rede. De uma forma geral, o gateway VPN pode assumir basicamente três posições específica dentro de uma DMZ: em conjunto com outros equipamentos de uma DMZ, em uma DMZ separada ou em uma configuração de múltiplas DMZs. Cada uma dessas configurações será vista em mais detalhes a seguir.

Em conjunto com outros equipamentos de uma DMZ

Uma possível configuração do gateway VPN ao lado do firewall é sua colocação em conjunto com outros equipamentos de uma DMZ, como ilustrado na Figura 7.6. Estes equipamentos tipicamente oferecem serviços a usuários externos à corporação, e possivelmente algum acesso específico a usuários internos. Os desdobramentos deste tipo de colocação dependem do perfil de usuário que tem acesso à VPN.

No caso de uma VPN ligando parceiros de uma rede externa, o tráfego que chega pelo gateway VPN pode não estar destinado, a priori, a qualquer um dos servidores situados na DMZ, e sim para algum outro destino. Neste caso, o tráfego decifrado é passível de filtragem antes de alcançar o seu destino, pois após ser decifrado pelo gateway VPN, tem que passar novamente pelo firewall. Contudo, esta configuração não impede que um usuário malicioso, situado na rede do parceiro, envie pacotes aos servidores situados na DMZ. Quando isto acontece, os pacotes originados na rede desses parceiros não são submetidos às regras adequadas de filtragem, pois o datagrama IP interno tunelado pela

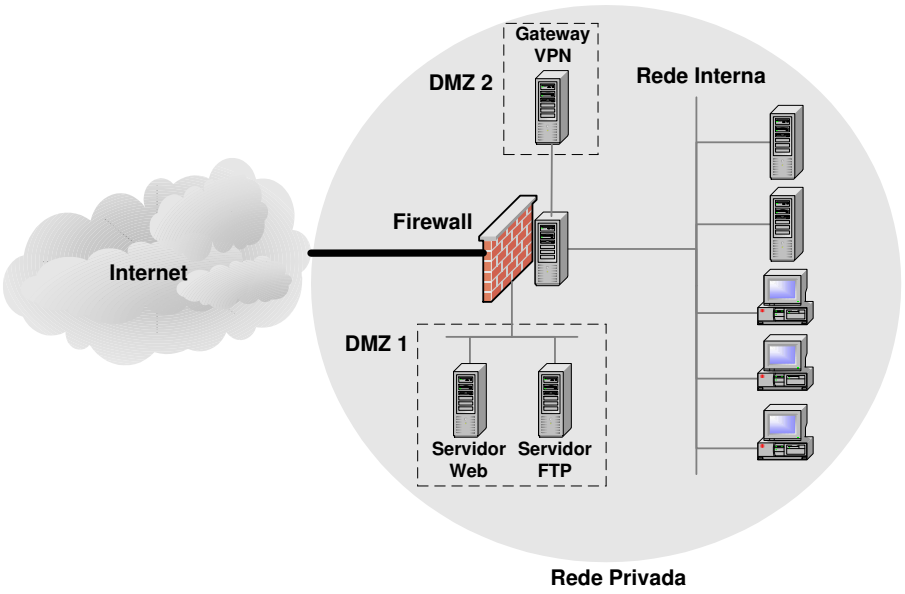


Figura 7.7: Gateway VPN em uma DMZ separada

VPN passa pelo firewall uma única vez de forma cifrada, impedindo a filtragem de seu conteúdo. Dessa forma, uma parte da política de segurança da organização, expressa através de regras de filtragem, não será aplicada a uma parcela importante do tráfego da rede.

Quando na outra extremidade da VPN há uma filial da empresa, a situação também é parecida. Este tipo de arquitetura é um tanto confusa, pois há a mistura de tráfego proveniente de uma rede considerada confiável com tráfego originado por usuários externos. Nesse caso, o comprometimento de qualquer um dos servidores localizados na DMZ implicará em uma possível observação de todo o tráfego da VPN, sem qualquer proteção que garanta a confidencialidade das informações.

Em uma DMZ separada

Muitos dos problemas anteriormente mencionados podem ser solucionados com a colocação do gateway VPN em uma DMZ separada, como mostrado na Figura 7.7, pois esta nova configuração proporciona um isolamento do tráfego da VPN em relação ao tráfego destinado a outros servidores.

A complexidade de configuração nas regras do firewall são maiores, pois há a necessidade da adição de mais uma interface para administração e aplicação de regras. Porém, com o uso de softwares como o IPTables, é possível que haja um conjunto de regras de filtragem a ser aplicado numa determinada interface em um bloco separado. Isto torna a administração destas regras mais simples, controlando de modo mais transparente os

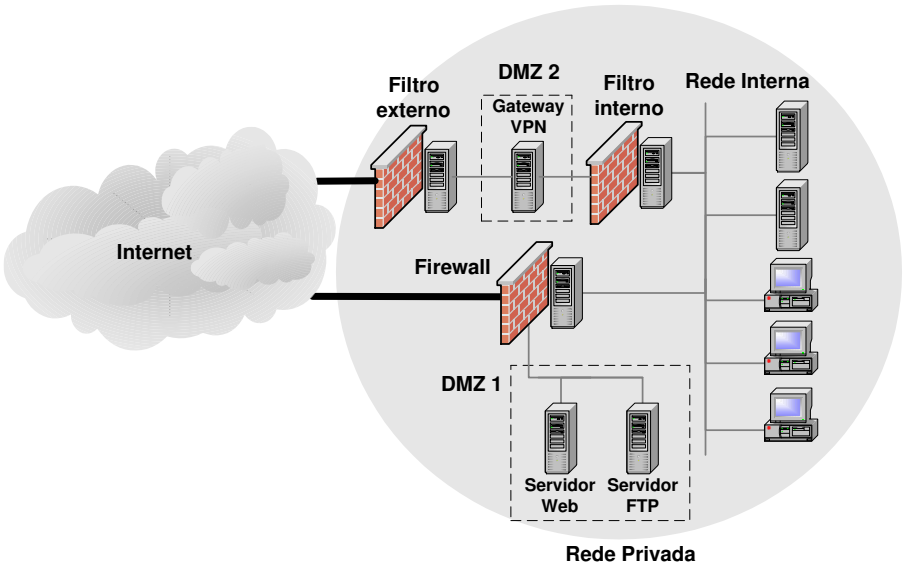


Figura 7.8: Gateway VPN em uma configuração de múltiplas DMZs

acessos aos recursos da VPN.

É possível também aproveitar a existência desta DMZ para a inclusão de alguns outros serviços necessários aos usuários remotos ou de redes externas cooperativas [NdG02], evitando o acesso desnecessário à rede interna para atender a solicitações de usuários dessa natureza. É importante destacar que, neste caso específico, não será realizada novamente a filtragem dos pacotes destinados aos servidores localizados na DMZ onde se encontra o gateway VPN.

Sendo assim, a solução que oferece um maior nível de segurança é a colocação do gateway VPN isoladamente dentro dessa nova DMZ, sendo todo o tráfego da VPN encaminhado adequadamente para seu destino, seja ele a rede interna ou mesmo outra DMZ.

Este tipo de solução apresenta a grande vantagem de permitir uma distinção bem clara do que é ou não tráfego da VPN. Dessa forma, a aplicação da política de segurança expressa através das regras de filtragem pode assumir um caráter mais específico de acordo com o perfil de usuário da VPN.

Em uma configuração de múltiplas DMZs

Uma alternativa que pode se tornar interessante em alguns casos é colocação do gateway VPN em uma DMZ completamente distinta, em uma configuração de múltiplas DMZs, como ilustrado na Figura 7.8. Nesta situação, que pode ser considerada um extensão do cenário anterior, existe um filtro externo e um filtro interno reservados exclusivamente para a VPN.

As vantagens dessa abordagem são a maior facilidade de gerenciamento nas regras de filtragem e no roteamento do tráfego relacionado à VPN, tornando a distinção entre tráfego VPN e tráfego externo ainda mais clara. Além disso, essa nova abordagem diminui a sobrecarga no firewall da corporação.

Nesse cenário, qualquer alteração nas regras relacionadas à VPN não afeta as regras mais gerais de filtragem do firewall. Mesmo a regras de filtragem da própria VPN podem ser divididas em dois conjuntos completamente distintos, devido à existência de um filtro externo e um filtro interno dedicados.

É claro que uma configuração deste tipo implica em uma duplicação dos recursos físicos necessários e em um custo adicional significativo.

Isto pode ser minimizado com a combinação do gateway VPN e o filtro externo ou interno em um único equipamento. Diversas soluções comerciais e não comerciais se baseiam neste tipo de topologia. Porém, este cenário recai nos mesmos problemas de cenários semelhantes apresentados anteriormente, constituindo um único ponto de falha e expondo os filtros à exploração de vulnerabilidades existentes no software utilizado no gateway VPN.

Além disso, tal configuração pode se tornar perigosa, considerando que a adição de uma entrada alternativa para a rede interna enfraquece o conceito de segurança perimetral introduzido pelo firewall.

Capítulo 8

Conclusão

O acesso remoto VPN possui uma grande aplicabilidade em um ambiente cooperativo, onde os usuários remotos podem deixar de realizar ligações interurbanas, acessando os recursos da organização utilizando um túnel virtual criado através da Internet.

Além disso, a utilização de uma rede pública, como a Internet, proporciona uma redução no custos e uma maior flexibilidade e escalabilidade com relação a usuários remotos e a mudanças nas conexões, se comparado com as conexões privadas, que possuem custos altos para mudanças em sua infra-estrutura.

Contudo, junto a esses benefícios, surgem também uma série de implicações, principalmente quanto à segurança das informações, que passam a correr riscos com relação à sua confidencialidade e à sua integridade, já que passam a trafegar através de uma rede pública.

Nesse contexto, a utilização de mecanismos capazes de suprir as necessidades de segurança impostas torna-se fundamental. É importante também que tais mecanismos atendam a requisitos relacionados a performance, flexibilidade, interoperabilidade e escalabilidade.

A carência de mecanismos capazes de proteger o acesso remoto VPN culminou na especificação de diferentes protocolos. Após a análise dos principais protocolos utilizados foi possível observar alguns dos pontos positivos e negativos de cada tecnologia, facilitando assim a opção por uma tecnologia mais adequada às necessidades de cada cenário.

Como resultado dessa análise, foi possível constatar a existência de diversas falhas de segurança nos protocolos PPTP e L2TP, inviabilizando o uso desses protocolos em ambientes onde seja exigido um nível de segurança aceitável. A utilização do protocolo L2TP protegido pelo protocolo IPSec, apresenta muitas das funcionalidades necessárias para o acesso remoto VPN. Contudo, tal solução causa um overhead considerável na pilha de protocolos, além de outros problemas operacionais, não apresentando na prática bons resultados. A conclusão final desta análise foi que a utilização do protocolo IPSec em modo

túnel é a solução mais adequada ao acesso remoto VPN, devido às suas características de segurança mais capazes.

No entanto, existem vários diferentes cenários possíveis de acesso remoto VPN utilizando IPSec, que possuem de uma maneira geral, em maior ou menor grau, requisitos em comum importantes para a completa viabilidade de uma solução, como a autenticação dos extremos da comunicação, a configuração do sistema remoto, a configuração das políticas de segurança, o registro de eventos e a passagem por intermediários.

Analisando algumas das soluções existentes para cada um desses requisitos, foi possível avaliar as vantagens e desvantagens de cada um desses mecanismos, facilitando a opção por tecnologias que atendam mais convenientemente a cada uma das exigências, e que provavelmente virão a se tornar um padrão.

Avaliando os mecanismos propostos para prover o suporte a autenticação legada no IPSec, foi possível perceber, por exemplo, que o XAUTH apresenta algumas falhas conceituais que inviabilizam o seu uso em algumas circunstâncias. Também ficou patente que mecanismos que exigem modificações no atual padrão do protocolo IKE, como o XAUTH, a autenticação híbrida e o CRACK, apesar de já se encontrarem implementados em algumas soluções comerciais, certamente não serão padronizados pelo IETF. Já mecanismos como o PIC, atendem perfeitamente aos requisitos apresentados pelo *IPSRA Working* Group do IETF, vindo a ser provavelmente a solução padrão para esta funcionalidade.

A apresentação dos mecanismos de configuração do sistema remoto, também nos permitiu avaliar as principais características das soluções atualmente mais utilizadas, o ModeConfig e o DHCP sobre IPSec. Ambos possuem funcionalidades interessantes, o que provavelmente levará o primeiro a ser incluído na especificação do protocolo IKEv2 sendo desenvolvido pelo IETF, e que levou o segundo a ser padronizado durante a realização deste trabalho, por apresentar uma maior flexibilidade na configurações e não exigir modificação no atual padrão do IKE.

O estudo dos aspectos de configuração da política de segurança levantou alguns pontos importantes como a necessidade de proteção da máquina remota, possivelmente utilizando softwares anti-vírus e firewalls pessoais gerenciáveis, a fim de impedir que este sistema seja utilizado como ponte para um ataque à rede da organização. Outras considerações importantes também foram feitas em relação às aspectos que devem ser levados em conta durante a concepção de uma política de segurança que atenda aos cenários de acesso remoto VPN.

Por fim, a análise das soluções existentes também possibilitou uma visão mais abrangente dos problemas envolvidos na passagem de tráfego IPSec por um dispositivo de NAT e também um melhor entendimento da solução atualmente mais utilizada, o NAT Traversal.

Como resultado desse amplo estudo realizado sobre os diversos aspectos relaciona-

dos ao acesso remoto VPN, foi possível implementar uma solução baseada no software FreeS/WAN sobre sistemas Linux. Tal solução procurou abranger diversas tecnologias recentes e promissoras, além de prover compatibilidade com clientes VPN utilizando sistemas Windows.

Além disso, várias características não suportadas nativamente pelo FreeS/WAN, como o suporte a autenticação e controle de acesso baseado em certificados digitais, a configuração do sistema remoto utilizando o protocolo DHCP sobre IPSec e o suporte ao NAT-T para a passagem por dispositivos de NAT intermediários, foram incorporadas a essa solução com a adição de alguns patchs.

Dessa forma foi possível desenvolver uma solução segura e viável de acesso remoto VPN que, além de ser uma alternativa de baixo custo por ser baseada em um software Open Source como o FreeS/WAN, possui ainda compatibilidade com o software cliente VPN nativo dos sistemas operacionais Windows e também é compatível com outras soluções comerciais.

Um outro ponto que merece atenção especial em relação à segurança do acesso remoto VPN é a adição do gateway VPN na estrutura de segurança já existente de um ambiente corporativo. Isto porque uma decisão inadequada pode comprometer não só a segurança das informações que trafegam através da VPN, mas também a segurança da rede privada como um todo.

Após uma análise de todos os aspectos envolvidos nesse processo, foi possível concluir que a opção mais adequada de posicionamento do gateway VPN na estrutura de um ambiente clássico de rede segura é ao lado do firewall, em uma DMZ separada. Tal configuração permite uma clara diferenciação entre o tráfego que faz e o que não faz parte da VPN, possibilitando uma aplicação mais efetiva da política de segurança definida para o acesso remoto.

8.1 Trabalhos futuros

Diversos aspectos de segurança foram abordados neste trabalho, com o intuito de garantir um nível de segurança aceitável no acesso remoto VPN. Contudo, apesar da segurança ser um fator obrigatório em uma solução VPN, diversos outros aspectos também necessitam de um estudo aprofundado para o provimento de uma solução que seja realmente escalável e ao mesmo tempo gerenciável.

Um fato relevante é que com o crescimento no número de clientes remotos e conexões VPN em geral, um único gateway VPN torna-se incapaz de atender e gerenciar à demanda de túneis IPSec criados. Isto ocorre não só por limitações nos equipamentos, mas também pelo uso intenso de pesados algoritmos criptográficos e pelo aumento na complexidade do roteamento necessário. Dessa forma, é importante que sejam estudadas formas de facilitar

e suportar esse crescimento, que é uma conseqüência natural do uso dessa tecnologia. Além disso, em ambientes cooperativos com um alto grau de conectividade, torna-se bem mais difícil gerenciar os limites de acesso de um determinado usuário.

A tradução efetiva das políticas de segurança em alto nível para sua respectiva implementação em baixo nível, também constitui um problema ainda difícil de ser solucionado. Principalmente em relação aos sistemas remotos, onde a segurança física é difícil de ser implementada. Por isso, o desenvolvimento de mecanismos que permitam impor certas restrições e configurações a sistemas remotos é um tópico que deve ser alvo de intensa pesquisa.

Além desses, diversos outros fatores envolvidos em um cenário de acesso remoto ainda permanecem em aberto. Desde uma interatividade mais amigável com o usuário final até a integração com tecnologias de rede amplamente difundidas, muitas das barreiras impostas ao acesso remoto VPN ainda precisam ser superadas, necessitando do desenvolvimento de trabalhos que apresentem alternativas viáveis para a efetiva disseminação e popularização desta tecnologia.

Apêndice A

Arquivos de Configuração

O FreeS/WAN é composto basicamente por duas partes fundamentais, o KLIPS e o Pluto. O KLIPS é a implementação IPSec propriamente dita, responsável pela adição dos cabeçalhos AH e ESP, e também pelo tratamento dos pacotes dentro do kernel. Já o Pluto é a implementação de um daemon IKE, responsável pela negociação dos parâmetros específicos de cada conexão e pelo estabelecimento de associações de segurança (SAs).

As configurações do FreeS/WAN se concentram de maneira geral em dois arquivos. O primeiro deles, o arquivo `ipsec.conf`, contém todos os parâmetros que determinam o comportamento do FreeS/WAN, bem como as definições relacionadas ao roteamento e à criação de associações de segurança, sendo composto por seções de configuração (`config`) e seções de conexão (`conn`). O segundo arquivo, denominado `ipsec.secrets`, contém informações sobre os segredos pré-compartilhados e as chaves privadas necessárias na autenticação dos extremos do túnel IPSec.

A seguir serão apresentados alguns exemplos de arquivos de configuração que ilustram uma implementação de acesso remoto VPN utilizando FreeS/WAN. Para uma melhor compreensão dessas configurações, serão detalhadas também as opções e funcionalidades providas por cada parâmetro.

A.1 Exemplo de configuração

Um exemplo de arquivo de configuração `ipsec.conf` para conexões de acesso remoto VPN, com suporte a atribuição de endereços IP virtuais utilizando DHCP sobre IPSec, é mostrado a seguir:

```
config setup
    interfaces="ipsec0=eth0 ipsec1=eth1"
    klipsdebug=none
```

```
    plutodebug=none
    plutoload=%search
    plutostart=%search
    hidetos=no
    uniqueids=yes
    plutowait=no
    nat_traversal=yes
    virtual_private=%v4:10.1.2.0/255.255.255.0

conn %default
    keyingtries=10
    disablearrivalcheck=no
    authby=rsasig
    leftrsasigkey=%cert
    leftcert=gatewayVPN.pem
    left=143.106.60.15
    leftnexthop=143.106.60.1
    leftid="C=BR,O=UNICAMP,OU=IC,CN=GatewayVPN"
    rightrsasigkey=%cert
    auto=route
    keylife=20m
    rekeymargin=5m
    ikelifetime=3h
    ike=aes128-sha,aes128-md5
    esp=aes128-sha,aes128-md5
    pfsgroup=modp1536

conn vpn-dhcp
    right=%any
    rightsubnet=vnet:%all
    leftsubnet=0.0.0.0/0.0.0.0
    leftprotoport=udp/bootps
    rightprotoport=udp/bootpc
    rekey=no
    keylife=20s
    rekeymargin=10s
    auto=add
```

```
conn AcessoRemotoVPN
    right=%any
    rightid=*@las.ic.unicamp.br
    rightsubnetwithin=10.1.2.0/24
    # rightsubnet=vnet:%priv
    leftsubnet=10.1.1.0/255.255.255.0
    auto=add
    leftupdown=/etc/ipsec.d/X509updown

conn ClientesSSHSentinel
    right=%any
    rightid="C=BR,O=UNICAMP,OU=IC,CN=*"
    rightsubnetwithin=10.1.2.0/255.255.255.0
    # rightsubnet=vnet:%priv
    leftsubnet=0.0.0.0/0.0.0.0
    auto=add
    leftupdown=/etc/ipsec.d/X509updown
```

Para permitir o suporte à autenticação utilizando certificados digitais, um exemplo de arquivo de configuração `ipsec.secrets` seria o seguinte:

```
: RSA myKey1.pem %prompt
: RSA myKey2.pem "<passphrase opcional>"
```

O uso do parâmetro `%prompt` permite que a *passphrase* que protege a chave privada seja fornecida interativamente pelo usuário, garantindo um maior nível de segurança em relação às *passphrases* armazenadas no próprio arquivo `ipsec.secrets`.

A.2 Seções de configuração (`config`)

Uma seção de configuração (`config`) define os parâmetros necessários ao funcionamento do FreeS/WAN, determinando o comportamento inicial do Pluto e do KLIPS. A única seção de configuração atualmente definida para o FreeS/WAN é a seção denominada `config setup`.

Exemplos de parâmetros utilizados em uma seção de configuração (`config setup`) são:

- `interfaces="ipsec0=eth0 ipsec1=eth1"` — associa uma interface ipsec a uma interface física

▷ `%defaultroute` — será associada à interface ipsec a interface física usada para acessar o gateway default

- `forwardcontrol=yes|no(default)` — determina se o FreeS/WAN deve ou não habilitar o repasse de pacotes IP (*IP forwarding*) quando for iniciado ou finalizado.

- `plutowait=yes(default)|no` — define se o Pluto deve aguardar o estabelecimento de uma conexão antes de iniciar o estabelecimento de outra conexão.

- `plutodebug=none|all` — habilita ou desabilita a geração de logs do Pluto

- `klipsdebug=none|all` — habilita ou desabilita a geração de logs do KLIPS

- `plutoload=list` — lista de conexões que o Pluto deve adicionar à sua base de dados ao ser iniciado

  ▷ `%search` — significa que o Pluto deve procurar nas definições de conexão pelo valor do parâmetro `auto`

- `plutostart=list` — lista de conexões que o Pluto deve ativar ao ser iniciado

  ▷ `%search` — significa que o Pluto deve procurar nas definições de conexão pelo valor do parâmetro `auto`

- `prepluto=pathname` — define o script que deve ser executado antes do Pluto ser iniciado

- `postpluto=pathname` — define o script que deve ser executado após o Pluto ser iniciado

- `fragicmp=yes(default)|no` — envia ao usuário um pacote ICMP para reduzir a MTU se necessário para evitar fragmentação

- `hidetos=yes(default)|no` — define se os bits de TOS (*Type Of Service*) no pacote IPSec devem ser preenchidos com 0, a despeito do seu valor no pacote original

- `uniqueids=yes(default)|no` — determina se uma nova conexão contendo o mesmo ID de uma conexão existente sobrepõe a conexão antiga

- `overridemtu=value` — redefine a MTU padrão das interfaces IPSec

- `nat_traversal=yes|no` — habilita ou desabilita o suporte ao NAT-T

- `virtual_private=%method` — define a faixa de endereços privados que será aceita como válida. O caracter "!" pode ser utilizado para indicar negação. O parâmetro `%method` pode assumir um dos seguintes valores:
  - ▷ `%no` — rejeita endereços IP virtuais, aceitando somente endereços IP públicos
  - ▷ `%v4:x` — aceita qualquer endereço IPv4 listado em `x`
  - ▷ `%v6:x` — aceita qualquer endereço IPv6 listado em `x`
  - ▷ `%all` — aceita qualquer endereço IP virtual

    $\Longrightarrow$ Necessário na definição de conexões DHCP
- `strictcrlpolicy=yes|no(default)` — define se serão aceitos ou rejeitados certificados emitidos por uma CA para a qual não há uma CRL válida.

A.3 Seções de conexão (`conn`)

As seções de conexão (`conn`) definem os parâmetros relacionados ao roteamento e à criação de associações de segurança (SAs). Usualmente, existem múltiplas seções de conexão distintas que definem, cada uma, parâmetros específicos relacionados a uma determinada conexão ou classe de usuário. Os parâmetros comuns a todas as conexões podem ser definidos em uma seção denominada `conn %default`, que estabelece os valores que serão assumidos para uma variável caso ela não seja definida em uma seção de conexão específica.

Exemplos de parâmetros utilizados em uma seção de conexão (`conn name`) são:

- `left=x.x.x.x` — define o endereço IP de um dos extremos do túnel, normalmente o endereço IP público do gateway VPN
  - ▷ `%defaultroute` — será usado o endereço IP da interface usada para acessar o gateway default
  - ▷ `%any` — significa que será aceito qualquer endereço IP durante a negociação IKE, sendo normalmente usado em cenários de acesso remotos
- `right=y.y.y.y` — define o endereço IP do outro extremo do túnel, normalmente usado como `%any` em cenários de acesso remoto
- `leftnexthop=z.z.z.z` — define o próximo roteador no caminho para esta conexão, que normalmente é o gateway default

  $\Longrightarrow$ Não deve ser definido se o parâmetro `left` for preenchido com o valor `%defaultroute`

▷ `%direct` — significa que o nó está diretamente ligado à rede

▷ `%defaultroute` — utiliza o gateway default

⟹ Requer que o parâmetro interfaces na seção config seja preenchido com o valor `%defaultroute`

- `leftsubnet=x.x.x.x/m.m.m.m|x.x.x.x/bits` — define a rede privada que será acessada

- `rightsubnet=x.x.x.x/m.m.m.m|x.x.x.x/bits` — define a rede protegida pelo outro extremo do túnel, podendo também ser o cliente remoto

- `rightsubnetwithin=x.x.x.x/m.m.m.m|x.x.x.x/bits` — define a faixa aceita como endereço IP virtual do cliente remoto em conexões utilizando o DHCP sobre IPSec

- `rightsubnet=type:%method` — define a faixa aceita como endereço IP virtual do cliente remoto.

  O parâmetro `type` pode assumir um dos seguintes valores:

  ▷ `vhost` — será definido o endereço IP da máquina

  ▷ `vnet` — será definida uma faixa de endereços IP aceitos

  O parâmetro `%method` pode assumir um dos seguintes valores:

  ▷ `%no` — rejeita endereços IP virtuais, aceitando somente endereços IP públicos

  ▷ `%priv` — aceita os endereços IP virtuais definidos no parâmetro `virtual_private`

  ▷ `%v4:x` — aceita qualquer endereço IPv4 listado em `x`

  ▷ `%v6:x` — aceita qualquer endereço IPv6 listado em `x`

  ▷ `%all` — aceita qualquer endereço IP virtual

  ⟹ Necessário na definição de conexões DHCP

- `leftupdown=pathname` — define o script que será executado durante a inicialização da conexão onde esse parâmetro foi definido

- `authby=secret(default)|rsasig` — define o método de autenticação utilizado, podendo ser:

  ▷ `secret` — segredos pré-compartilhados

  ▷ `rsasig` — assinaturas digitais RSA, necessário para o uso de certificados X.509

- `auto=add|route|start|ignore(default)` — define o que deve ser feito com cada conexão durante a inicialização do FreeS/WAN. Este parâmetro só é válido quando os parâmetros `plutostart` e `plutoload` estiverem preenchido com o valor `%search`.
  - ▷ `add` — adiciona a conexão à base de dados do Pluto
  - ▷ `route` — adiciona a conexão e estabelece a rota apropriada
  - ▷ `start` — adiciona a conexão, estabelece a rota apropriada e inicia a conexão
  - ▷ `ignore` — ignora a conexão
- `leftid=ID` — define o identificador (`ID`) usado para autenticar uma conexão
- `leftcert=pathname` — define que certificado será utilizado para uma conexão
- `leftrsasigkey=public_key` — define a chave pública utilizada em uma conexão
  - ▷ `%dns` — a chave pública será obtida através do DNS
  - ▷ `%cert` — a chave púbica será obtida através de um certificado digital
- `leftrsasigkey2=public_key` — permite o uso de uma segunda chave pública
- `leftprotoport=ip_protocol/port` — especifica que protocolo provocará o estabelecimento da conexão
- `pfs=yes(default)|no` — habilita ou desabilita o uso de PFS (*Perfect Forward Secrecy*)
- `pfsgroup=modp1024|1536|2048|3072|4096` — determina o grupo Diffie-Hellman usado na Fase 2 do IKE
- `ike=list` — especifica os algoritmos propostos na Fase 1 do IKE, como por exemplo, `ike=aes128-sha,aes128-md5,3des-sha,3des-md5`
- `esp=list` — especifica os algoritmos propostos na Fase 2 do IKE, como por exemplo, `esp=aes128-sha1,aes128-md5,3des-sha1,3des-md5`
- `keylife=(number)s|m|h|d` — define o tempo de vida da chave utilizada na Fase 2 do IKE, podendo ser informado em segundos (`s`), minutos (`m`), horas (`h`) ou dias (`d`)
- `rekey=yes(default)|no` — habilita ou desabilita a renovação de chaves após a chave utilizada ter expirado
- `rekeymargin=(number)s|m|h|d` — define quanto tempo antes da chave atual expirar deve ser feita a renovação

- `rekeyfuzz=x%` — define a porcentagem máxima que o valor de `rekeymargin` pode aumentar aleatoriamente a fim de criar um padrão de chave mais aleatório
- `keyingtries=number` — define o número máximo de tentativas de renovação de chaves
- `ikelifetime=(number)s|m|h|d` — define o tempo de vida da Fase 1 do IKE
- `compress=yes|no(default)` — habilita ou desabilita a compressão dos dados antes de ser realizada a cifragem
- `disablearrivalcheck=yes(default)|no` — habilita ou desabilita a checagem da validade dos pacotes após passarem pelo KLIPS

Glossário

AC	Autoridade Certificadora
AH	*Authentication Header*
ARP	*Address Resolution Protocol*
AS	*Authentication Server*
ATM	*Asynchronous Transfer Mode*
CCP	*Compression Control Protocol*
CHAP	*Challenge Handshake Authentication Protocol*
CRACK	*IKE Challenge/Response for Authenticated Cryptographic Keys*
DDoS	*Distributed Denial-of-Service*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DoS	*Denial-of-Service*
DSL	*Digital Line Subscriber*
EAP	*Extensible Authentication Protocol*
ECP	*Encryption Control Protocol*
ESP	*Encapsulation Security Payload*
GRE	*Generic Routing Encapsulation*
ICP	Infra-estrutura de Chaves Públicas

IETF *Internet Engineering Task Force*

IKE *Internet Key Exchange*

IKEv2 *Internet Key Exchange version 2*

IP *Internet Protocol*

IPCP *Internet Protocol Control Protocol*

IPSec *Internet Protocol Security*

IPSRA *IP Security Remote Access Working Group*

ISAKMP *Internet Security Association and Key Management Protocol*

ISO *International Standards Organization*

ISP *Internet Service Provider*

L2F *Layer 2 Forwarding*

L2TP *Layer Two Tunneling Protocol*

LAN *Local Area Network*

LCR Lista de Certificados Revogados

LDAP *Lightweight Directory Access Protocol*

MMC *Microsoft Management Console*

MTU *Maximum Transmission Unit*

NAPT *Network Address Port Translation*

NAS *Network Access Server*

NAT *Network Address Translation*

NAT-D *NAT Discovery*

NAT-T *NAT Traversal*

NetBIOS *Network Basic Input Output System*

NIS *Network Information System*

NTP *Network Time Protocol*

OCSP *Online Certificate Status Protocol*

OSI *Open Systems Interconnect*

OTP *One Time Password*

PAT *Port Address Translation*

PFS *Perfect Forward Secrecy*

PIC *Pre-IKE Credential Provisioning Protocol*

PIN *Personal Identification Number*

POP *Post Office Protocol*

PPP *Point-to-Point Protocol*

PPTP *Point-to-Point Tunneling Protocol*

PSTN *Public Switched Telephone Network*

RADIUS *Remote Authentication Dial-In User Service*

SA *Security Association*

SAD *Security Association Database*

SMTP *Simple Mail Transfer Protocol*

SNMP *Simple Network Management Protocol*

SPD *Security Policy Database*

SSL *Secure Sockets Layer*

TTL *Time to Live*

URI *Uniform Resource Indicator*

VIP *Virtual IP*

VPN *Virtual Private Network*

WINS *Windows Internet Naming Service*

XAUTH *IKE Extended Authentication*

Referências Bibliográficas

[AL99] Carlisle Adams and Steve Lloyd. *Understanding Public-Key Infrastructure (PKI)*. NewRiders Publishing, 1999.

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

[Bel97] Steven M. Bellovin. Probable Plaintext Cryptanalysis of the IP Security Protocols. In *Proceedings of the Symposium on Network and Distributed System Security*, pages 155–160, San Diego, California, 1997.

[BM00] S. Bellovin and B. Moskowitz. *Client Certificate and Key Retrieval for IKE*. Internet Engineering Task Force, Internet Draft, 2000.

[BV98] L. Blunk and J. Vollbrecht. *PPP Extensible Authentication Protocol (EAP)*. Internet Engineering Task Force, RFC 2284, 1998.

[DA01] R. Droms and W. Arbaugh. *Authentication for DHCP Messages*. Internet Engineering Task Force, RFC 3118, 2001.

[dRdG02] Edmar R. S. de Rezende and 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, Brazil, 2002.

[Dro97] R. Droms. *Dynamic Host Configuration Protocol*. Internet Engineering Task Force, RFC 2131, 1997.

[EF94] K. Egevang and P. Francis. *The IP Network Address Translator (NAT)*. Internet Engineering Task Force, RFC 1631, 1994.

[Far00] D. Farinacci. *Generic Routing Encapsulation (GRE)*. Internet Engineering Task Force, RFC 2784, 2000.

[FdG02] Francisco J. C. Figueiredo and 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, Brazil, 2002.

[Fra01] Sheila Frankel. *Demystifying the IPsec Puzzle*. Artech House, Norwood, Massachusetts, 2001.

[Gle00] B. Gleeson. *A Framework for IP based Virtual Private Networks*. Internet Engineering Task Force, RFC 2764, 2000.

[Ham99] K. Hamzeh. *Point-to-Point Tunneling Protocol (PPTP)*. Internet Engineering Task Force, RFC 2637, 1999.

[HC98] D. Harkins and D. Carrel. *The Internet Key Exchange (IKE)*. Internet Engineering Task Force, RFC 2409, 1998.

[HKP99] D. Harkins, B. Korver, and D. Piper. *IKE Challenge/Response for Authenticated Cryptographic Keys*. Internet Engineering Task Force, Internet Draft, 1999.

[JRV03] J. Jason, L. Rafalow, and E. Vyncke. *IPsec Configuration Policy Information Model*. Internet Engineering Task Force, RFC 3585, 2003.

[KA98a] S. Kent and R. Atkinson. *IP Authentication Header (AH)*. Internet Engineering Task Force, RFC 2402, 1998.

[KA98b] S. Kent and R. Atkinson. *IP Encapsulating Security Payload (ESP)*. Internet Engineering Task Force, RFC 2406, 1998.

[KA98c] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*. Internet Engineering Task Force, RFC 2401, 1998.

[Kau03] Charlie Kaufman. *Internet Key Exchange (IKEv2) Protocol*. Internet Engineering Task Force, Internet Draft, 2003.

[Kin03] Christopher M. King. The 8 Hurdles to VPN Deployment. Disponível em: <http://infosecuritymag.techtarget.com/articles/1999/vpn.shtml>, Acesso em: 11/10/2003.

[Kle90] Daniel V. Klein. "Foiling the Cracker" – A Survey of, and Improvements to, Password Security. In *Proceedings of the second USENIX Workshop on Security*, pages 5–14, Summer 1990.

[KR03a] S. Kelly and S. Ramamoorthi. *Requirements for IPsec Remote Access Scenario*. Internet Engineering Task Force, RFC 3457, 2003.

[KR03b] Brian Korver and Eric Rescorla. *The Internet IP Security PKI Profile of ISAKMP and PKIX*. Internet Engineering Task Force, Internet Draft, 2003.

[Kra96] H. Krawczyk. SKEME: A Versatile Secure Key Exchange Mechanism for Internet. In *IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security*, 1996.

[KSHV03] T. Kivinen, B. Swander, A. Huttunen, and V. Volpe. *Negotiation of NAT-Traversal in the IKE*. Internet Engineering Task Force, Internet Draft, 2003.

[LSZ00] M. Litvin, R. Shamir, and T. Zegman. *A Hybrid Authentication Mode for IKE*. Internet Engineering Task Force, Internet Draft, 2000.

[MAM+99] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. Internet Engineering Task Force, RFC 2560, 1999.

[McG92] G. McGregor. *The PPP Internet Protocol Control Protocol (IPCP)*. Internet Engineering Task Force, RFC 1332, 1992.

[Mey96] G. Meyer. *PPP Encryption Control Protocol (ECP)*. Internet Engineering Task Force, RFC 1968, 1996.

[MMS98] D. Maughan and et al. M. Schertler. *Internet Security and Key Management Protocol (ISAKMP)*. Internet Engineering Task Force, RFC 2408, 1998.

[NdG02] Emílio Tissato Nakamura and Paulo Lício de Geus. *Segurança de Redes em Ambientes Cooperativos*. Editora Berkeley, São Paulo, Brasil, 2002.

[Orm98] H. Orman. *The OAKLEY Key Determination Protocol*. Internet Engineering Task Force, RFC 2412, 1998.

[PAKG03] B. Patel, B. Aboba, S. Kelly, and V. Gupta. *Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPSec Tunnel Mode*. Internet Engineering Task Force, RFC 3456, 2003.

[PAP99] R. Pereira, S. Anand, and B. Patel. *The ISAKMP Configuration Method*. Internet Engineering Task Force, Internet Draft, 1999.

[Pat01a] B. Patel. *Securing L2TP Using IPSec*. Internet Engineering Task Force, RFC 3193, 2001.

[Pat01b] M. Patrick. *DHCP Relay Agent Information Option.* Internet Engineering Task Force, RFC 3046, 2001.

[PB99] R. Pereira and S. Beaulieu. *Extended Authentication within ISAKMP/Oakley (XAUTH).* Internet Engineering Task Force, Internet Draft, 1999.

[Pip98] D. Piper. *The Internet IP Security Domain Of Interpretation for ISAKMP.* Internet Engineering Task Force, RFC 2407, 1998.

[Ran96] D. Rand. *The PPP Compression Control Protocol (CCP).* Internet Engineering Task Force, RFC 1962, 1996.

[RMK+94] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. *Address Allocation for Private Internets.* Internet Engineering Task Force, RFC 1918, 1994.

[RRSW97] C. Rigney, A. Rubens, W. Simpson, and S. Willens. *Remote Authentication Dial In User Service (RADIUS).* Internet Engineering Task Force, RFC 2138, 1997.

[RRSW00] C. Rigney, A. Rubens, W. Simpson, and S. Willens. *Remote Authentication Dial In User Service (RADIUS).* Internet Engineering Task Force, RFC 2865, 2000.

[SAdG02] Jansen Carlo Sena, Alessandro Augusto, and Paulo Lício de Geus. Impactos da transição e utilização do IPv6 sobre a segurança de ambientes computacionais. In *II Workshop em Segurança de Sistemas Computacionais*, pages 73–80, Búzios, Rio de Janeiro, Brazil, 2002.

[Sch96] Bruce Scheneier. *Applied Cryptography.* John Wiley & Sons, New York, 2 edition, 1996.

[Sen02] Jansen Carlo Sena. *Um modelo para proteção do tráfego de serviços baseado em níveis de segurança.* Tese de Mestrado, Campinas: IC/UNICAMP, 2002.

[Sim96a] W. Simpson. *PPP Challenge Handshake Authentication Protocol (CHAP).* Internet Engineering Task Force, RFC 1994, 1996.

[Sim96b] W. Simpson. *The Point-to-Point Protocol (PPP).* Internet Engineering Task Force, RFC 1661, 1996.

[SKA02] Y. Sheffer, H. Krawczyk, and B. Aboba. *PIC, A Pre-IKE Credential Provisioning Protocol.* Internet Engineering Task Force, Internet Draft, 2002.

[SM98] Bruce Schneier and P. Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). In *5th ACM Conference on Computer and Communications Security*, pages 132–141, San Francisco, California, 1998.

[SMW99] Schneier, Mudge, and Wagner. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). In *CQRE: International Exhibition and Congress on Secure Networking – CQRE [Secure]*, 1999.

[Sri00] P. Srisurech. *Secure Remote Access with L2TP.* Internet Engineering Task Force, RFC 2888, 2000.

[Ste96] W. Richard Stevens. *TCP/IP Illustrated*, volume 1. Addison-Wesley, Reading, Massachusetts, 2 edition, 1996.

[Ste03a] Andreas Steffen. Virtual Private Networks - Coping with Complexity. In *17th DFN-Workshop on Communications Networks*, 2003.

[Ste03b] Andreas Steffen. X.509 FreeS/WAN Patch – Instalation and Configuration Guide. Disponível em: <http://www.strongsec.com/freeswan/>, Acesso em: 20/11/2003.

[Str03] Mario Strasser. DHCPv4 Configuration of IPSec Tunnel Mode HOWTO. Disponível em: <http://www.strongsec.com/freeswan/dhcprelay/>, Acesso em: 20/11/2003.

[Tow99] W. Townsley. *Layer Two Tunneling Protocol (L2TP).* Internet Engineering Task Force, RFC 2661, 1999.

[VLK98] A. Valencia, M. Littlewood, and T. Kolar. *Cisco Layer Two Forwarding.* Internet Engineering Task Force, RFC 2341, 1998.

[WHK97] M. Wahl, T. Howes, and S. Kille. *Lightweight Directory Access Protocol (v3).* Internet Engineering Task Force, RFC 2251, 1997.

[ZCC00] Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman. *Building Internet Firewalls.* O'Reilly & Associates, Sebastopol, California, 2 edition, 2000.