Integração de IPv6 em um Ambiente Cooperativo Seguro

Cleymone Ribeiro dos Santos

Dissertação de Mestrado

Instituto de Computação
Universidade Estadual de Campinas

Integração de IPv6 em um Ambiente Cooperativo Seguro

Cleymone Ribeiro dos Santos

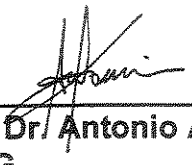
Fevereiro de 2004

Banca Examinadora:

- Prof. Dr. Paulo Lício de Geus (Orientador)
- Prof. Dr. Antônio Alfredo Ferreira Loureiro
  Departamento de Ciência da Computação, UFMG
- Prof. Dr. Ricardo Dahab
  Instituto de Computação, UNICAMP
- Prof. Dr. Edmundo Madeira (Suplente)
  Instituto de Computação, UNICAMP

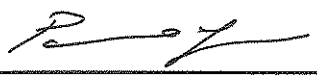
TERMO DE APROVAÇÃO

Tese defendida e aprovada em 27 de fevereiro de 2004, pela Banca examinadora composta pelos Professores Doutores:



Prof. Dr. Antonio Alfredo Ferreira Loureiro
UFMG

Prof. Dr. Ricardo Dahab
IC - UNICAMP



Prof. Dr. Paulo Lício de Geus
IC - UNCIAMP

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Santos, Cleymone Ribeiro dos

Sa59i Integração de IPv6 em um ambiente cooperativo seguro / Cleymone Ribeiro dos Santos -- Campinas, [S.P. :s.n.], 2004.

Orientador : Paulo Lício de Geus

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Computação.

1. Sistemas de segurança. 2. Redes de computadores – Protocolos.3. Internet (Redes de computação). I. Geus, Paulo Lício de. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Integração de IPv6 em um Ambiente Cooperativo Seguro

Este exemplar corresponde à redação final da Dissertação devidamente corrigida e defendida por Cleymone Ribeiro dos Santos e aprovada pela Banca Examinadora.

Campinas, fevereiro de 2004

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.

Resumo

A Internet cresceu na comunidade acadêmica, de modo que mecanimos de segurança não eram parte do protocolo original IP e do projeto de serviços. Durante a discussão de redefinição do atual Protocolo Internet (IPv4), se tornou claro que o novo projeto (IPv6) deveria incorporar algumas características básicas de segurança. A intenção era que estas características provessem autenticidade, privacidade e um nível mínimo de segurança contra muitos ataques baseados no IP. A provisão de características de segurança em IPv6 (IPSec) é um passo importante em direção a prover segurança nativa na Internet. Entretanto, IPSec não é a solução para todos os problemas de segurança.

O objetivo deste trabalho é analisar as implicações da adoção de IPv6 em Ambientes Cooperativos Seguros, particularmente do IPSec, que provê um *framework* nativo de segurança para a camada IP, assim como para as camadas acima. Será visto que a característica de criptografia fim-a-fim do IPSec impossibilita a utilização efetiva de vários mecanismos de segurança consolidados em Ambientes Cooperativos Seguros atuais (IPv4).

Considerando que uma rede IPv6 não será efetivamente útil se não permitir a ocorrência de comunicação com outras redes na Internet, tanto IPv4 quanto IPv6, este trabalho também objetiva estudar os cenários de integração entre redes IPv6 e IPv4 bem como os mecanismos de transição aplicáveis a cada cenário.

Abstract

The Internet grew up within the academic community in such a manner that security mechanisms were neither required nor incorporated into the original IP protocol. During the discussions to redefine and improve the actual internet protocol (IPv4), it became clear that the new project (IPv6) should incorporate some basic security characteristics. The intention was that these characteristics would provide authentication, privacy and a minimum level of security against attacks based on the protocol IP. Providing security characteristics in IPv6 (IPSec) is an important step in the direction of providing native security on the Internet. However, IPSec, does not provide a solution for all security problems that might happen when accessing the Internet.

The aim of this work is to analyze the implications of the adoption of IPv6 in Secure Cooperative Environments, in particular IPSec, which provides the native security framework in the network layer, as well as the layers above it. It will be seen that the adoption of IPSec and its characteristic of end-to-end encryption, does have drawbacks since it is incompatible with the consolidated security mechanisms used currently in Secure Cooperative Environments (IPv4).

Considering that IPv6 networks must be compatible with the existing IPv4 networks used in the Internet in order to have a gradual transition between both protocols, this work also discusses the scenarios involved when integrating the two protocols and the transition mechanisms that are relevant to each scenario.

Para meus pais e meu companheiro.

"I am enough of an artist to
draw freely upon my imagination.
Imagination is more important than knowledge.
Knowledge is limited.
Imagination encircles the world."
Albert Einstein

Agradecimentos

A Deus, por estar sempre ao meu lado.

À minha mãe, Elena, que acredita na minha capacidade, agradeço pelo incentivo, carinho e amor.

Ao meu companheiro, Sidney, pelo incentivo durante esta trajetória e, sobretudo, pelo carinho, paciência, compreensão e amor.

Ao meu orientador, Paulo Lício de Geus, por toda paciência com minhas falhas, além da orientação, apoio e atenção fornecidas durante o desenvolvimento deste trabalho.

Aos meus tios e tias, primos e primas, pela preocupação em acompanhar minha trajetória.

A minha avó querida, Vó Julia, pelo carinho eterno.

Aos meus sogros, Sr. Sidney e Dna Antônia, pelo carinho recebido.

À amiga Helen, pelas palavras de incentivo e apoio nos momentos difíceis.

A todos os meus amigos de Goiânia, pelos grandes momentos que passamos juntos e, especialmente, à Alessandra, Eubia e Edwagney, pela amizade constante e valiosa.

À Dna Claúdia e Sr Carlos, pela amizade e apoio em Campinas.

Aos amigos do IC, especialmente ao Gregs, Amanda e Thaísa, pela amizade e companheirismo.

Aos amigos do LAS, Arthur, Bene, Diogo, Eduardo, Edmar, Fabrício, Felipe, Fernando, Ivete, João, Martim, Ruppert, Thiago, por nossas reuniões semanais, pela contribuição no meu aprendizado e pela amizade estabelecida.

Aos amigos, colegas e funcionários do Instituto de Computação.

Ao pessoal do CPqD, pelo incentivo e sugestões enriquecedoras, em especial ao Luciano e Marcelo.

Conteúdo

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

Originalmente projetada para compartilhar informações entre pesquisadores, a Internet agora está sendo usada para um número crescente de interações comerciais. Essas interações exigem um nível suficiente de segurança, abrangendo desde a correta identificação de seus participantes até métodos de pagamento seguro. A Internet cresceu na comunidade acadêmica, de modo que mecanimos de segurança não eram parte do protocolo original IP e do projeto de serviços. Ao invés disto, temos mecanismos incompatíveis e diferentes, que foram adicionados a algumas aplicações individuais (senha em *telnet* e FTP), enquanto outros serviços (protocolos de roteamento, SMTP) não são seguros ou são seguros apenas para mecanismos limitados e proprietários.

Durante a discussão de redefinição do atual Protocolo Internet (IPv4), tornou-se claro que o novo projeto (IPv6) deveria incorporar algumas características básicas de segurança. A intenção era que estas características provessem um nível mínimo de segurança contra muitos ataques baseados no IP.

Muito do desenvolvimento de IPSec ocorreu durante a definição e desenvolvimento de IPv6, cuja intenção é e foi, desde o início, incorporar IPSec como seu *framework* de segurança. Em razão da lenta adoção de IPv6 e da crescente necessidade de segurança dos pacotes IP, IPSec foi modificado para ser compatível com o IPv4. Suporte aos cabeçalhos IPSec é uma característica opcional em IPv4, porém é obrigatória em IPv6.

A provisão de características de segurança em IPv6 (IPSec) é um passo importante em direção a prover segurança nativa na Internet. Há diferentes aplicações do IPSec, tais como confidencialidade geral na transmissão, autenticação por entidades (atualização de roteamento, auto-configuração baseada em DHCP etc.) e prevenção, ou no mínimo redução, de ataques de negação

de serviço, *man-in-the-middle*, reenvio de mensagens e falsificação de endereços e dados. Contudo, IPSec não resolve todos os problemas de segurança existentes na Internet.

Na verdade, IPv6, com seu suporte nativo à criptografia fim-a-fim (através do IPSec), traz problemas às tecnologias de segurança implementadas em redes IPv4, tais como *firewalls*, IDS, *proxies* de aplicação etc., que são importantes no combate a outros tipos de ataques além de limitarem a exposição da rede interna às ameaças externas. Estas tecnologias disponíveis são integradas em uma mesma estrutura de segurança, chamada *firewall cooperativo* [NAK 03], que é utilizado em um ambiente cooperativo para torná-lo seguro, permitindo a comunicação entre diferentes tecnologias, usuários, culturas e políticas internas de cada organização.

1.1 Objetivos

Este trabalho tem como objetivo caracterizar o que chamamos de Ambiente Cooperativo Seguro (Capítulo 2.3, página 28), acompanhando a evolução dos vários cenários de rede, apresentar algumas tecnologias, técnicas e conceitos de segurança disponíveis, até chegar ao conceito de *firewall cooperativo* e, então, analisar o impacto da adoção de IPv6, principalmente de seu modelo de segurança IPSec, em tal ambiente. Esta parte do trabalho foi desenvolvida visando antecipar e buscar soluções para amenizar, senão resolver, os problemas advindos da integração de IPv6 em Ambientes Cooperativos Seguros, que utilizam várias ferramentas e tecnologias de segurança.

O suporte nativo à segurança em IPv6 apresenta cabeçalhos de extensão para autenticação e confidencialidade (IPSec), como características de criptografia fim-a-fim, o que garante que quaisquer pares de uma comunicação possam estabelecer canais seguros entre eles. No entanto, criptografia fim-a-fim traz problemas às tecnologias de segurança implementadas em redes IPv4. Um exemplo a ser citado é do *firewall* que não consegue vistoriar o tráfego cifrado que passa por ele. Logo, este novo protocolo também introduz complexidade ao Ambiente Cooperativo Seguro, pois traz nativamente características, como criptografia fim-a-fim, que são incompatíveis com o *modus operandi* das tecnologias tradicionais de segurança, tais como *firewall*, IDS, *proxy* etc.

Além disto, os cabeçalhos IPv4 e IPv6 não são interoperáveis, já que um roteador ou máquina precisa implementar ambos os protocolos para conseguir reconhecer e processar seus cabeçalhos. Logo, este trabalho também tem como objetivo apresentar os vários mecanismos de transi-

ção existentes entre IPv4 e IPv6, buscando caracterizar os vários cenários existentes de interoperabilidade bem como os mecanismos de transição aplicáveis a estes cenários.

1.2 Organização do trabalho

Do ponto de vista lógico, este trabalho pode ser dividido em duas partes principais. A primeira parte, representada pelos Capítulos 2, 3, 4 e 5, está relacionada ao impacto da adoção de IPv6, principalmente de seu modelo de segurança IPSec, em um Ambiente Cooperativo Seguro. É importante evidenciar que o processo de adoção pode acontecer pela migração de uma rede IPv4 para IPv6 como também pela formação de uma rede nativa IPv6. A segunda parte lógica do trabalho, representada pelo Capítulo 6, é um estudo sobre a coexistência de uma rede IPv4 migrada para IPv6 com outras redes, que tanto podem ser IPv4 como IPv6.

Segundo a primeira parte do trabalho, no Capítulo 2 é caracterizado o Ambiente Cooperativo Seguro, acompanhado da evolução de seus vários cenários de rede, bem como das tecnologias e ferramentas de segurança utilizadas em cada cenário, até culminar no conceito de *firewall cooperativo*.

A seguir, no Capítulo 3, são explicadas as características de IPv6, os tipos de endereços existentes e o estado atual de designação, desenvolvimento e implantação de IPv6 no Brasil e no Mundo.

Logo após, no Capítulo 4 são explicados os aspectos de segurança de IPv6, tais como seu *framework* de segurança IPSec e o SEND, que provê segurança para as atualizações de roteamento e auto-configuração do *Neighbor Discovery*.

No Capítulo 5 são analisados os problemas de integração de IPv6 com as ferramentas de segurança já consolidadas e implantadas em um Ambiente Cooperativo Seguro.

Conforme a segunda parte do trabalho, o Capítulo 6 detalha os mecanismos de transição existentes entre IPv4 e IPv6, sendo apresentados os vários cenários de interoperabilidade e os mecanismos aplicáveis.

No Apêndice A estão os detalhes de configuração de IPv6 no Laboratório de Administração e Segurança (LAS) do Instituto de Computação (IC) da Unicamp [LAB 04], e no Apêndice B estão as alocações de endereços IP no Brasil e no Mundo.

Capítulo 2

O Ambiente Cooperativo Seguro

Este capítulo, que é baseado em [NAK 03], tem como objetivo apresentar o ambiente cooperativo, que é um ambiente no qual as várias organizações que o compõem trocam informações de vários tipos através de uma rede integrada virtualmente. Visa também apresentar os diversos cenários que representam as redes das organizações, nas quais o aumento evolutivo das conexões leva à formação do ambiente cooperativo. A complexidade dos cenários aumentará a cada nova conexão, o que implica na análise das tecnologias e ferramentas necessárias à elaboração da arquitetura de segurança da organização, bem como de suas configurações, como o *firewall* [CHA 00] [CHE 94], Redes Virtuais Privadas (VPN) [KOS 98] [SCO 98], Sistemas de Detecção a Intrusão (IDS) [SAN 03a] e uma Infra-estrutura de Chave Pública (PKI) [ADA 99]. Será apresentada também a arquitetura do *firewall* cooperativo [NAK 03], que integra o Ambiente Cooperativo Seguro. Finalmente, o capítulo introduz a problemática da adoção de IPv6 em Ambientes Cooperativos Seguros, que será analisado em mais detalhes na Seção 5.1.

2.1 O Ambiente Cooperativo

Comunicação é o coração dos negócios. Não apenas as empresas dependem de comunicação em suas interações internas como também precisam comunicar com seus fornecedores, distribuidores e clientes, se esperam permanecer no mercado. Na década de 90, a Internet se tornou a estrela da comunicação. Ela capturou a imaginação de indivíduos e empresários como um novo meio para se comunicarem com clientes e com parceiros comerciais etc.

A disseminação das redes e, particularmente, da Internet é o fenômeno tecnológico de maior impacto social atualmente. A onipresença da Internet e a popularização do microcomputador

trouxeram um novo ambiente global, no qual um universo de possibilidades convive de forma desordenada e descontrolada, porém com crescente vitalidade. Todos reconhecem que a Internet nasceu e se desenvolveu com pouquíssimo controle central. Isso eliminou muitas barreiras de entrada e foi, certamente, um dos principais fatores de sua rápida adoção e sucesso.

O contexto atual de transformações comerciais, fusões entre organizações e parcerias estratégicas, acrescido da utilização cada vez maior da Internet, cria um novo ambiente, chamado ambiente cooperativo [NAK 03], no qual as várias organizações (matrizes, filiais, parceiros comerciais, distribuidores, clientes etc) trocam informações técnicas, comerciais e financeiras através de uma rede integrada virtualmente. O ambiente cooperativo é o ambiente no qual a rápida e eficiente troca de informações, entre as matrizes e suas filiais, parceiros comerciais etc, é fator determinante de sucesso. É caracterizado pela integração dos diversos sistemas das várias organizações, que compõem o ambiente cooperativo, e tem como objetivo a cooperação entre todos para alcançarem um objetivo comum: sucesso na realização de negócios.

É imprescindível que a rede integrada, utilizada pelas várias organizações em um ambiente cooperativo, proteja as informações que trafegam por ela, pois destas informações dependem o sucesso das organizações. Desta forma, torna-se mais e mais necessário munir a Internet dos recursos que garantam a segurança, não só dos internautas, como também das empresas que realizam negócios pela rede, já que muitas empresas querem abrir suas corporações à rede, sem contudo expor suas bases de informação e seus sistemas aos ataques de agressores reais e virtuais que infestam a Internet. Várias das tecnologias necessárias e disponíveis, para prover uma comunicação segura e confiável, ainda estão em processo de adaptação para o uso diário. O uso rotineiro da Internet em relações comerciais já é fato, contudo não alcançou o estágio *plug-and-play* para várias de suas aplicações. Os avanços tecnológicos em cada nível de rede pode tornar difícil, senão impossível, encontrar uma solução única e integrada para as necessidades das empresas.

Os ambientes cooperativos, formados a partir de conexões entre organizações e filiais, fornecedores, parceiros comerciais, distribuidores, vendedores ou usuários móveis, criam a necessidade de um novo tipo de abordagem quanto à segurança. Em oposição à idéia inicial, quando o objetivo era proteger a rede da organização isolando-a das redes públicas, nos ambientes cooperativos, o objetivo é justamente o contrário: disponibilizar cada vez mais serviços e permitir a comunicação entre sistemas de diferentes organizações, de forma segura. A complexidade

aumenta, pois, agora, a proteção deve funcionar contra os ataques vindos da rede pública, como também contra ataques que podem ser considerados internos, originados a partir de qualquer ponto do ambiente cooperativo. A formação de um ambiente cooperativo (Figura 2.1), por intermédio do aumento evolutivo do número de conexões, é mostrado na próxima subseção.

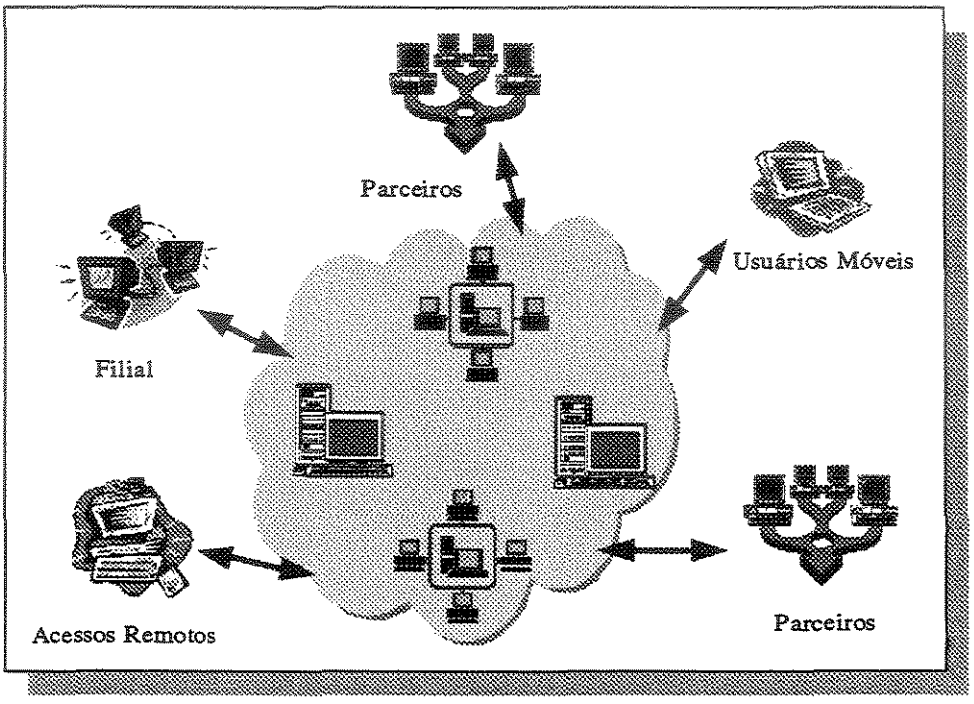


Figura 2.1: O ambiente cooperativo - diversidade de conexões. [NAK 03]

2.2 Configurações de um Ambiente Cooperativo

A formação do ambiente cooperativo é resultado da evolução de uma rede, em termos de números de conexões, o que implica em sua conseqüente e gradual necessidade de proteção. Os diversos cenários evolutivos de uma rede serão apresentados a seguir, o que permitirá, de forma progressiva, a análise das várias etapas de expansão das conexões de uma organização, a discussão sobre os seus problemas de segurança e a proposição de soluções encontradas.

2.2.1 Rede inicial

Uma rede típica inicial de uma organização é montada para conectar seus recursos internamente (Figura 2.2), com o fim exclusivo de facilitar e agilizar a execução das tarefas básicas da organi-

zação. Nesse primeiro cenário evolutivo, a rede da organização não é conectada a uma rede pública, isto é, os usuários internos não acessam a Internet, pois fazem somente acessos internos.

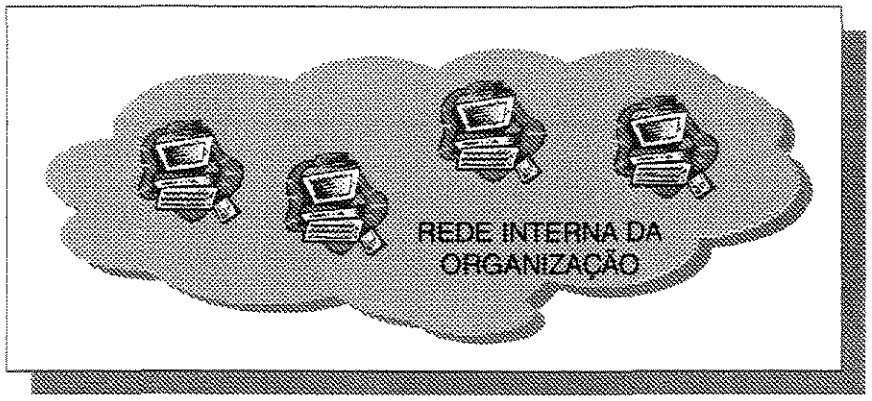


Figura 2.2: A rede interna de uma organização. [NAK 98]

Este cenário não apresenta riscos de segurança para as informações e recursos da organização, já que sua rede é isolada fisicamente da Internet. As únicas ameaças existentes serão provenientes de engenharia social ou de ataques originados por usuários internos à rede.

2.2.2 Matriz e filiais

O cenário acima mudará em decorrência da necessidade que a matriz da organização tem de se comunicar com suas filiais e vice-versa. Neste caso, serão utilizadas conexões dedicadas (Figura 2.3), porém possuem um custo bastante alto.

A preocupação com a segurança é semelhante ao caso anterior, já que ambas as redes também estão isoladas fisicamente da Internet, não fazendo acessos externos por meio de *modems* tampouco. A comunicação entre matriz e filial ocorrerá de forma privada e dedicada, contudo ainda existirão ameaças de engenharia social, usuários internos insatisfeitos ou usuários tercerizados, que podem acessar informações privilegiadas da organização.

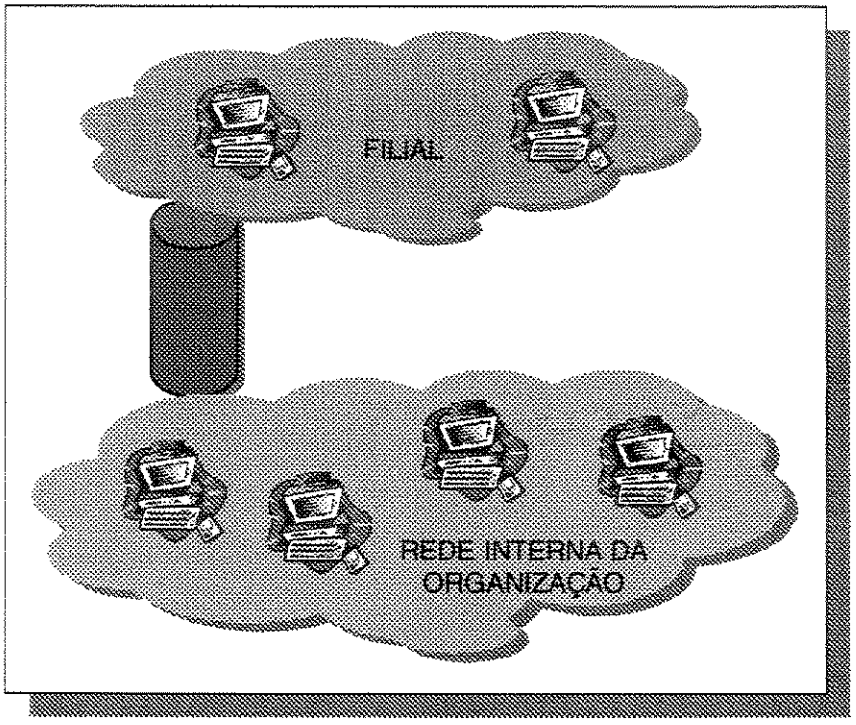


Figura 2.3: A comunicação entre organizações através de conexão dedicada. [NAK 03]

2.2.3 *Modem*

Neste cenário, é preciso considerar que acessos remotos através de *modems* podem se constituir em novos pontos de ataques, a exemplo do ataque realizado por Kevin Mitnick [GUL 01].

Os *modems* são pontos ativos de ataques, que podem comprometer a organização, principalmente através da criação de um atalho para enganar o *firewall*, se ele for mal implementado. Os *modems* aumentam a complexidade da segurança, pois exigem proteções específicas, tanto para a estrutura de acesso remoto quanto para os usuários internos que se utilizam dos *modems*. Adicionalmente, ainda existem problemas de segurança relacionados aos novos tipos de acessos remotos, como as conexões via cabo ou xDSL, que devem ser tratados com extremo cuidado, já que também podem ser utilizados como um desvio do *firewall*.

Conseqüentemente, é necessário que a organização utilize-se de algum método de autenticação eficiente, tais como *smartcards*, *tokens* de autenticação ou *dial-back*, para aumentar o nível de segurança do acesso remoto. Além disto, uma política de segurança bem definida e que

contemple todos os aspectos envolvidos, é extremamente importante para reduzir os riscos de invasão que, nos casos exemplicados no parágrafo anterior, são grandes.

2.2.4 Internet

A utilização dos recursos da Internet pela organização intensifica a preocupação com os problemas de segurança, pois a partir do momento que o acesso à Internet faz parte da rede da organização, o inverso também se torna verdade, já que qualquer um da Internet pode acessar a rede da organização. Logo, o *firewall* é uma tecnologia essencial às organizações, que se utilizam do acesso dedicado à Internet (Figura 2.4).

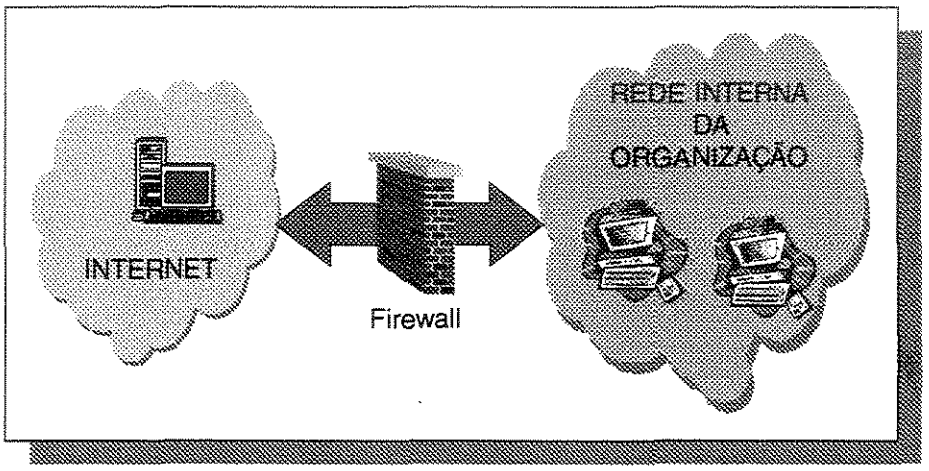


Figura 2.4: A necessidade do *firewall* nas conexões com a Internet. [NAK 03]

Neste cenário, o único tráfego necessário e permitido pelo *firewall* deve ser o originado na rede interna da organização, pois somente os usuários da organização acessarão informações da Internet. O tráfego no sentido contrário, da Internet para a rede interna da organização, não é permitido e necessário, caracterizando-se uma tentativa de ataque à rede interna na sua ocorrência, o que implica na configuração do *firewall* de forma simples, já que basta impedir este tráfego e permitir aquele.

O *firewall* pode ser constituído de *proxies* de serviços [CHA 00], tais como HTTP e FTP, o que aumentará significativamente a segurança do ambiente, visto que os *proxies* podem mascarar o endereço IP dos usuários internos da organização, efetuar filtragem em nível de aplicação e exigir autenticação dos usuários para acessar serviços. Adicionalmente ao *proxy*, o *firewall* pode

incorporar a funcionalidade do *Network Address Translation* (NAT) [SRI 01] para esconder os endereços da rede interna da organização, o que dificulta o mapeamento da rede interna e a execução de ataques a máquinas internas.

2.2.5 Provisão de serviços

O cenário anterior muda gradualmente quando a organização inicia o fornecimento de serviços para a comunidade de internautas, o que implica no acesso aos recursos da organização por partes de usuários externos, principalmente a servidores Web, servidores FTP e servidores de *e-mail* (Figura 2.5).

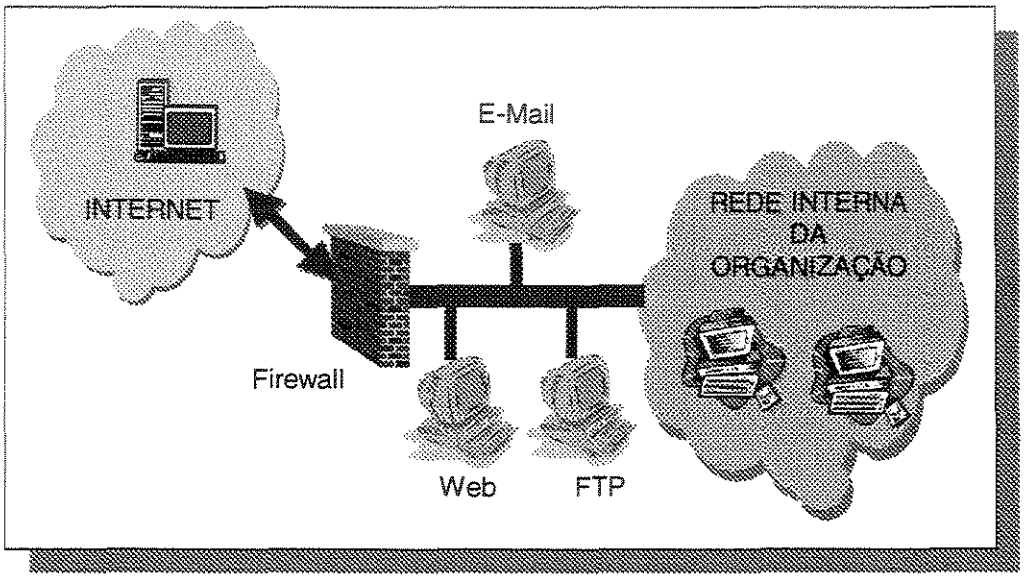


Figura 2.5: A organização provendo serviços para os usuários externos. [NAK 03]

A questão de onde localizar os servidores culminou no conceito de DMZ [CHA 00], onde o sucesso de um ataque contra esses servidores não significa o comprometimento da rede interna da organização. Na Figura 2.5 pode-se observar que o comprometimento de um dos serviços providos para a Internet resulta no acesso automático do *hacker* aos recursos internos da organização, ou seja, sem a DMZ, o sucesso de um ataque fará com que o *hacker* esteja dentro da rede da organização. A DMZ evita esse tipo de risco ao criar uma sub-rede formada por duas barreiras (Figura 2.6). Caso o *hacker* passe pela primeira barreira e ataque um dos serviços providos, ainda existe a segunda barreira a ser vencida pelo *hacker*, para que ele tenha acesso aos

recursos internos da organização. Esse *firewall* (Figura 2.6) pode ser composto de um filtro de estados na barreira 1, e de *proxies* na barreira 2. As duas barreiras que formam a DMZ podem

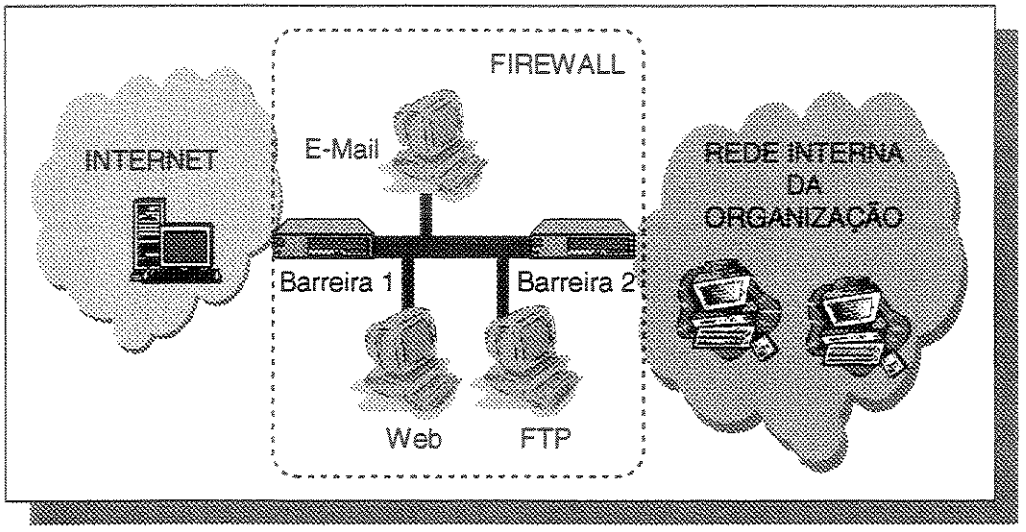


Figura 2.6: As duas barreiras que formam a DMZ do *firewall*. [NAK 03]

ser colocadas nas interfaces de um *firewall*, como pode ser observado na Figura 2.7. Agora será analisado qual esquema é mais interessante. Pode-se verificar que nos dois esquemas os serviços

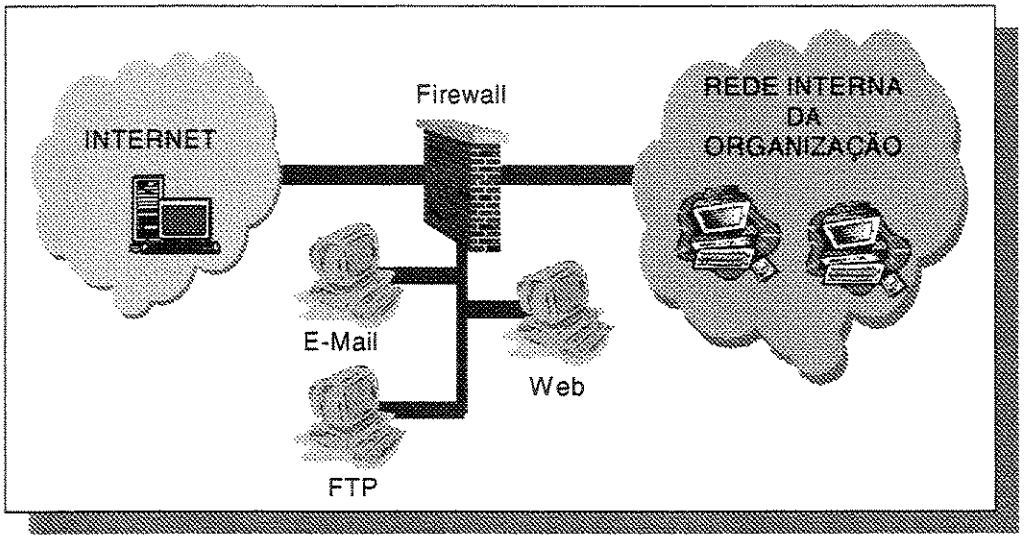


Figura 2.7: O *firewall* composto por 3 interfaces de rede. [NAK 03]

são providos através da DMZ. A diferença é que na Figura 2.6 o *firewall* é composto por dois componentes (barreira 1 e barreira 2), fora a DMZ, enquanto na Figura 2.7 o *firewall* é formado por um único componente, com 3 interfaces de rede.

Uma questão interessante é se existe uma diferença no nível de segurança entre os dois esquemas. *Bugs* podem resultar em acessos não autorizados através da exploração de *buffer overflow*, condições inesperadas ou de *race conditions*. Além disto, complexidade é inversamente proporcional ao nível de segurança dos sistemas, assim como a complexidade dos *firewalls* vêm aumentando através da combinação de diversas funcionalidades em um único equipamento. Essa observação é coerente, uma vez que a complexidade traz maiores possibilidades de erros em sua implementação, que resultam em *bugs* que podem ser explorados, diminuindo assim o nível de segurança do sistema. E o que vem acrescentando a complexidade dos *firewalls* é a adição de novas funcionalidades.

Assim, o melhor para um *firewall* é que ele seja o mais simples possível, o que de fato é verdade, se forem consideradas as tecnologias básicas que funcionam como barreira na rede da organização (filtros de pacotes, filtros de estados, *proxies*). Os filtros de pacotes e de estados atuam no *kernel* do sistema operacional, sendo extremamente simples, com a mínima possibilidade de *bugs* que possam ser explorados. *Race conditions*, que podem resultar em inconsistências de informações, não aparecem nos filtros, e o *buffer overflow* não pode ser explorado, pois os pacotes IP são regidos pelo MTU, ou seja, pacotes com tamanho grande não podem ser utilizados sem que antes exista a fragmentação desses pacotes em unidades menores. Os *proxies*, que atuam na camada de aplicação, também possuem poucas chances de conterem erros, pois a maioria deles realizam apenas a função de *relay*, no nível de circuitos, entre o cliente e o servidor. Os *proxies* de nível de aplicação podem realizar algumas filtragens no conteúdo dos pacotes, porém, como esses pacotes não ultrapassam o tamanho determinado pelo MTU, não podem sofrer com o *buffer overflow*, tampouco com *race conditions*.

Desta maneira, pode-se afirmar que o esquema 2 (Figura 2.7) é tão seguro quanto o esquema 1 (Figura 2.6), possuindo a vantagem de facilitar a administração, devido ao menor número de equipamentos a serem gerenciados. O que deve ser lembrado é que nenhum outro serviço deve estar sendo executado no equipamento [CHA 00]. O desempenho pode sofrer algumas alterações, sobretudo em um ambiente complexo como o ambiente cooperativo, porém a importância

deve ser dada em torno da segurança, sendo o desempenho um fator secundário. Se necessário, mais equipamentos podem ser utilizados para que a carga seja distribuída entre eles.

Implementando-se uma das configurações acima, a organização está apta a acessar serviços da Internet e também prover serviços para usuários externos.

2.2.6 Provisão de acesso à base de dados

Seguindo os passos da evolução, a organização então passa a ter a necessidade de prover informações mais específicas a seus usuários, como informações sobre compras *on-line*. Esse tipo de informação, que é normalmente específica e confidencial, e portanto deve ser protegida contra acessos indevidos, fez surgir a necessidade de maiores cuidados com relação à localização do banco de dados. A sua localização na DMZ, como um *bastion host* [CHA 00], poderia ser uma opção (Figura 2.8). Um ponto importante é a escolha do método de autenticação utilizado para que o acesso seja provido. Porém, sabe-se que os recursos residentes na DMZ possuem acesso externo permanente, sendo portanto alvos de tentativas de ataques.

Essa configuração coloca em risco as informações do banco de dados, resultando então na

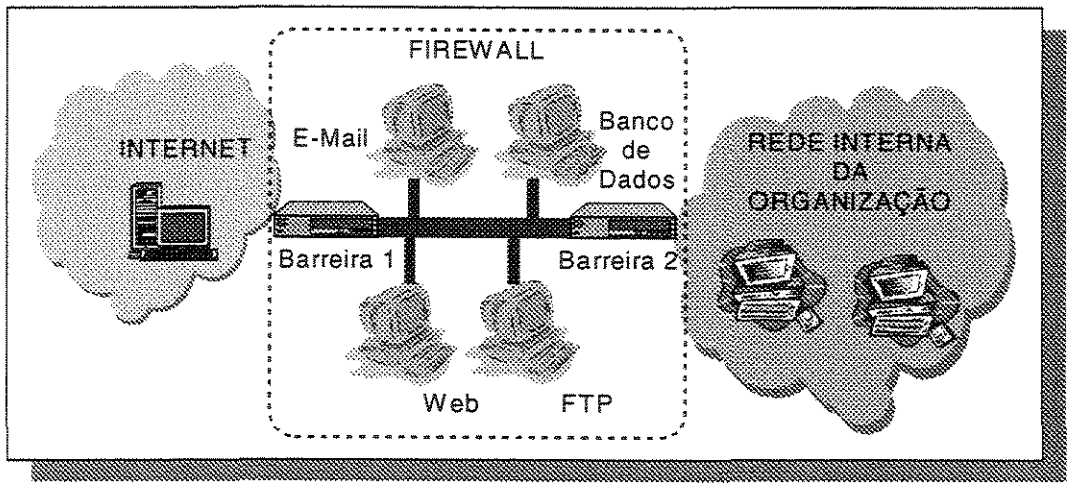


Figura 2.8: O servidor de banco de dados na DMZ. [NAK 03]

idéia de colocar o banco de dados na rede interna da organização (Figura 2.9).

Essa configuração, porém, dá a impressão de que um ataque ao servidor de banco de dados resulta no acesso à rede interna da organização, o que de fato é verdade, mas que pode ter o

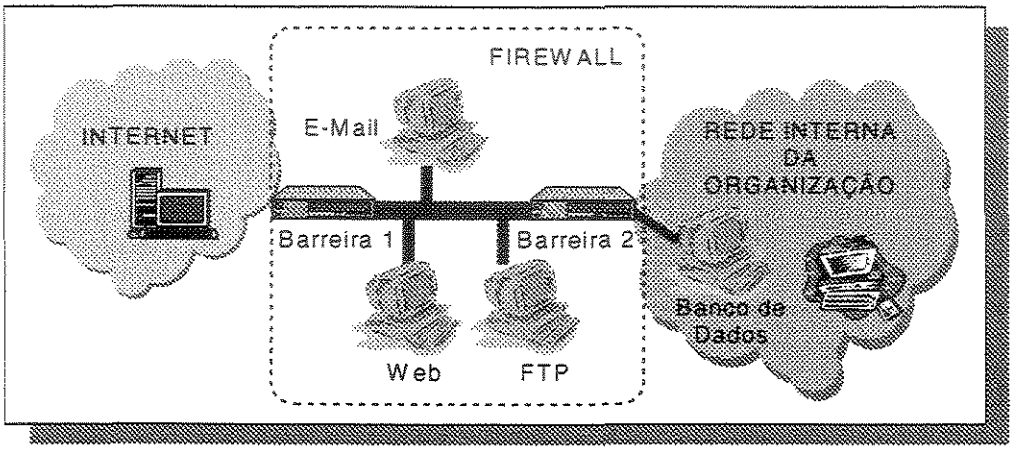


Figura 2.9: O servidor de banco de dados na rede interna da organização. [NAK 03]

risco minimizado com o correto desenvolvimento e correta implementação da política de segurança no *firewall*. A idéia aqui é fazer com que a segunda barreira permita passar apenas o tráfego referente à conexão entre o servidor Web e o servidor de banco de dados, não sendo possível o acesso direto ao banco de dados. Assim, para que o *hacker* tenha acesso não-autorizado à base de dados, seria necessário primeiro comprometer o servidor Web, e depois o servidor de banco de dados. É importante lembrar ainda que a autenticação deve fazer parte desse esquema de acesso aos dados. No entanto, existe outra configuração que traz maior nível de segurança à organização, que é a utilização de uma segunda rede DMZ (Figura 2.10):

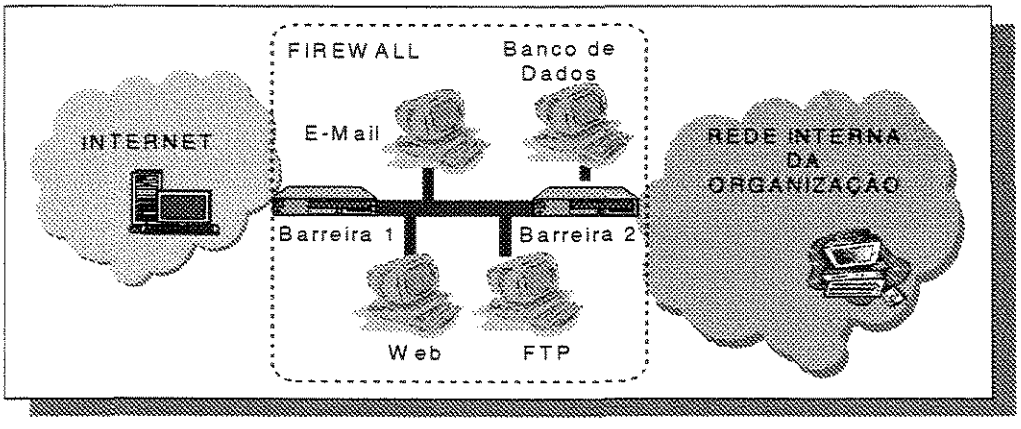


Figura 2.10: O utilização de uma segunda DMZ para o servidor de banco de dados. [NAK 03]

Esse esquema possui o mesmo grau de segurança do esquema da Figura 2.9, com relação à base de dados da organização. A vantagem é que esse novo esquema evita o problema do comprometimento da rede interna da organização caso um ataque ao servidor de dados tenha sucesso. A mesma arquitetura, utilizando-se um único componente de *firewall*, com quatro *interfaces* de rede, pode ser vista na Figura 2.11.

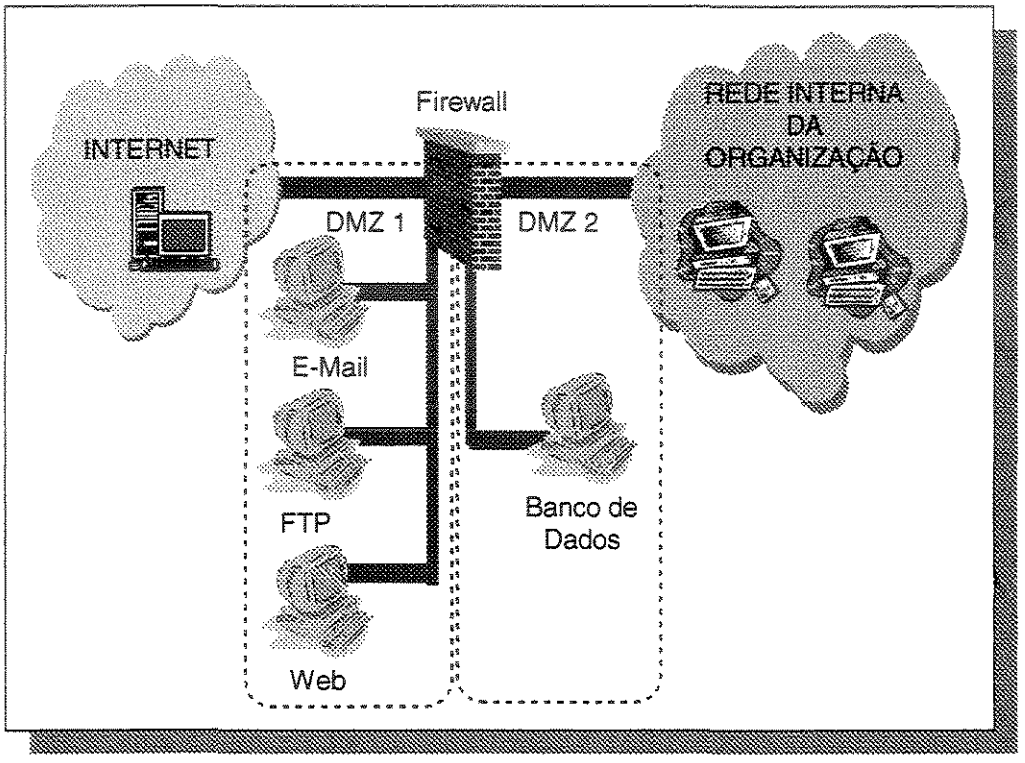


Figura 2.11: Duas DMZs em um único componente de *firewall*. [NAK 03]

2.2.7 Conexão com filial

Neste ponto, a organização possui o acesso à Internet, provê serviços para os usuários, sendo que um deles é o acesso às informações consideradas confidenciais. Pode-se considerar também que a organização possui ainda uma linha dedicada com a sua filial, e deseja reduzir os custos referentes a essa linha, através da utilização de uma VPN. De acordo com o esquema visto até o momento, a arquitetura da organização seria a que pode ser vista na Figura 2.12.

Aqui, o que entra em discussão são as conexões existentes na filial. No esquema da Figura 2.12 pode-se ver que a filial não possui nenhum outro tipo de conexão, de modo que

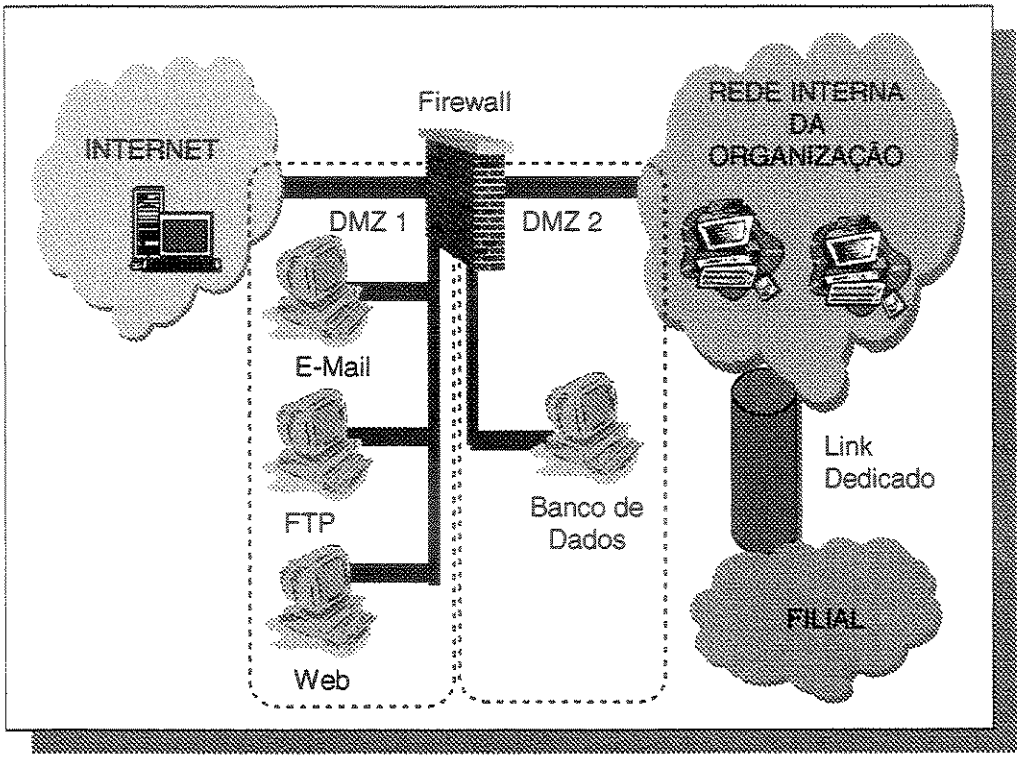


Figura 2.12: A arquitetura da organização com os acessos à Internet e à filial. [NAK 03]

tudo está de acordo, ou seja, ataques vindos do exterior são improváveis, podendo-se considerar a segurança como estando no nível interno da organização. Porém, a existência de outras conexões na filial pode colocar em risco a rede interna da organização, como pode ser visto na Figura 2.13.

No esquema da Figura 2.13, a rede interna da organização corre o risco de acessos não-autorizados dos usuários da Rede A, que podem chegar à rede interna através da rede da filial. Essa situação pode se tornar ainda mais crítica se a Rede A possui acesso à Internet sem a proteção necessária (Figura 2.14).

Nesse esquema (Figura 2.14), qualquer usuário da Internet pode chegar à rede interna da organização passando antes pela rede A, depois pela filial, até chegar à rede interna. Pode-se observar que o *firewall*, implementado para proteger a rede interna contra acessos não autorizados, passa a não ter função alguma, ao ser driblado através da passagem pela rede A e pela rede da filial.

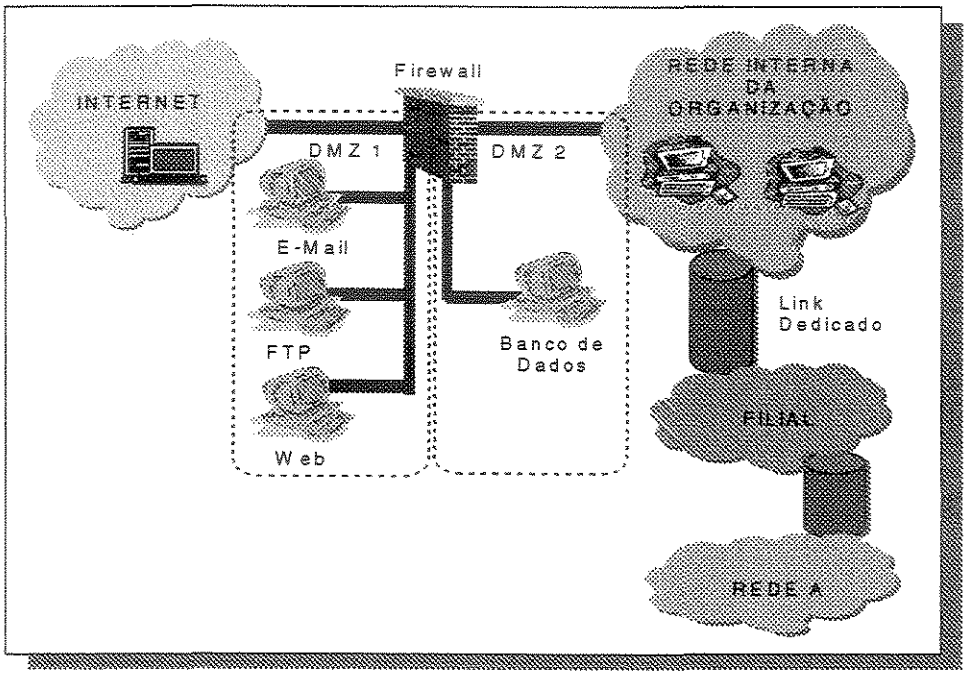


Figura 2.13: Os riscos envolvidos em múltiplas conexões. [NAK 03]

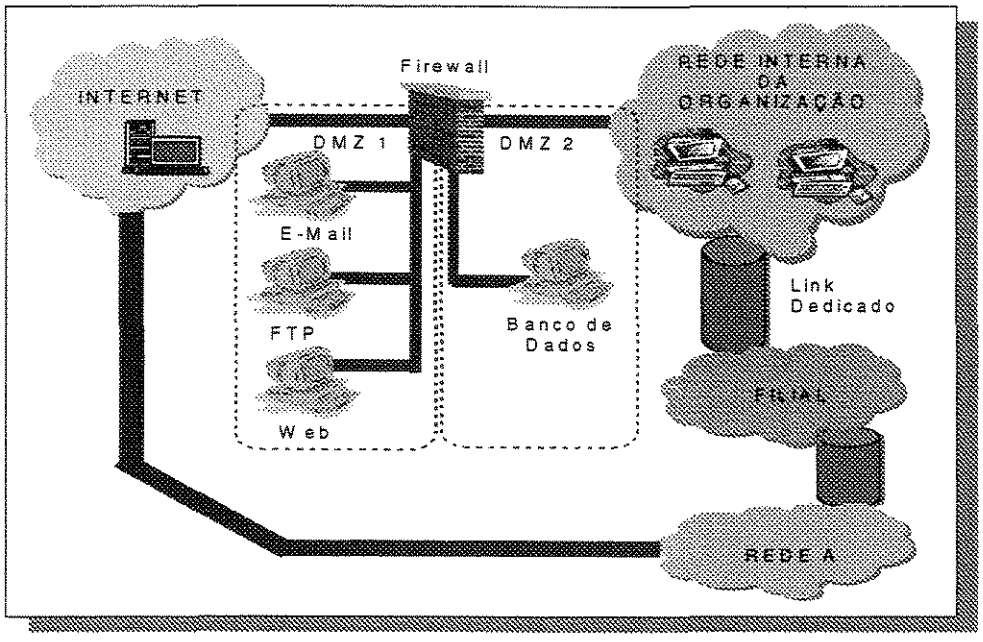


Figura 2.14: Múltiplas conexões envolvendo a Internet. [NAK 03]

Na realidade, esses dois passos (rede A e rede da filial) não são ao menos necessários, caso a própria filial possua o acesso à Internet. Como pode ser visto na Figura 2.15, essa é uma configuração reconhecidamente perigosa, já que a filial não possui os mesmos mecanismos de segurança da rede interna da organização, ou seja, a filial não possui o *firewall*.

Deve-se considerar, no entanto, que uma avaliação dos perigos existentes na filial, resultantes

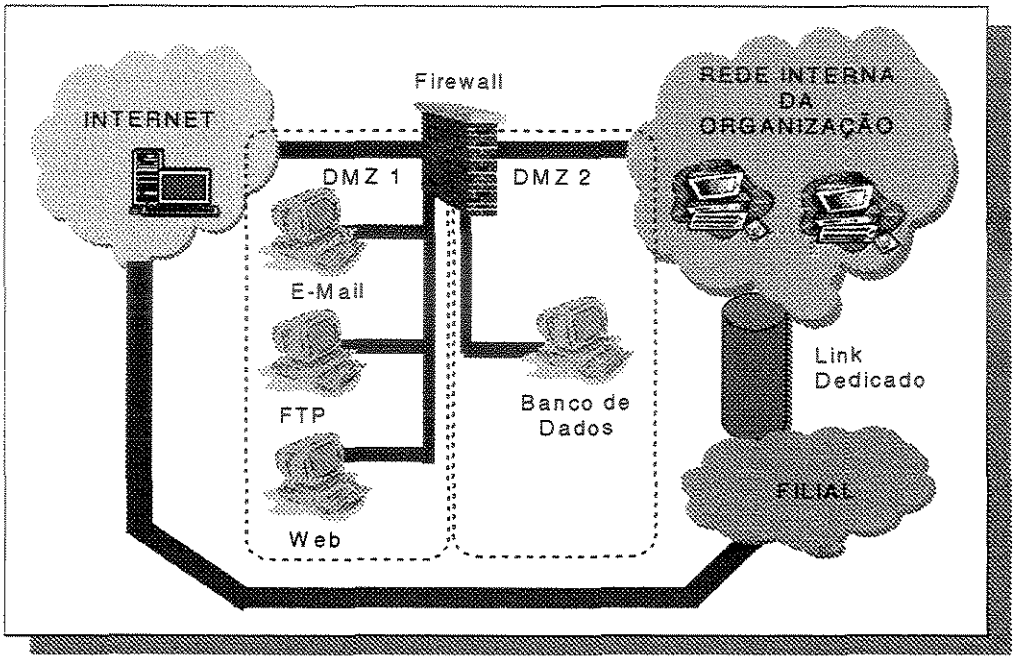


Figura 2.15: Mecanismos de Segurança não Equivalentes entre Matriz e Filial. [NAK 03]

da conexão à Internet, deve ser realizada. Neste ponto, já é possível vislumbrar o início de um ambiente cooperativo, o que implica na aplicabilidade da política de segurança desenvolvida para estes ambientes.

Se for levada em consideração que cada organização deve cuidar da sua própria segurança, então a abordagem a ser seguida é a de implementar um *firewall* entre a filial e a rede interna da organização. Assim, mesmo que a filial sofra um ataque, os riscos quanto à rede interna podem ser minimizados. De fato, essa é uma abordagem que deve mesmo ser seguida (*firewall* interno), porém, em se tratando de uma mesma organização, geralmente uma outra abordagem é seguida. A mais utilizada é a duplicação da configuração da borda de rede da matriz na borda de rede da filial.

No entanto, como a duplicação de esforços, para que a rede da filial possua o mesmo nível de segurança da rede interna, significa altos custos de implementação e gerenciamento, ela não é justificada para casos de acessos aos serviços básicos da Internet, como são a Web, FTP e *e-mail*. Assim, a configuração mais utilizada a princípio é a que se segue (Figura 2.16), onde o acesso à Internet é realizado através da linha dedicada até a rede interna da organização, onde a partir daí o acesso à Internet é permitido, passando-se pelo *firewall*. Esse esquema não resulta em nenhuma implicação de segurança, pois a filial não possui outros tipos de conexões, sendo que todas as comunicações são realizadas através da rede interna da organização, que está protegida dos acessos externos indevidos pelo *firewall*.

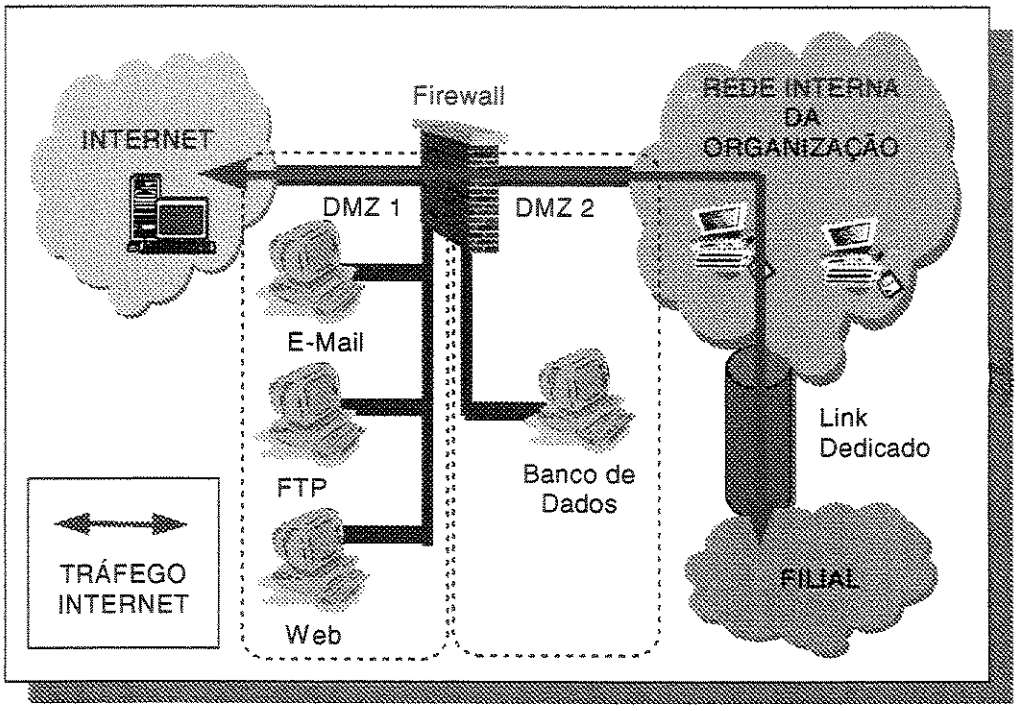


Figura 2.16: Acesso à Internet da filial através de linha dedicada. [NAK 03]

2.2.8 Redes Privadas Virtuais (VPN)

Entretanto, a utilização de uma linha dedicada para o tráfego Internet resulta em custos bastante altos, sobretudo em uma organização onde a filial possui um grande número de usuários. Assim, a organização deve considerar a idéia de utilizar uma conexão direta com a filial via Internet, para que a linha dedicada possa ser economizada. Uma das idéias é a utilização da VPN para

realizar essa função (Figura 2.17). Porém, pode-se verificar que essa alternativa é totalmente desnecessária para o caso do acesso apenas aos serviços da Internet. O primeiro passo para a utilização da VPN é a necessidade de uma conexão com a Internet, por onde o túnel virtual será criado. Deste modo, o túnel é criado no *gateway* da rede da filial e finalizado no *gateway* da rede da matriz.

Esse tipo de conexão, que é feito entre duas redes organizacionais, é conhecida como *gateway-to-gateway VPN*. Não serão abordados neste cenário os outros tipos de conexões VPN, que podem ser feitos entre o cliente e a rede da organização (*client-to-gateway VPN*) e entre um cliente e outro (*client-to-client* VPN). No esquema da Figura 2.17 aparecem duas questões essen-

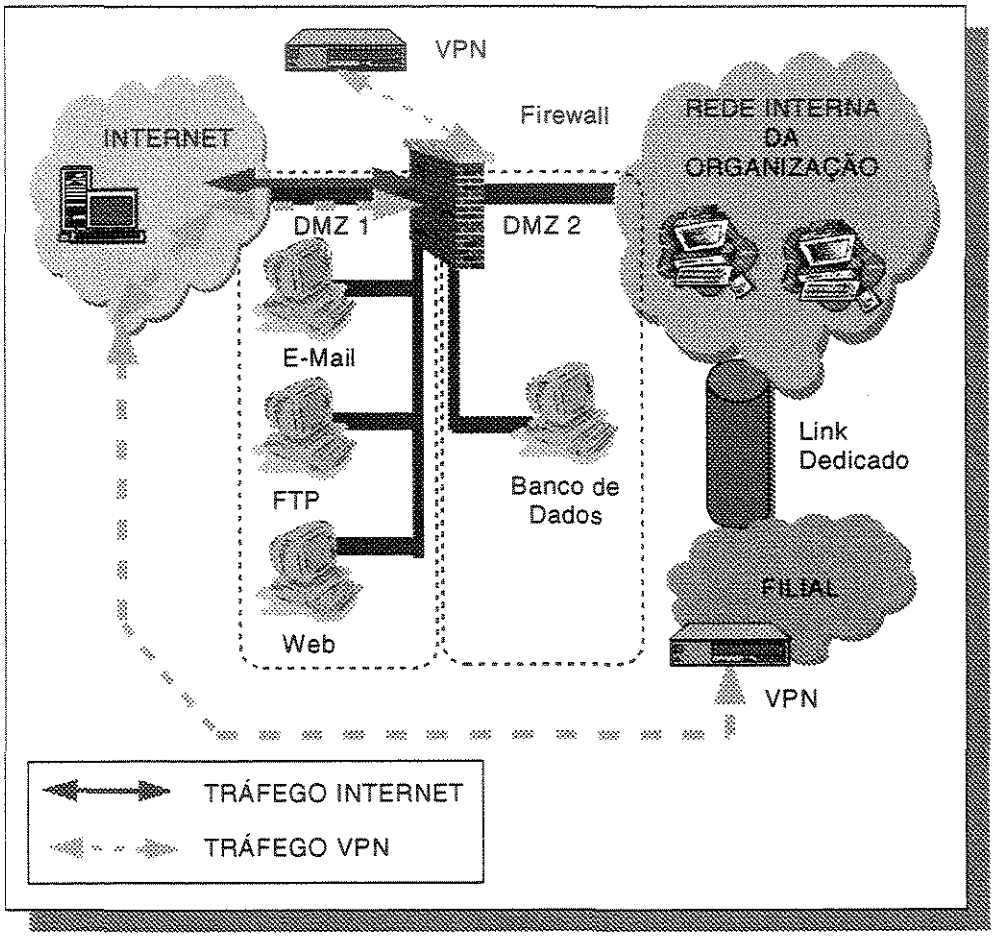


Figura 2.17: Acesso à Internet da filial através de VPN. [NAK 03]

ciais para a segurança da organização: do que consiste a VPN que funciona no gateway da filial e como deve ser a configuração da VPN no *firewall*.

Pode-se observar que o tráfego Internet nessa conexão é realizado de modo a desperdiçar recursos, já que a requisição do usuário da filial passa pelo túnel virtual, vai até a Internet, chega até o *firewall* da matriz, e vai até o dispositivo VPN, onde o túnel é desfeito, e a requisição chega novamente à Internet, dessa vez até o seu destino. O caminho inverso, da resposta, é feito da mesma maneira, ou seja, a resposta retorna ao *firewall*, onde então o encapsulamento da resposta é feito pela VPN, e a resposta é enviada via túnel para a Internet, até que chegue à origem, ou seja, o usuário da filial. Pode-se observar que o mesmo pacote de requisição e resposta passa 3 vezes pela Internet, sendo que em circunstâncias normais existe uma única passagem pela Internet, bidirecional, que é a requisição e a resposta direta ao cliente.

A utilização da VPN somente para o tráfego Internet passa assim a ser injustificável, a não ser que a confidencialidade dos dados seja um requerimento essencial, o que pode ocorrer no caso de transferência de *e-mails* entre a matriz e a filial através da Internet, em oposição à utilização da linha dedicada.

Porém, independentemente com relação à utilização, o ponto primordial a ser considerado nesse esquema surge a partir da questão 1 referida a pouco: do que consiste a VPN que funciona no *gateway* da filial? Essa questão surge porque o ponto fundamental a ser tratado quando uma organização passa a ter uma conexão direta com a Internet é: se possui acesso à Internet, então o controle de borda, realizado pelo *firewall*, deve existir, para que os acessos indevidos sejam evitados. Levando-se isso em consideração, será que no esquema visto anteriormente (Figura 2.17), as funcionalidades VPN são acompanhadas pela proteção de borda, ou seja, será que o dispositivo VPN está fazendo também o papel de *firewall*? Não é o que está representado na Figura 2.17, e essa questão é relevante, uma vez que o *firewall* muitas vezes é visto erroneamente como sendo a solução de todos os problemas de segurança. E o esquema visto parece estar se aproveitando dessa afirmação, ao fazer com que o tráfego passe obrigatoriamente pelo *firewall* da matriz, como se assim o nível de segurança fosse assegurado. Considerando então que, quando a conexão com a Internet existe, o *firewall* também tem que existir, utilizar a VPN para que o *firewall* da matriz seja utilizado não faz sentido, pois o *firewall* tem que existir na rede da filial de qualquer modo, devido à necessidade de proteção contra os ataques vindos a partir dessa conexão com a Internet.

Esse *firewall* na filial pode ser implementado de maneira extremamente simples, pois nenhum serviço será provido a partir da filial. O *firewall* apresentado na Figura 2.4 pode resolver o problema do acesso à Internet da filial, sem comprometer a segurança da matriz. O *firewall* da filial deve permitir apenas que somente os pacotes dos serviços básicos permitidos para os usuários internos passem pelo filtro.

A VPN pode ser utilizada para o tráfego de *e-mails* entre a matriz e a filial, por exemplo, além de ser possível também utilizá-la como canal de troca de documentos com informações confidenciais. A Figura 2.18 mostra a configuração ideal para essa situação. O que foi abordado res-

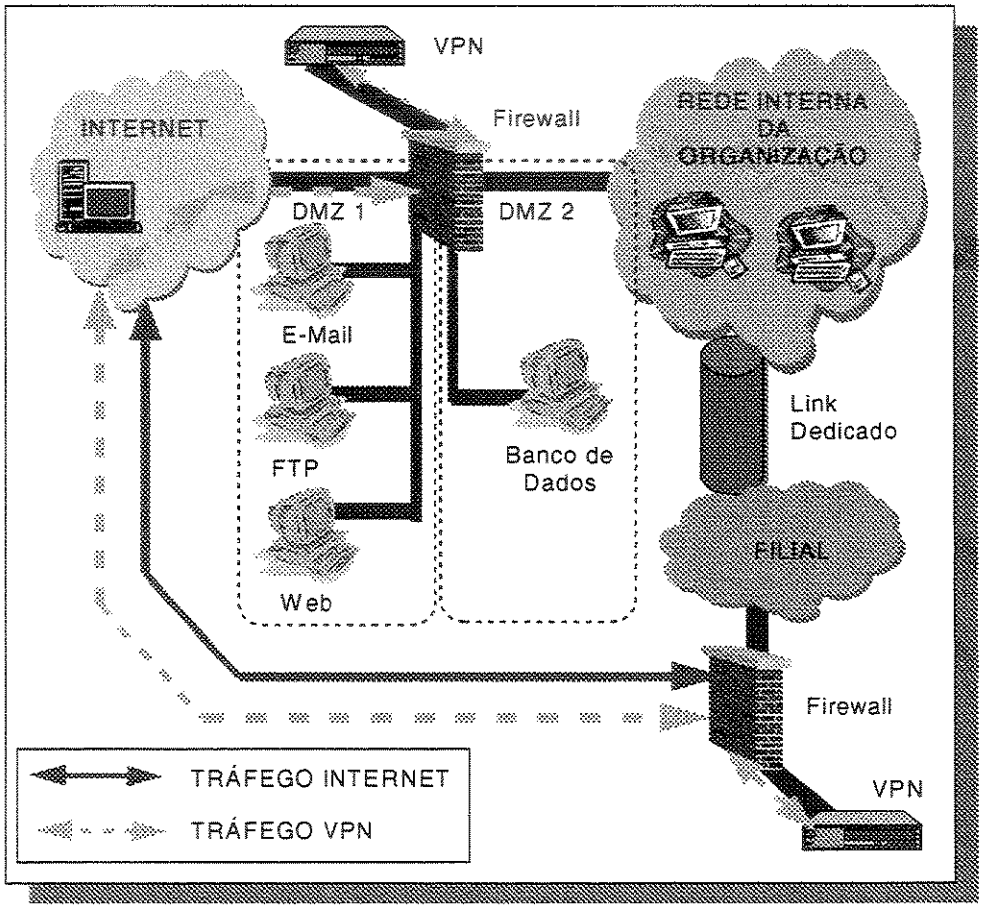


Figura 2.18: Acesso à Internet em conjunto com VPN. [NAK 03]

ponde à questão 1, faltando ainda abordar a questão 2, que aparece com a utilização da VPN:

como deve ser a configuração da VPN no *firewall*? As possibilidades de configurações do VPN com relação ao *firewall* são apresentadas em [NAK 03].

2.2.9 Conexão com fornecedor

Pode ser visto claramente que a complexidade da arquitetura de segurança vem aumentando (Figura 2.19), de acordo com as novas necessidades de conexões. Essa complexidade passa a ser maior e mais séria quando acessos à rede interna devem ser providos. Um caso típico é quando um fornecedor deseja acessar informações internas da organização, referente aos estoques. Esse tipo de acesso pode ser realizado através de uma aplicação específica, e o requerimento básico é que as informações não possam trafegar em claro pela rede, além de ser necessário também garantir a integridade desses dados para que eles não sejam alterados no meio do caminho entre o servidor e o cliente (ataque *man-in-the-middle* [BHA 01]). Outro requerimento básico é garantir que apenas os usuários legítimos tenham acesso ao servidor. O primeiro requerimento pode ser obtido através da utilização da VPN, e o segundo através de um esquema forte de autenticação e controle de acesso.

Pode-se observar, a partir da Figura 2.19, que a complexidade é bastante alta, que aumenta ainda mais em um ambiente cooperativo, onde um número maior de níveis de conexões diferentes é necessário (*telecommuters*, revendas, clientes, parceiros comerciais, etc). Quando existem, por exemplo, 10 níveis de conexões diferentes, a política de segurança torna-se difícil de ser desenvolvida, e principalmente, de ser implementada.

2.2.10 Autenticação com Autoridade Certificadora

Ao mesmo tempo em que o número de diferentes conexões vai aumentando, a autenticação dos usuários torna-se mais complicada, requerendo também um método mais forte de autenticação. A autenticação baseada em certificados digitais pode ser considerada uma solução ideal para o ambiente cooperativo. A autoridade certificadora (CA) da infra-estrutura de chaves públicas pode atuar em conjunto com a VPN, uma vez que somente ela deve se comunicar com a CA para que as autenticações sejam validadas. Os certificados digitais dão a garantia de confidencialidade, integridade e não-repúdio, necessárias em conexões críticas.

A posição da CA dentro da arquitetura de segurança é um ponto a ser discutido. A localização da CA na DMZ, como pode ser vista na Figura 2.20, pode ser válido, porém essa localização faz

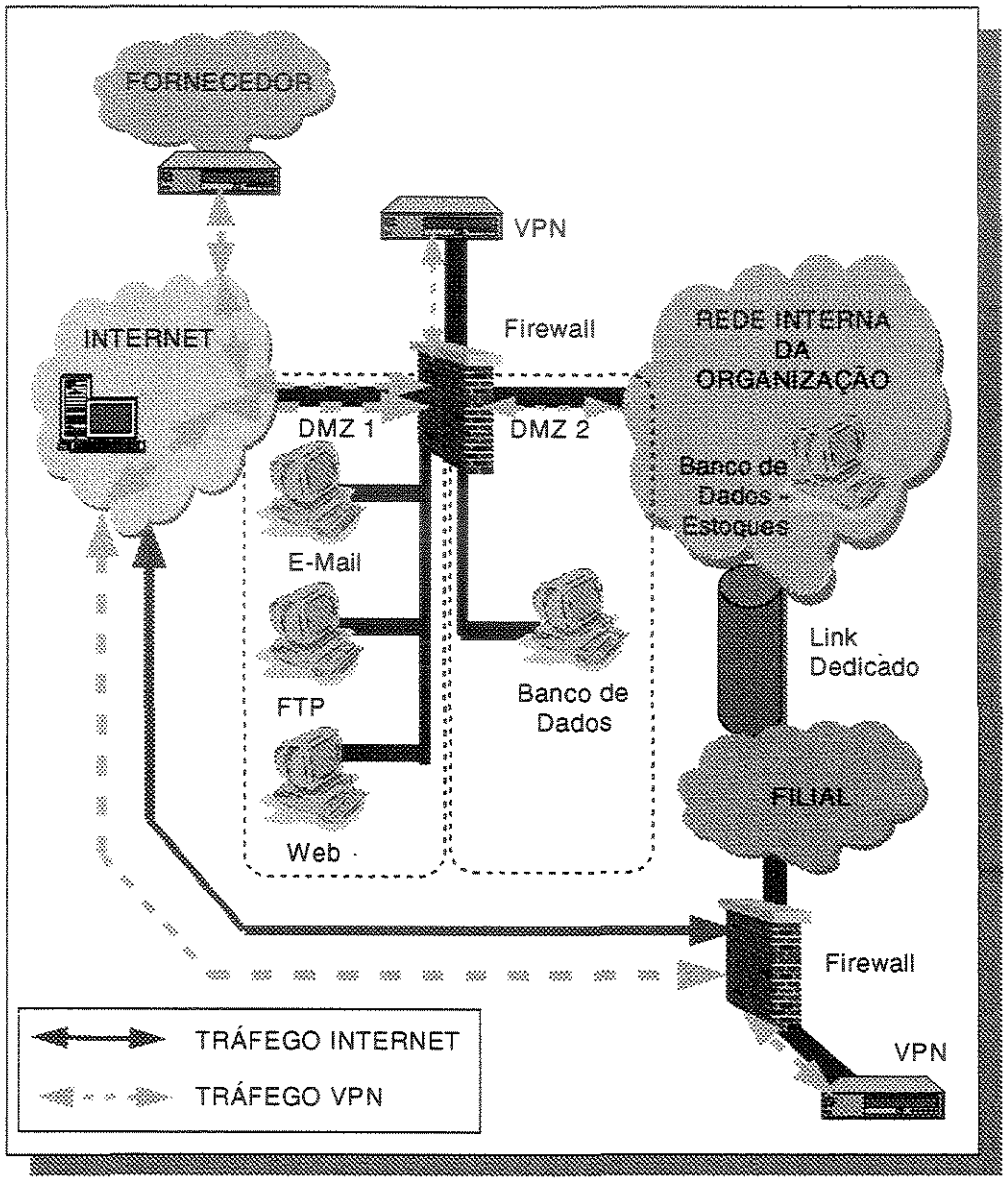


Figura 2.19: Aumento da complexidade das conexões. [NAK 03]

com que ela esteja diretamente exposta aos acessos externos, o que inviabiliza essa posição. O sucesso de um ataque à CA pode resultar no comprometimento dos certificados digitais dos usuários, culminando na falha total da estratégia de segurança da organização.

A sua localização na segunda DMZ (DMZ 2), do mesmo modo que o banco de dados foi localizado (somente o servidor Web se comunica com o banco de dados), pode ser utilizado

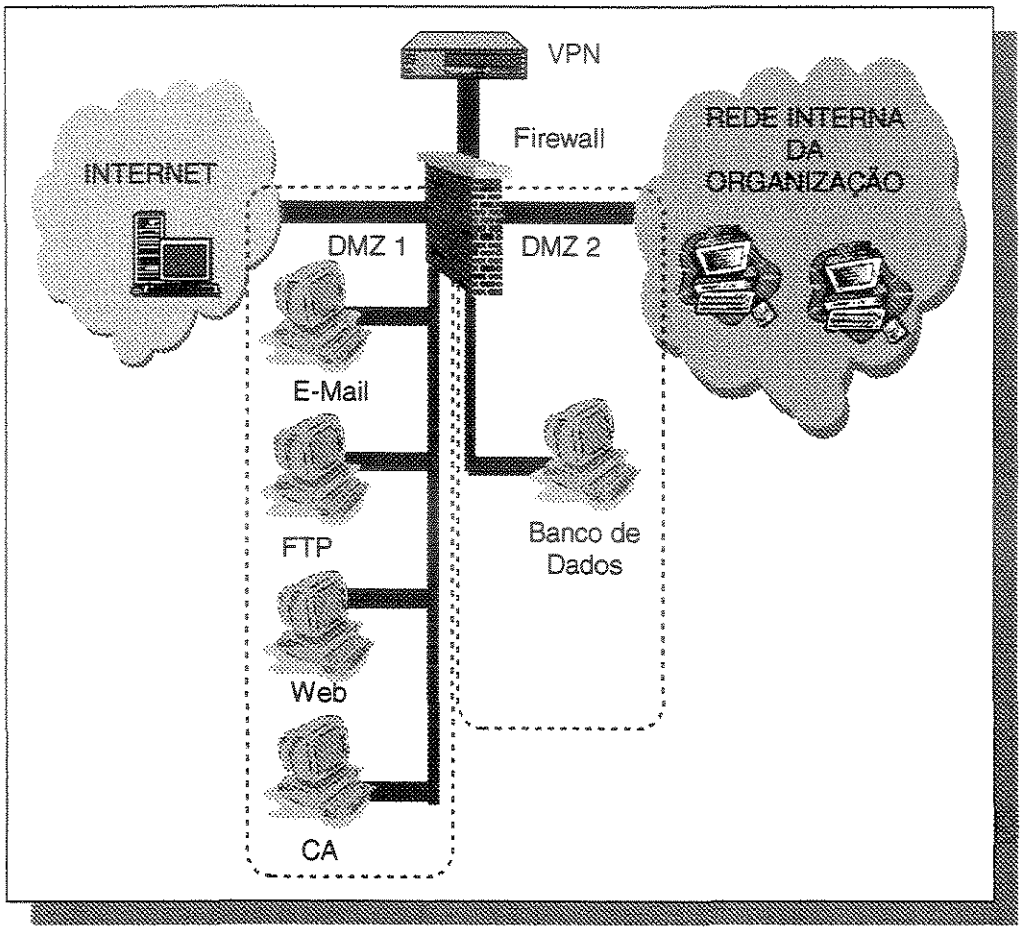


Figura 2.20: Localização do CA na DMZ. [NAK 03]

(somente a VPN pode se comunicar com a CA). Essa arquitetura pode ser vista na Figura 2.21, e ela elimina a possibilidade da CA sofrer acessos externos diretos. O usuário somente teria a permissão de acessar os recursos da rede interna da organização após a CA confirmar a sua identidade.

Apesar de ainda estar em processo de padronização, as certificações cruzadas fazem parte de uma funcionalidade fundamental em um ambiente cooperativo, ao permitir que, por exemplo, os usuários de uma fornecedora acessem recursos da matriz e das filiais, sem a necessidade de que certificados específicos para cada um deles sejam criados em cada uma das partes envolvidas nessa comunicação. Essa certificação cruzada faz com que uma infra-estrutura de chaves públicas seja um componente importante na estratégia de segurança da organização.

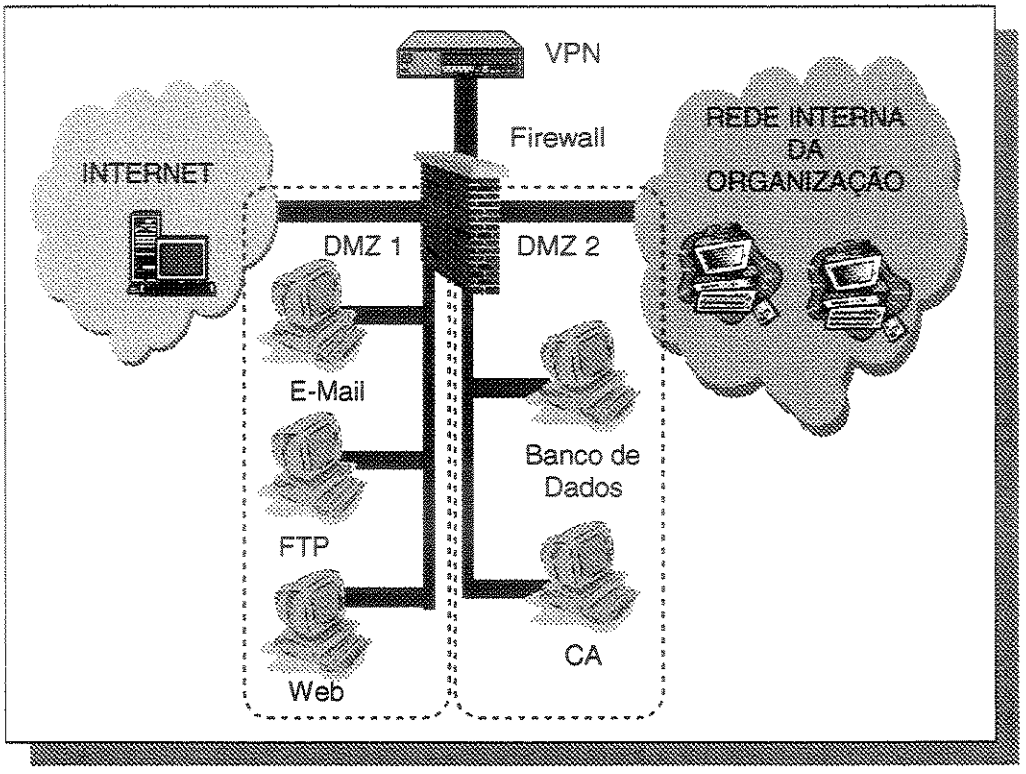


Figura 2.21: Localização do CA na segunda DMZ. [NAK 03]

2.2.11 Detecção de ataques com IDS

Um outro componente de segurança importante, principalmente no nível interno das organizações, são os sistemas de detecção de intrusões (IDS). Esses sistemas monitoram todas as atividades dos usuários dentro da rede da organização, de forma a poderem detectar anormalidades que podem ser prenúncios de ataques. A arquitetura de segurança com IDS pode ser implementada como no esquema da Figura 2.22: (1) IDS 1 – pouco utilizada, pois o *firewall* gera poucas informações que servem para análise; (2) IDS 2 – detecta ataques, que conseguiram burlar a proteção do *firewall*; (3) IDS 3 – detecta ataques contra o *firewall*; (4) IDS 4 – detecta ataques originados na rede interna da organização.

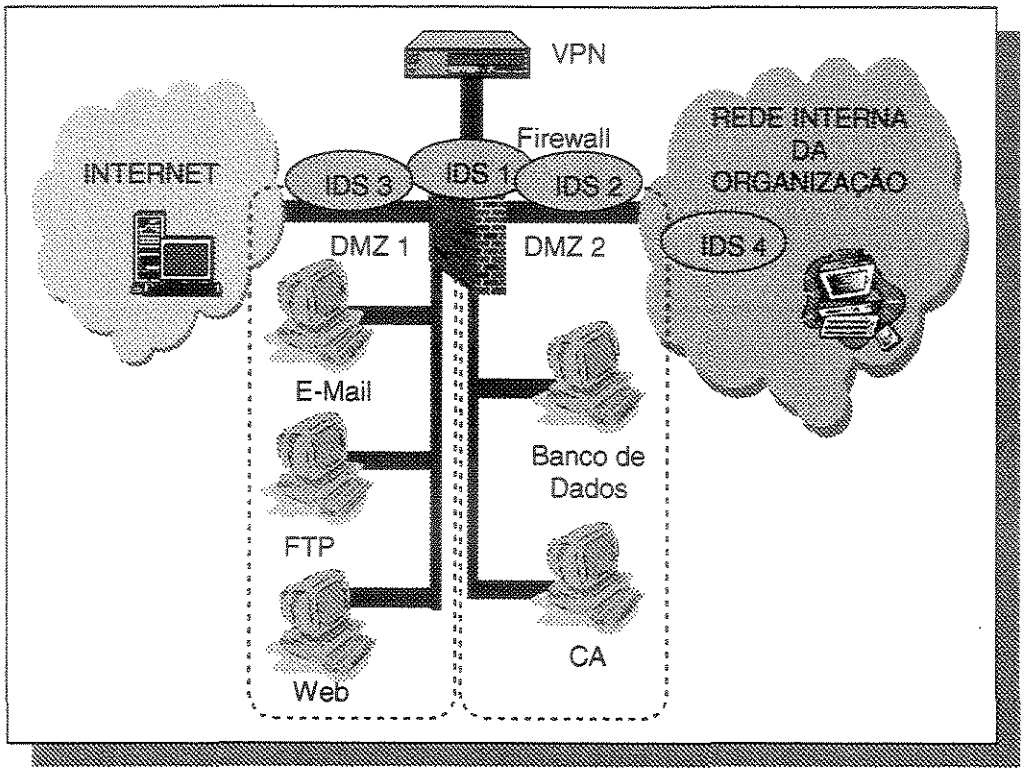


Figura 2.22: A arquitetura de segurança com o IDS. [NAK 03]

2.3 Ambiente Cooperativo Seguro

Uma característica dos ambientes cooperativos é a complexidade que envolve a comunicação entre diferentes tecnologias, usuários, culturas, e políticas internas de cada organização, sendo que o maior desafio do ambiente cooperativo é a forma escolhida para lidar com esta complexidade, sem comprometer a segurança da organização e de seus integrantes.

O desafio do ambiente cooperativo é grande, principalmente considerando as várias conexões existentes em conjunto, e na ausência de proteções específicas e regras, o que intensifica o risco de interferência e possibilidade de acesso às conexões de outros usuários.

Uma solução proposta para resolver este desafio é a utilização de um *firewall cooperativo* [NAK 03], cujo objetivo é tornar mais simples a administração da segurança do ambiente cooperativo, ao integrar e posicionar tecnologias específicas, tais como *firewall*, DMZ, VPN, PKI, IDS, NAT etc, para a proteção do ambiente (Figura 2.23).

Portanto, o Ambiente Cooperativo Seguro é definido como sendo a rede integrada virtualmente utilizada pelas várias organizações, que compõem o ambiente cooperativo para trocarem informações de vários tipos, combinada com o *firewall cooperativo*, cujo objetivo é proteger o ambiente formado.

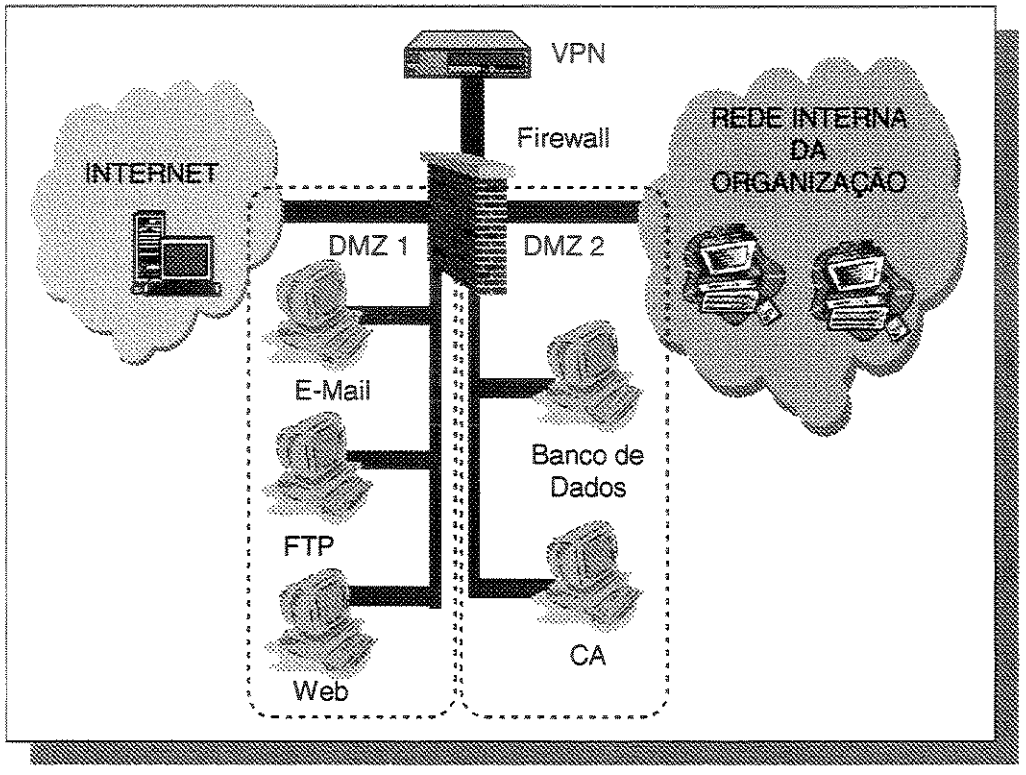


Figura 2.23: A arquitetura do *firewall* cooperativo. [NAK 03]

2.4 Novo elemento no Ambiente Cooperativo Seguro

É interessante notar que, assim como as relações comerciais entre as organizações são muito dinâmicas e evoluem constantemente, as tecnologias existentes à disposição das organizações sofre o mesmo processo de transformação, pois muitas delas são extintas, outras permanecem exatamente como foram concebidas e outras evoluem, como é o caso do protocolo de rede IP. A Internet, as redes privadas e públicas, as organizações e o próprio usuário doméstico, usam

IPv4, que nasceu na década de 70. Portanto, ele tinha o objetivo simples de facilitar a interconexão entre diferentes tecnologias físicas de rede usadas na ARPANET.

Em razão da distribuição irregular de endereços IP no mundo, IPv4 tem apresentado um número limitado de endereços disponíveis, o que motivou, além de outros acontecimentos não antecipados, a partir de 1993, esforços em projeto, desenvolvimento e implementação da versão do protocolo de rede, chamado IPv6, o qual é considerado uma das mais significativas atualizações de rede do momento [HUI 98].

IPv6 provê uma plataforma para as novas funcionalidades Internet, que serão exigidas num futuro muito próximo, tais como endereçamento expandido, suporte nativo a segurança e a mobilidade, assim como características de qualidade de serviço (QoS) dentre outras.

IPv6, ao contrário do seu antecessor, em sua especificação, foi fortemente influenciado por aspectos de segurança. Os projetistas de IPv6 buscaram manter os pontos fortes de IPv4 e trabalhar os pontos considerados problemáticos, sendo que falta de segurança no nível de rede é um deles.

A migração de uma rede IPv4 para IPv6 pode ocorrer passo a passo, começando com uma única máquina ou uma sub-rede, ou ainda, com a rede inteira da organização. No Capítulo 3 Seção 3.2, página 34 estão compiladas as principais características de IPv6, que podem motivar uma migração de IPv4 para IPv6 ou, ainda, motivar a formação de uma rede nativa IPv6, sem passar por uma rede IPv4 inicial.

2.5 Conclusão

Este capítulo discutiu a importância da informática para os negócios de todas as organizações. A necessidade cada vez maior de conexões resulta em uma complexidade alta nas configurações de redes de todos os envolvidos. O *firewall cooperativo* surge como uma solução para este problema, uma vez que integra todas as tecnologias disponíveis numa mesma estrutura de segurança. Contudo, a tecnologia não está estagnada, bem como as relações comerciais entre as organizações estão em constante mutação, o que impulsiona mudanças e adaptações nas tecnologias disponíveis, a exemplo do IPv6. O protocolo IPv6 será explicado no Capítulo 3, objetivando fornecer embasamento teórico para entendimento do restante do trabalho.

Capítulo 3

IPv6 - Protocolo da Próxima Geração

Neste capítulo será apresentado a próxima versão do protocolo da Internet, chamado Internet Protocol version 6 (IPv6). Baseados nas lições aprendidas com IPv4, os projetistas buscaram manter seus aspectos fortes e reformular suas deficiências. Conseqüentemente, IPv6 traz novas funcionalidades, tais como suporte nativo a segurança e a mobilidade, suporte melhorado para cabeçalhos de extensão, simplificação do cabeçalho base entre outras, o que constituem uma evolução da versão anterior.

3.1 Introdução

A atual versão do protocolo IP (conhecida como Versão 4 ou IPv4) não foi substancialmente alterada desde que a RFC 791 foi publicada em 1981. IPv4 provou ser robusto, fácil de implementar e suportou o teste de escalabilidade de uma rede pequena para o tamanho atual da Internet. Isto é um tributo ao projeto inicial de IPv4, que, contudo, não antecipou os seguintes acontecimentos:

- *o recente crescimento exponencial da Internet e a ameaça de exaustão do espaço de endereçamento IPv4*: os endereços IPv4 se tornaram relativamente escassos, forçando algumas organizações a usarem *Network Address Translator* (NAT) [SRI 01] para mapear múltiplos endereços privados em um único endereço IP público;
- *o crescimento da Internet e a capacidade dos roteadores de backbone manterem grandes tabelas de roteamento*: em função da forma como os identificadores de redes são alocados, existem mais de 85 mil rotas nas tabelas de roteamento do roteadores de backbone;

- *necessidade de configuração simplificada*: muitas implementações IPv4 atuais precisam ser configuradas manualmente ou usar um protocolo de configuração de endereço *stateful* como o *Dynamic Host Configuration Protocol* (DHCP). Com o acréscimo no número de computadores e outros dispositivos usando IP, há uma necessidade mais premente de simplificar e automatizar o processo de configuração de endereços e outras características;
- *a exigência de segurança no nível de rede IP*: privacidade em comunicações sobre o meio público da Internet exige serviços de criptografia, que protejam os dados de serem vistos ou alterados em trânsito. Embora exista o padrão IPSec para prover segurança para pacotes IPv4, sua implementação é opcional e prevalecem as soluções proprietárias;
- *a necessidade de um suporte melhorado para a entrega de dados em tempo-real, também chamado de Qualidade de Serviço (QoS)*: o campo ToS (*Type of Service*) do IPv4 tem funcionalidade limitada e muitas implementações não honram este campo.

Objetivando resolver estes e outros problemas, a *Internet Engineering Task Force* (IETF) [IET 86] desenvolveu um conjunto de protocolos e padrões conhecido como IP versão 6 (IPv6). Esta nova versão, anteriormente chamada de IP - *The Next Generation* (IPng), incorporou os conceitos de vários métodos propostos para atualizar o protocolo IPv4. O projeto de IPv6 objetiva causar o mínimo impacto nos protocolos das camadas acima e abaixo, eliminando a adição aleatória de novas características.

3.1.1 Características de IPv6

Abaixo estão compiladas as principais características do protocolo IPv6:

- *simplicação do formato do cabeçalho*: o cabeçalho IPv6 tem um novo formato para manter seu *overhead* o mínimo possível, o que é alcançado com a remoção de alguns campos não essenciais e opcionais para os cabeçalhos de extensão, que vêm logo após o cabeçalho base do IPv6. Desta forma, os pacotes são processados de forma mais eficiente pelos roteadores intermediários. Contudo, os cabeçalhos IPv4 e IPv6 não são interoperáveis, já que um roteador ou máquina precisa implementar ambos os protocolos para conseguir reconhecer e processar seus cabeçalhos;

- *espaço de endereçamento expandido*: IPv6 tem endereços IP de origem e destino de 128 *bits* ou 16 *bytes*. Embora 128 *bits* possam expressar $3{,}4x10^{38}$ possíveis combinações, o espaço de endereçamento IPv6 foi projetado para permitir diversos níveis de sub-redes. Com um espaço de endereçamento expandido, técnicas de conservação de endereços, como o NAT, não são mais necessárias;

- *suporte melhorado para extensões e opções*: em IPv4 as opções eram integradas no cabeçalho base do IPv4. Contudo, em IPv6 as opções são consideradas Cabeçalhos de Extensão. Os Cabeçalhos de Extensão são opcionais e inseridos apenas entre o cabeçalho base IPv6 e a carga útil de dados (*payload*), se necessário;

- *extensibilidade*: esta característica é conseqüência da anterior, pois IPv6 pode facilmente incorporar novas funcionalidade com a adição de Cabeçalhos de Extensão após o cabeçalho base IPv6. Enquanto as opções no cabeçalho IPv4 podem suportar somente 40 *bytes*, o tamanho dos cabeçalhos de extensão é limitado somente pelo tamanho do pacote IPv6;

- *configuração de endereço stateless e stateful*: para simplificar a configuração de máquinas, IPv6 suporta configuração de endereços *stateful*, que precisa de um servidor de DHCP, e configuração de endereços *stateless*, que ocorre na ausência de um servidor DHCP. Com a configuração *stateless*, as máquinas no mesmo enlace automaticamente se auto-configuram com endereços IPv6 do enlace, chamados endereços *link-local*, e com endereços derivados dos prefixos anunciados pelos roteadores locais. Mesmo na ausência de um roteador, as máquinas no mesmo enlace podem automaticamente se auto-configurar com endereços *link-local* e se comunicarem sem configuração manual;

- *suporte nativo a segurança*: suporte ao IPSec é uma exigência de IPv6, através das extensões de autenticação e confidencialidade;

- *suporte nativo a mobilidade*: IPv6 móvel permite roteamento transparente de pacotes IPv6 para nós móveis, tirando vantagem das oportunidades criadas pelo projeto da nova versão do IP. Além disto, cada nó móvel é sempre identificado pelo seu endereço *home*, independente de seu ponto de conexão na Internet. Enquanto o nó móvel estiver distante de sua subrede originária, ele está associado com um endereço *care-of*, que indica sua localização corrente. Desta forma, IPv6 móvel permite que qualquer nó IPv6 aprenda e armazene o endereço *care-of* associado com o endereço *home* do nó móvel e, então, envia pacotes destinados ao nó móvel diretamente para o endereço *care-of* usando o cabeçalho de *routing* do IPv6.

- *suporte melhorado para QoS*: novos campos no cabeçalho IPv6 definem como o tráfego é manipulado e identificado. Identificação de tráfego, usando o campo *Flow Label* do cabeçalho base IPv6, permite que roteadores identifiquem e providenciem manipulação especial para pacotes de um fluxo, que é uma série de pacotes entre uma origem e um destino;
- *novo protocolo para interação entre nós vizinhos*: o protocolo *Neighbor Discovery* [NAR 98] é uma série de mensagens *Internet Control Message Protocol* para IPv6 (ICMPv6), que gerencia a interação entre nós vizinhos (nós no mesmo enlace). O *Neighbor Discovery* substitui as mensagens do protocolo *Address Resolution Protocol* (ARP) [STE 94], *ICMPv4 Router Discovery* [STE 94] e *ICMPv4 Redirect* [STE 94] com suas mensagens *unicast* e *multicast Neighbor Discovery*.

3.2 Cabeçalho IPv6

O cabeçalho IPv6 [DEE 98] é uma versão otimizada do cabeçalho IPv4, uma vez que eliminou campos que não eram necessários ou raramente usados e adicionou campos para prover melhor suporte a tráfego em tempo real.

3.2.1 Estrutura do pacote IPv6

A Figura 3.1 mostra a estrutura do pacote IPv6. O cabeçalho IPv6 está sempre presente e tem comprimento fixo de 40 *bytes*, sendo que os dois campos de endereço origem e destino usam 16 bytes cada, o que resta somente 8 bytes para informação geral no cabeçalho.

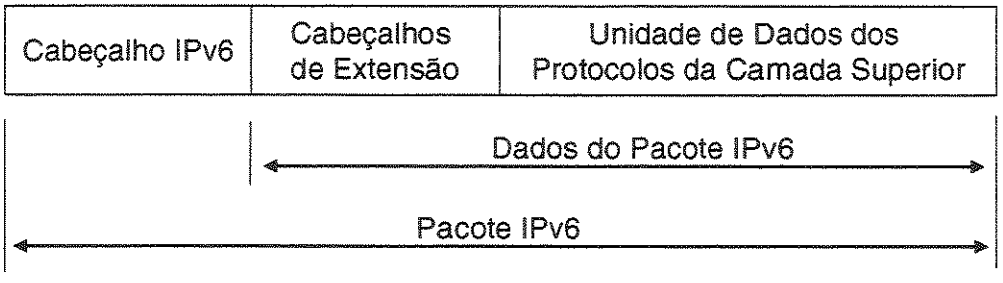


Figura 3.1: Estrutura do Pacote IPv6.

Os cabeçalhos de extensão podem estar ou não presentes no pacote IPv6, além de serem de tamanhos variáveis. A forma de implementação dos cabeçalhos de extensão permite que IPv6 suporte novas funcionalidades no futuro.

A unidade de dados dos protocolos da camada superior consiste usualmente do cabeçalho do protocolo da camada superior e sua carga útil de dados (por exemplo, mensagem ICMPv6 ou mensagem UDP ou segmento TCP). Os dados do pacote IPv6 são uma combinação dos cabeçalhos de extensão com a unidade de dados dos protocolos da camada superior.

3.2.2 Estrutura geral do cabeçalho IPv6

Cinco campos do cabeçalho IPv4 foram removidos do cabeçalho IPv6:

- *header length*: o cabeçalho IPv6 tem tamanho fixo de 40 bytes;
- *identification, flags e fragment offset*: informação de fragmentação não aparece no cabeçalho IPv6, uma vez que existe o cabeçalho de extensão *Fragment* específico para quando a fragmentação for necessária;
- *header checksum*: foi removido para melhorar a velocidade de processamento dos pacotes IP. Além disso, a detecção de erros no nível de *bit* é realizada pela camada de enlace, assim como existe *checksum* na camada de transporte UDP e TCP.

A Figura 3.2 ilustra o cabeçalho IPv6, seguida da descrição dos campos:

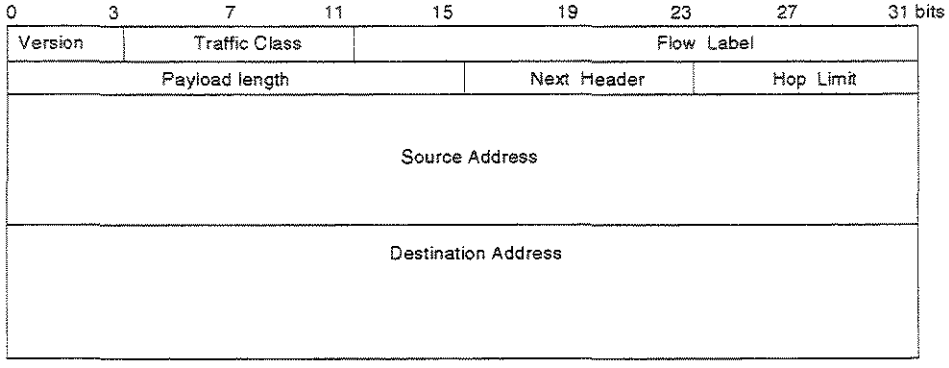


Figura 3.2: Cabeçalho IPv6.

- *Version (4 bits)*: indica a versão do protocolo IP, no caso de IPv6 o número é 6;

- *Traffic Class (1 byte)*: indica a classe ou prioridade do pacote IPv6;
- *Flow Label (20 bits)*: indica que este pacote pertence a uma seqüência específica de pacotes entre uma origem e um destino, exigindo tratamento especial pelos roteadores IPv6 intermediários;
- *Payload Length (2 bytes)*: indica o comprimento da carga do pacote IPv6, o que inclui os cabeçalhos de extensão e a unidade de dados da camada superior;
- *Next Header (1 byte)*: indica qual é o próximo cabeçalho após o cabeçalho base IPv6, podendo ser tanto os cabeçalhos de extensão como os protocolos da camada superior, como TCP, UDP ou ICMPv6;
- *Hop Limit (1 byte)*: indica o número máximo de saltos que o pacote IPv6 pode dar antes de ser descartado;
- *Source Address (16 bytes)*: armazena o endereço IPv6 da máquina origem;
- *Destination Address (16 bytes)*: armazena o endereço IPv6 da máquina destino.

3.2.3 Cabeçalhos de extensão

A especificação de IPv6 [DEE 98] define seis cabeçalhos de extensão:

- *hop-by-hop options*: carrega informações opcionais que precisam ser examinadas por cada nó que esteja no caminho do pacote até o destino. Por isto, quando necessário, ele deve vir logo após o cabeçalho base IPv6, já que ele é o único cabeçalho a ser examinado por cada nó intermediário;
- *routing*: é usado para fornecer uma lista de um ou mais nós intermediários que devem ser visitados no caminho do pacote até o destino;
- *fragment*: é usado para serviços de fragmentação e remontagem de pacotes. Se um pacote a ser enviado é maior que o *Maximum Transmission Unit* (MTU) suportado, então o nó origem fragmenta o pacote, já que em IPv6, somente os nós origem podem fragmentar;
- *destination options*: é usado para especificar parâmetros opcionais que são examinados pelos nós intermediários ou pelo destino final, o que dependerá da posição onde ele estiver na ordem dos cabeçalhos de extensão;

- *authentication* e *encapsulating security payload*: serão analisados em detalhes no Capítulo 4.

A Figura 3.3 ilustra a ordem dos cabeçalhos de extensão em um pacote IPv6. É interessante observar que o cabeçalho de extensão *destination options* aparece em dois lugares: (1) para ser analisado por nós intermediários, quando o cabeçalho *Routing* estiver presente e (2) para ser analisado pelo destino final do pacote.

Figura 3.3: Ordem dos Cabeçalhos de Extensão em um Pacote IPv6.

3.3 Endereçamento IPv6

Sem dúvida, a mais drástica mudança provida por IPv6 é o aumento do tamanho do campo endereço. O tamanho de um endereço IPv6 é 128 bits, o que representa quatro vezes o tamanho do endereço IPv4. Um espaço de endereço de 32 bits permite 2^{32} ou 4.294.967.296 possíveis endereços, assim como um espaço de endereço de 128 bits permite 2^{128} ou 340.282.366.920.938.463.463.374.607.431.768.211.456 ou, ainda, $3{,}4x10^{38}$ possíveis endereços.

3.3.1 Sintaxe do endereço IPv6

Um endereço IPv6 [HIN 03a] é dividido em oito blocos de 16 bits cada, sendo que os blocos são convertidos em número hexadecimal de 4 dígitos e separados por dois pontos. Um exemplo é este endereço IPv6: 3FFE:2B00:0100:0000:0000:0000:02AA:00FF. Esta representação pode também ser simplificada removendo os zeros a esquerda em cada bloco de 16 bits, conforme segue 3FFE:2B00:100:0:0:0:2AA:FF. Alguns tipos de endereço contém longas seqüências de zeros. Para simplificar ainda mais a representação do endereço IPv6, uma seqüência contígua de blocos de zeros podem ser substituídos por dois pontos duplo "::", conforme pode ser verificado no exemplo: 3FFE:2B00:100::2AA:FF. Note que o dois pontos duplo pode ocorrer somente uma vez no endereço. A razão para esta regra é que o computador sempre usa a representação binária completa do endereço com 128 bits, mesmo se o endereço mostrado for simplificado. Quando

um computador encontra um dois pontos duplo, ele o expande com quantos zeros são necessários para chegar a 128 bits. Se um endereço tem mais de um dois pontos duplo, o computador não saberá quantos zeros adicionar a cada um dos dois pontos duplos.

3.3.2 Prefixo IPv6

O prefixo é a parte do endereço, geralmente os bits de mais alta ordem, que identifica uma rede, sub-rede ou o tipo específico de endereço. A notação do prefixo IPv6 é muito similar à notação *Classless Inter-Domain Routing* (CIDR) para IPv4. Um prefixo IPv6 é escrito na notação *address/prefix-length*, conforme este exemplo: 3FFE:2B00::/48, onde 3FFE:2B00:: é o prefixo da rota e / 48 é o comprimento do prefixo.

3.3.3 Tipos de endereços IPv6

A arquitetura de endereçamento IPv6 define 3 tipos diferentes de endereços [HIN 03a]:

- *unicast*: identificador de uma única interface. Um pacote enviado para um endereço *unicast* é entregue para a interface identificada por este endereço [REK 95];
- *anycast*: identificador de um conjunto de interfaces (pertencentes a nós diferentes). Um pacote enviado para um endereço *anycast* é entregue para uma das interfaces identificada por este endereço (o mais próximo, de acordo com a medida de distância do protocolo de roteamento). Este endereço é usado para comunicações *one-to-one-of-many* [PAR 93];
- *multicast*: identificador de um conjunto de interfaces (pertencentes a nós diferentes). Um pacote enviado para um endereço *multicast* é entregue para todas as interfaces identificadas por este endereço. Este endereço é usado em comunicações *one-to-many*. Note que o endereço *broadcast* não aparece em IPv6, pois sua função é substituída pelo *multicast*.

Em IPv6, todos os bits "zero" e "um" são valores permitidos para qualquer campo em um endereço. Os endereços IPv6 são designados para interfaces. De modo que um nó, assim como um roteador, pode ter múltiplas interfaces e, portanto, múltiplos endereços *unicast*. Além disso, uma única interface pode ter múltiplos endereços de qualquer tipo (*unicast*, *multicast*, *anycast*) ou escopo.

Um endereço IPv6 típico consiste de 3 partes: o prefixo de roteamento global, o identificador de sub-rede e o de interface (Figura 3.4).

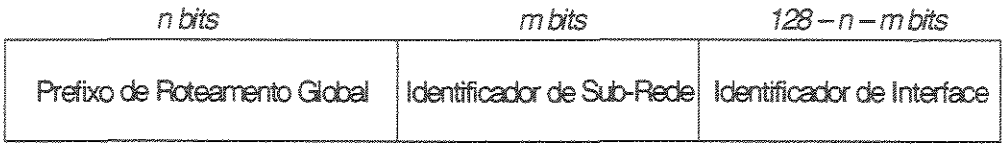


Figura 3.4: Formato Geral do Endereço IPv6.

3.3.4 *Unicast*

Os seguintes tipos de endereços são *unicast* IPv6:

- *global unicast*;
- *local-use unicast*;
- *special*.

3.3.4.1 Endereços *unicast* global

Endereços *unicast* global [HIN 03b] são equivalentes ao endereços públicos IPv4, já que eles são roteáveis globalmente na porção IPv6 da Internet. A Figura 3.5 mostra a estrutura de um endereço *unicast* global, que atualmente é alocado pela IANA [IAN 03]. Os campos definidos são:

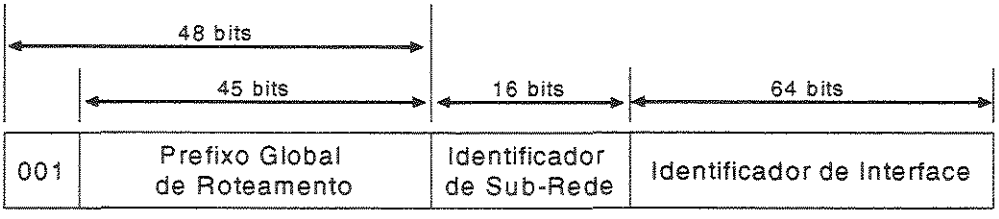


Figura 3.5: Estrutura do Endereço IPv6 *Unicast* Global.

- *porção fixa em 001*: os três bits de alta ordem são 001. O prefixo deste endereço é 2000::/3;
- *prefixo global de roteamento*: indica o prefixo global de roteamento para a rede específica de uma organização. A combinação dos três primeiros bits com os 45 bits do prefixo global routing é usada para criar o prefixo de 48 bits, que é usado para identificar a rede de uma organização;

- *identificador de sub-rede*: o identificador de sub-rede é usado na rede da organização para identificar sub-redes. O tamanho deste campo é 16 bits;
- *identificador de interface*: indica a interface numa sub-rede específica. O tamanho deste campo é 64 bits.

Os campos no endereço *unicast* global criam uma estrutura em três níveis, conforme mostra a Figura 3.6. A topologia pública é uma coleção de grandes e pequenos ISPs, que provêem acesso a rede IPv6. A topologia da rede é a coleção de sub-redes dentro da rede de uma organização, assim como o identificador de interface identifica uma interface específica em uma sub-rede da organização.

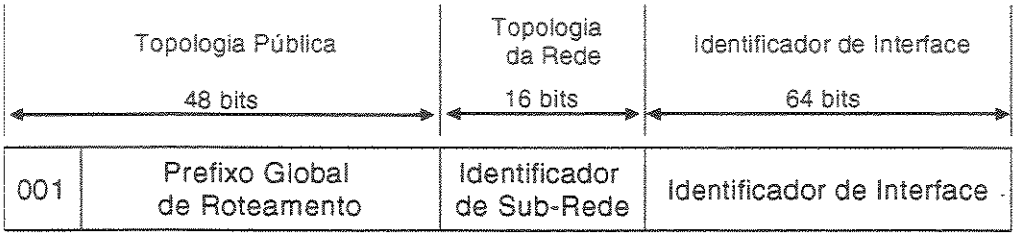


Figura 3.6: Estrutura em Três Níveis do Endereço IPv6 Unicast Global.

3.3.4.2 Endereços *local-use unicast*

Existem dois tipos de endereços *local-use* (uso local) *unicast*:

- *endereços link-local*: são usados por nós quando se comunicando com nós vizinhos no mesmo enlace. Por exemplo, em um único enlace IPv6 sem roteador, endereços *link-local* são usados pelas máquinas no enlace para se comunicarem entre si. O escopo deste endereço é o enlace local, de modo que os roteadores nunca encaminham para outro enlace pacotes com este endereço. Ele é usado também pelos processos do *Neighbor Discovery* e é sempre automaticamente configurado, mesmo na ausência de todos os outros tipos de endereços *unicast*. Os dez primeiros bits deste endereço sempre começam com FE80::/10;
- *endereços site-local*: estes endereços são equivalentes aos endereços IPv4 privados (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16). O escopo deste endereço é dentro da rede da organização, de modo que, não pode ser roteável para fora da rede. Ele pode ser usado

em conjunto com os endereços *unicast* global. Estes endereços não são automaticamente configurados e precisam ser designados com configuração *stateless* ou *stateful*. Os 10 primeiros bits deste endereço são fixos em FEC0::/10.

3.3.4.3 Endereços *special*

Os endereços seguintes são especiais:

- *unspecified*: é usado para identificar a ausência de um endereço e é representado por 0:0:0:0:0:0:0:0 ou ::. Ele pode ser usado no momento do *boot* de uma máquina, para solicitar informação para configuração de endereço;
- *loopback*: é usado para identificar a interface *loopback*, permitindo que o nó envie pacotes para ele mesmo. É representado por 0:0:0:0:0:0:0:1 ou ::1. Pacotes endereçados ao endereço *loopback* não devem ser enviados no enlace ou encaminhados por um roteador IPv6.

3.3.4.4 Endereços compatíveis

Para auxiliar na migração de IPv4 para IPv6 e na coexistência de ambos os tipos de máquinas, os seguintes endereços foram definidos:

- *endereço IPv4-compatible*: o endereço *IPv4-compatible*, 0:0:0:0:0:0:w.x.y.z ou ::w.x.y.z (onde w.x.y.z é a representação decimal de um endereço IPv4), é usado por nós IPv6/IPv4 que se comunicam usando IPv6. Os nós IPv6/IPv4 são nós que possuem os dois protocolos implementados;
- *endereço IPv4-mapped*: o endereço *IPv4-mapped*, 0:0:0:0:0:FFFF:w.x.y.z ou ::FFFF:w.x.y.z, é usado para representar um nó *IPv4-only* para um nó IPv6. É usado somente para representação interna. Além disto, este endereço nunca é usado como origem ou destino de um pacote IPv6;
- *endereço 6to4*: é usado para comunicação entre dois nós rodando IPv4 e IPv6 sobre uma infra-estrutura de roteamento IPv4. O endereço *6to4* é formado combinando o prefixo 2002::/16 com os 32 bits de um endereço IPv4 público de um nó, formando um prefixo de 48 bits. *6to4* é uma técnica de tunelamento [CAR 01].

3.3.5 *Anycast*

Um Endereço *Anycast* [PAR 93] é designado para múltiplas interfaces. Pacotes endereçados a um endereço *anycast* são encaminhados pela infra-estrutura de roteamento para a interface mais perto do endereço *anycast* designado. Para facilitar a entrega, a infra-estrutura de roteamento deve estar atenta às interfaces designadas como *anycast* e a suas "distâncias" em termos de métricas de roteamento.

Endereços *anycast* são alocados do espaço de endereçamento *unicast*, por isto não é possível identificá-los como *anycast* olhando apenas no prefixo. Se um endereço *unicast* for designado para várias interfaces, então ele se torna *anycast*, porém as interfaces devem ser configuradas para saberem que aquele endereço é *anycast*.

Um uso esperado para endereços *anycast* é identificar o conjunto de roteadores pertencentes a uma organização provendo algum serviço Internet. Um possibilidade é configurar todos os roteadores de uma organização, que provêem acesso à Internet, com um endereço *anycast* específico. Qualquer pacote enviado para este endereço *anycast*, será entregue para o roteador mais próximo que provê acesso à Internet. Existem algumas restrições no uso deste endereço: (1) não pode ser usado como endereço origem de um pacote IPv6 e (2) não pode ser designado para máquinas de trabalho, somente para roteadores.

3.3.6 *Multicast*

Um endereço *multicast* é um identificador de um grupo de nós, identificado pelo *byte* de alta ordem FF, ou 1111 1111 em representação binária. Um nó pode pertencer a mais de um grupo *multicast*. Além dos oito primeiros bits, o endereço *multicast* inclui estrutura adicional para identificar *flags*, escopo e grupo *multicast*. O formato do endereço *multicast* é mostrado na Figura 3.7.

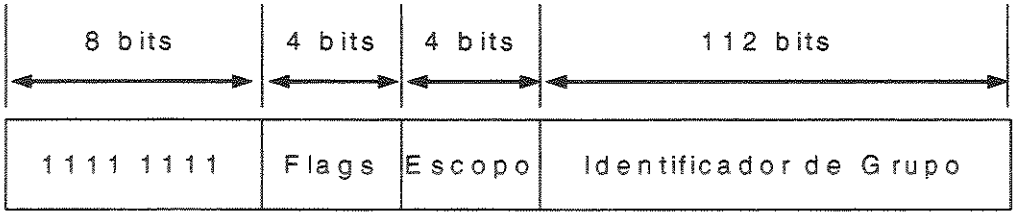


Figura 3.7: Formato Geral do Endereço *Multicast*.

O primeiro *byte* identifica o endereço como *multicast*. Os próximos 4 bits são usados como *flags*, sendo que os 3 primeiros bits são reservados para uso futuro e devem ser zerados, contudo o último bit, flag *Transient* (T), identifica se o endereço é designado permanentemente (bit T=0) ou temporariamente (bit T=1). O campo Escopo é usado para limitar o escopo do endereço *multicast*, sendo que os valores mais freqüentes são 1 (*interface-local scope*), 2 (*link-local scope*) e 5 (*site-local scope*). A seguir será explicado sobre o campo identificador de grupo.

3.3.6.1 Endereços *multicast* bem-conhecidos

O identificador do grupo identifica o grupo *multicast* e é único em um escopo. O tamanho deste campo é 112 bits. Identificadores de grupo permanentemente designados são independentes do escopo, contudo identificadores de grupo temporários são relevantes somente dentro de escopos específicos. A lista de endereços *multicast* permanentemente designados é encontrada em [HIN 98b].

Como um exemplo, considere os servidores de NTP. Eles podem receber qualquer identificador de grupo *multicast* designado permanentemente, neste caso será 0x101 (hex). Este identificador pode ser usado em diferentes escopos, como segue:

- FF01:0:0:0:0:0:0:101: todos os servidores NTP no mesmo nó do transmissor;
- FF02:0:0:0:0:0:0:101: todos os servidores NTP no mesmo enlace do transmissor;
- FF05:0:0:0:0:0:0:101: todos os servidores NTP na mesma rede do transmissor;
- FF0E:0:0:0:0:0:0:101: todos os servidores NTP da Internet.

3.3.6.2 Endereços *multicast solicited-node*

O endereço *solicited-node* otimiza o processo de resolução de endereço. Em IPv4, o *frame* da pergunta ARP é enviada em *broadcast*, o que atrapalha todos os nós no segmento de rede. IPv6 usa as mensagens de *Neighbor Discovery* para executar a resolução de endereços. Porém, ao invés de usar o endereço *multicast* de escopo *local-link* para todos os nós do enlace, o endereço *multicast solicited-node* é usado. Este endereço é formado com os últimos 24 bits do endereço IPv6, que é anexado ao prefixo FF02:0:0:0:0:1:FF00::/104, conforme a Figura 3.8.

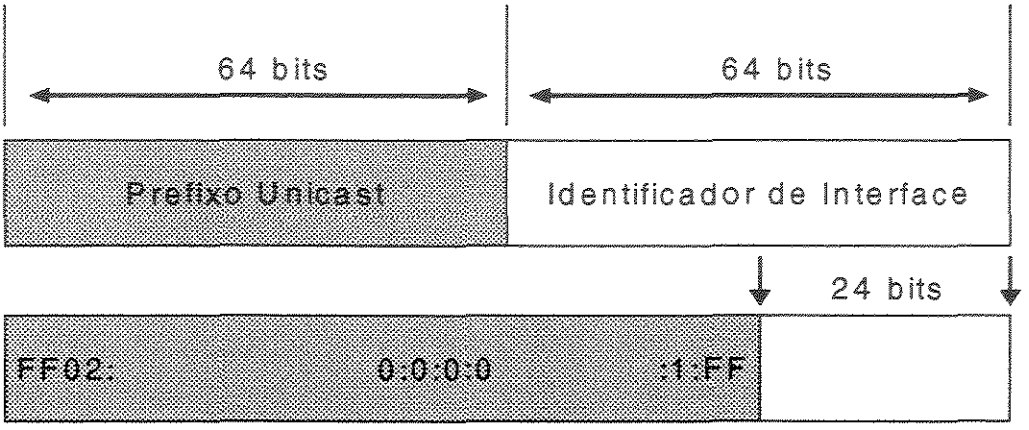


Figura 3.8: O Endereço *Multicast Solicited-Node*.

Por exemplo, o nó A tem o endereço *link-local* FE80::2AA:FF:FE28:9C5A e também o endereço correspondente *solicited-node* FF02::1:FF28:9C5A. O resultado de usar o endereço *multicast solicited-node* é que a resolução de endereço, uma ocorrência comum em um enlace, não usa um mecanismo que atrapalha todos os outros nós da rede. Na verdade, poucos nós são atrapalhados.

3.3.7 Endereços IPv6 para uma máquina

Uma máquina IPv6 usualmente tem múltiplos endereços IPv6, mesmo em uma única interface. Os endereços *unicast* e *multicast* designados para uma máquina IPv6 são:

- endereço *link-local* para cada interface;
- endereço *unicast* para cada interface (que pode ser um endereço *site-local* ou global);
- endereço *loopback* (::1) para a interface *loopback*;
- endereço *multicast solicited-node* para cada endereço *unicast* de cada interface;
- endereços *multicast* de escopo *interface-local* (FF01::1) e *link-local* (FF02::1) para todos os nós;
- endereços *multicast* para todos os grupos aos quais a máquina pertença.

3.3.8 Endereços IPv6 para um roteador

Os seguintes endereços são designados para um roteador:

- endereço *link-local* para cada interface;
- endereço *unicast* para cada interface (que pode ser um endereço *site-local* ou global);
- endereço *loopback* (::1) para a interface *loopback*;
- endereço *anycast*;
- endereço *multicast solicited-node* para cada endereço *unicast* de cada interface;
- endereços *multicast* de escopo *interface-local* (FF01::1) e *link-local* (FF02::1) para todos os nós;
- endereços *multicast* de escopo *interface-local* (FF01::2), *link-local* (FF02::2) e *site-local* (FF05::2) para todos os roteadores;
- endereços *multicast* para todos os grupos aos quais o roteador pertença.

3.4 ICMPv6

IPv6 usa uma versão atualizada do *Internet Control Message Protocol* (ICMP), chamada ICMP version 6 (ICMPv6) [CON 98], que fornece importantes informações sobre a saúde da rede, reportando erros ao IP. ICMPv6 suporta IPv6 Móvel [JOH 03], além de também prover um *framework* para:

- *Multicast Listener Discovery (MLD)* [HAB 03]: são três mensagens ICMPv6, que substituem a versão 2 do *Internet Group Management Protocol* (IGMP) [FEN 97], que é o protocolo usado para gerenciar o roteamento eficiente dos pacotes destinados a grupos *multicast*.
- *Neighbor Discovery Protocol (NDP)* [NAR 98]: são cinco mensagens ICMPv6, que gerenciam a comunicação nó a nó no enlace. NDP substitue as mensagens de *Address Resolution Protocol* (ARP), de *ICMPv4 Router Discovery* e de *ICMPv4 Redirect*.

3.4.1 Tipos de mensagens ICMPv6

Existem dois tipos de mensagens ICMPv6:

- *erro:* que são usadas para reportar erros na entrega e roteamento de pacotes IPv6, tanto no nó destino como em algum roteador intermediário. O valor do campo *Type* nas mensagens de erro está no intervalo de 0 a 127 (o bit de alta ordem é igual a 0). Além disso, inclui as mensagens de *Destination Unreachable, Packet Too Big, Time Exceeded* e *Parameter Problem*;

- *informação:* que são usadas para prover funções de diagnóstico e funcionalidades adicionais como MLD e NDP, além de incluir *Echo Request* e *Echo Reply*. O valor do campo *Type* nas mensagens de informação ICMPv6 está no intervalo de 128 até 255 (o bit de alta ordem é igual a 1).

3.4.2 Formato geral das mensagens ICMPv6

Todas as mensagens ICMPv6 têm a mesma estrutura do cabeçalho geral, conforme é possível observar na Figura 3.9. Os campos são:

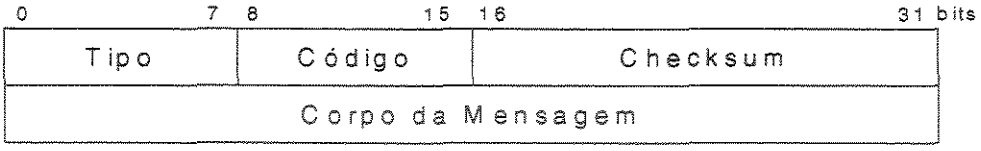


Figura 3.9: Formato Geral das Mensagems ICMPv6.

- *Tipo (1 byte)*: especifica o tipo de mensagem, o que determina o formato do restante da mensagem;
- *Código (1 byte)*: depende do tipo da mensagem e permite diferenciar entre múltiplas mensagens de um dado tipo de mensagem;
- *Checksum (2 bytes)*: é usado para detectar a corrupção de dados no cabeçalho ICMPv6 e em partes do cabeçalho IPv6, já que para calcular o *checksum*, um nó precisa determinar o endereço origem e destino no cabeçalho IPv6;
- *Corpo da Mensagem (tamanho variável)*: dependendo do tipo e código, o corpo da mensagem tem informações diferentes.

3.4.3 Neighbor Discovery

O Neighbor Discovery Protocol (NDP) é parte do ICMPv6. As funções do NDP são:

- *Router Discovery (RD)*: permite que máquinas IPv6 descubram os roteadores locais no enlace. Seu principal objetivo é encontrar roteadores vizinhos, que encaminham pacotes em benefício das máquinas;

- *Prefix Discovery (PD)*: descoberta do prefixo da rede envolve determinar se o destino está diretamente no enlace; esta informação é necessária para saber se o pacote será encaminhado para o roteador ou para o nó destino diretamente;
- *Address Autoconfiguration*: é usada para automaticamente designar endereços para as máquinas. Permite que uma máquina funcione sem configuração explícita de endereçamento IP. O mecanismo padrão de auto-configuração é o *stateless*. As máquinas usam qualquer informação de prefixo, para criarem seus endereços IP e, então, testarem se estes endereços não estão sendo usados por nenhuma outra máquina;
- *Address Resolution*: as máquinas no enlace resolvem o endereço IPv6 de uma máquina no correspondente endereço de enlace;
- *Neighbor Unreachability Detection (NUD)*: é usado para rastrear a acessibilidade das máquinas e dos roteadores;
- *Duplicate Address Detection (DAD)*: é usado para previnir colisões de endereços, que podem ocorrer durante o processo de auto-configuração de endereços. Uma máquina, que pretenda usar um novo endereço em alguma de suas interfaces, deve primeiro rodar o procedimento DAD para verificar se existe outra máquina usando o mesmo endereço;
- *Redirection*: é usada para automaticamente redirecionar uma máquina para um roteador mais conveniente ou para informar que um destino é na verdade um vizinho, ou seja, está no enlace.

As mensagens NDP seguem o formato da mensagem ICMPv6. Todas as funções NDP são realizadas usando as mensagens ICMPv6 *Router Solicitation* (RS), *Router Advertisement* (RA), *Neighbor Solicitation* (NS), *Neighbor Advertisement* (NA) e *Redirect*. Uma mensagem NDP consiste do cabeçalho da mensagem NDP e de nenhuma ou mais opções NDP (Figura 3.10). As opções da mensagem NDP seguem o formato Type-Length-Value.

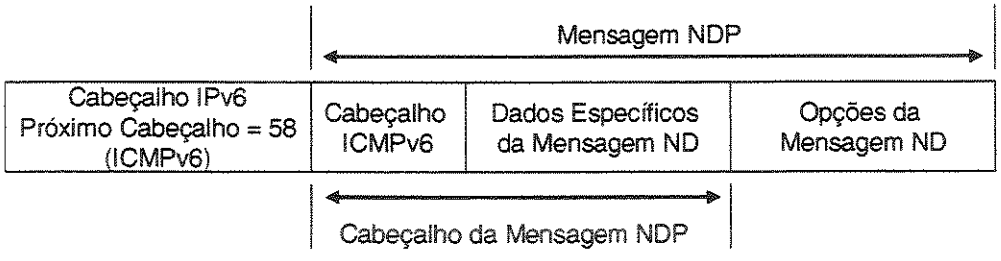


Figura 3.10: Formato Geral da Mensagem NDP.

Para assegurar que as mensagens NDP recebidas são originadas de um nó no enlace local, todas elas são configuradas com um *hop limit* de 255. Quando uma mensagem recebida não tem este valor, ela é descartada. Isto provê a proteção contra ataques de rede baseados em NDP originados de nós fora do enlace. No Capítulo 4 será analisada a questão de segurança no protocolo NDP.

3.4.4 Auto-configuração

A capacidade de auto-configuração de IPv6 [THO 98] foi projetada para assegurar que a configuração manual de máquinas, antes de conectá-las à rede, não seja necessária. Auto-configuração será uma característica chave de IPv6 quando todo tipo de equipamentos, tais como TVs, refrigeradores, *DVD players* e telefones móveis, usar um endereço IP.

Por padrão, uma máquina IPv6 pode configurar o endereço *link-local* para cada interface sem ajuda adicional. Contudo, usando *router discovery*, uma máquina pode também determinar o endereço do roteador, outros parâmetros de configuração, endereços adicionais e prefixos do enlace, ou seja, alguma configuração deve ser feita nos roteadores, contudo não é preciso ter um servidor DHCP. Roteadores podem anunciar vários prefixos e as máquinas determinam a informação do prefixo destes anúncios. O que simplifica o processo de renumerar uma rede, já que apenas a informação do prefixo precisa ser alterada nos roteadores.

Um endereço IPv6 é alocado para uma máquina por um certo tempo. Em razão disto, ele tem diferentes estados:

- *tentative* - é um endereço que ainda não foi designado, mas que está no estágio inicial de designação, quando a unicidade do endereço é verificada;
- *valid* - é um endereço que passou pelo estágio de verificação da unicidade e que pode receber e enviar tráfego *unicast*. Este endereço cobre os estados *preferred* e *deprecated*;
- *preferred* - é um endereço que foi designado para uma interface e que pode ser usado sem nenhuma restrição;
- *deprecated* - é um endereço ainda válido, já que comunicações em andamento podem usá-lo, contudo seu tempo de vida está próximo de expirar, então não deve ser usado para novas comunicações;

- *invalid* - é um endereço que o nó não pode mais usar para enviar ou receber tráfego *unicast*. Ele entra neste estado quando o tempo de vida válido expira.

A relação entre os estados de um endereço auto-configurado e os tempos de vida é mostrado na Figura 3.11.

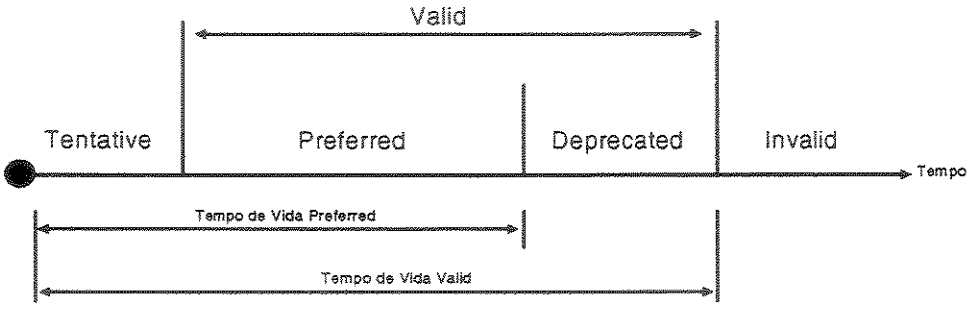


Figura 3.11: Os estados e os tempos de vida de um endereço auto-configurado.

O processo de auto-configuração do endereço para a interface física de um nó IPv6 é o seguinte:

- endereço *link-local* é gerado usando o prefixo *link-local* FE80::/64 e anexando o identificador da interface de 64 bits. Este endereço é considerado um endereço *tentative*;
- usando o processo DAD para verificar a unicidade do endereço *tentative link-local*, uma mensagem NS é enviada com o campo *Target Address* preenchido com o endereço *tentative link-local*;
- se alguma mensagem de NA é recebida em resposta à mensagem NS, isto indica que outro nó no enlace esta usando o mesmo endereço *tentative link-local*, então o processo de auto-configuração para e a configuração manual deve ocorrer;
- se nenhuma mensagem de NA é recebida em resposta à mensagem NS, então o endereço *tentative link-local* é considerado único e válido. Ele é inicializado para a interface e o correspondente endereço *solicited-node multicast link-layer* é registrado.

Contudo, se for uma máquina IPv6, então o processo de auto-configuração continua:

- a máquina envia até três mensagens de RS;
- se nenhuma mensagem de RA é recebida, então a máquina usa o protocolo *stateful* de configuração de endereço para obter endereços e outros parâmetros;

- se uma mensagem de RA é recebida, os valores *Hop Limit*, *Reachable Time*, *Retrans Timer* e MTU são configurados;
- para cada opção de informação de prefixo presente:
  - se o flag *On-Link* está setado em 1, então o prefixo é adicionado na lista de prefixos;
  - se o flag *Autonomous* está setado em 1, o prefixo e o identificador de interface de 64 bits são usados para derivar o endereço *tentative*.
    - DAD é usado para verificar a unicidade do endereço *tentative*. Se ele esta em uso em outra máquina, então ele não é inicializado. Se ele não está em uso, então é inicializado. Isto inclui configurar os tempos de vida *valid* e *preferred* baseado nos campos *Valid Lifetime* e *Preferred Lifetime* das opções de informação do prefixo. Também inclui registrar o endereço correspondente *solicited-node multicast link-layer*.
- se o flag *Managed Address Configuration* na mensagem RA está setado para 1, então o protocolo de configuração de endereço *stateful* é usado para obter endereços adicionais;
- se o flag *Other Stateful Configuration* na mensagem RA está setado para 1, então o protocolo *stateful* de configuração de endereço é usado para obter parâmetros de configuração adicionais.

O processo de auto-configuração de endereço IPv6 para uma máquina é ilustrado nas Figura 3.12 e Figura 3.13.

3.5 Estado Atual de Desenvolvimento e Implantação de IPv6 no Brasil e no Mundo

3.5.1 LACNIC - *Latin American and Caribbean Internet Addresses Registry*

O LACNIC [LAC 02] é a organização responsável pela administração do espaço de endereçamento IP, Números de Sistemas Autônomos (ASN), resolução reversa e outros recursos para a região da América Latina e Caribe em nome da comunidade Internet.

LACNIC é uma organização sem fins lucrativos e estabelecida juridicamente no Uruguai. Suas políticas e procedimentos são baseados em RFC's relacionadas com a administração de endereços IP, números de sistemas autônomos e resolução reversa. No entanto, mecanismos de parti-

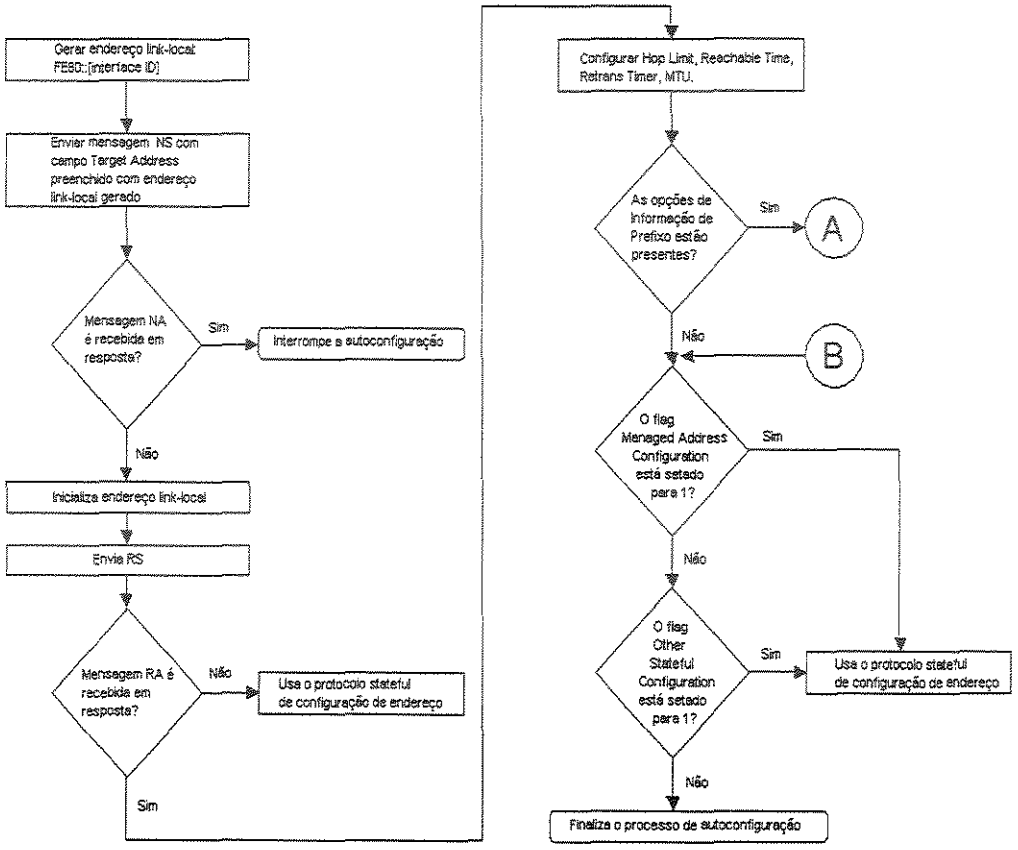


Figura 3.12: Processo de Auto-configuração de Endereço IPv6 para uma Máquina.

cipação e desenvolvimento serão implementados com o objetivo de atualizar e modificar estas políticas. Seus objetivos são:

- Fornecer serviços de registro de endereços IP, ASN, resolução reversa e recursos associados a fim de permitir e facilitar a comunicação através de redes de informação.
- Representar e promover os pontos de vista e os interesses, de sua área de competência, em organizações regionais internacionais.
- Oferecer suporte ao crescimento da Internet na América Latina e no Caribe.
- Oferecer suporte a comunidade latino americana e caribenha no desenvolvimento de procedimentos, mecanismos e padrões com a finalidade de assegurar a atribuição eficiente de recursos da Internet.

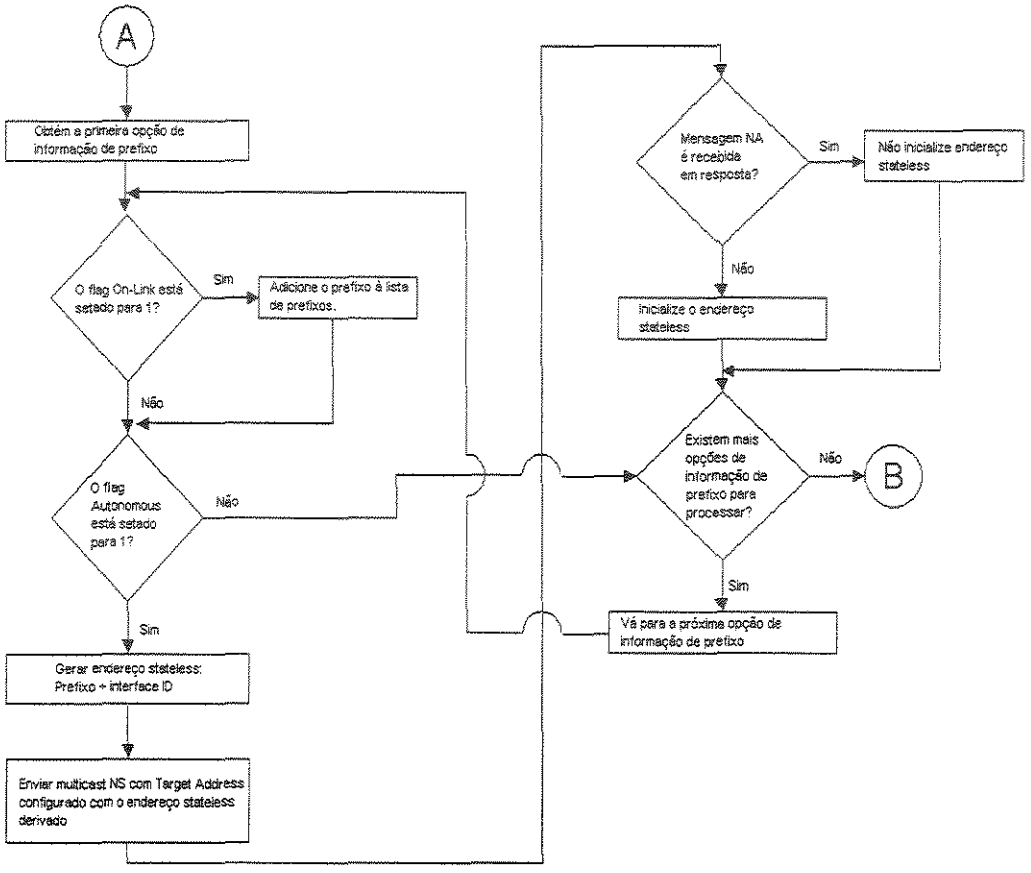


Figura 3.13: Processo de Auto-configuração de Endereço IPv6 para uma Máquina.

- Promover oportunidades educacionais a seus membros em suas áreas de atuação: técnica e política.
- Propor e desenvolver políticas públicas em suas áreas de competência.

A partir de 31 de outubro de 2002, o LACNIC é reconhecida pela IANA como o quarto RIR (Registro Internet Regional). Desde então, o LACNIC opera de forma independente, recebendo e processando as solicitações de recursos Internet de organizações em sua área de cobertura. Os outros RIRs existentes são ARIN [ARI 97] com cobertura na América do Norte, APNIC [APN 93] na Ásia e RIPE-NCC [RIP 97] na Europa. A alocação de endereços IPv6 *unicast* global, feita pela IANA aos RIRs, está no Apêndice B.

3.5.1.1 Políticas e procedimentos da LACNIC

As políticas e os procedimentos baseiam-se nas RFCs relacionadas à administração de IP, números de sistemas autônomos e resolução reversa. As políticas de gerenciamento de recursos da Internet são:

- Políticas de atribuição de IPv4.
- Políticas para atribuição de ASN.
- Políticas de atribuição de IPv6.

Entretanto, interessa-nos aqui somente as políticas de atribuição de endereços IPv6. A LACNIC possui duas políticas para alocação de IPv6. A primeira segue um modelo global e é chamada de Política de Designação e Alocação de endereços IPv6, que também é utilizada pelos outros registros regionais. Segundo esta política, endereços IPv6 são alocados somente para os chamados LIR (*Local Internet Registry*), que seriam os ISPs ou provedores de acesso.

Existe outra política, chamada Política de Micro-Alocação de IPv6, que foi aprovada recentemente e prevê a alocação de blocos IPv6 menores do que previsto na política inicialmente definida, porém somente para as infra-estruturas consideradas críticas para a Internet, como operadores de *root servers*, registros de recursos Internet e pontos de troca de tráfego.

No entanto, nenhuma destas duas políticas prevê designação para usuários finais, ou seja, a LACNIC não tem uma política definida de designação de endereços IPv6 para usuários finais.

Os recursos alocados pelo LACNIC são:

- endereçamento IPv4, para outros países que não seja Brasil e México, pois estes tem seus próprios registros locais;
- endereçamento IPv6;
- ASN.

IPv4	IPv6	ASN
200/8	2001:1200::/23	26592-26623
201/8		27648-28671

Tabela 3.1: Recursos alocados pela LACNIC

3.5.1.2 Acordos de cooperação

A LACNIC firmou importantes acordos com:

- o Comitê Gestor da Internet Brasil [COM 95], organização que administra recursos internet no Brasil. NIC-BR concorda conceder ao LACNIC, sem custo pelo período inicial de dois anos, os recursos de infra-estrutura necessária (equipamentos, locais físicos, comunicações e Recursos Humanos) para começar os trabalhos referentes à administração de números IP, ASN, Resolução Inversa e recursos associados, delegados a LACNIC para América Latina e Caribe e todas as tarefas técnicas relacionadas, como forma de apoio ao inicio da organização.
- o NIC México [NIC 89], organização que administra endereçamento IP e ASN para todo o México. NIC-México e LACNIC concordam que NIC-México será o responsável por coordenar os programas de qualificação, instrução e treinamento que tenha relação com os objetivos do LACNIC, de acordo com as decisões da diretoria, como forma de apoio ao início da organização.

Estes dois acordos têm sido fundamentais para propiciar a estabilidade e viabilidade do LACNIC na sua fase inicial.

3.5.1.3 Serviço de registro IPv6

Os critérios para alocação de endereçamento IPv6 são os seguintes:

- ser um LIR;
- não ser um usuário final;
- objetivar oferecer conexões IPv6 as organizações, para as quais irá designar blocos de prefixo /48;
- ter um plano de ação para fazer, pelo menos, 200 designações de blocos de prefixo /48 a outras organizações no período de 2 anos.

3.5.1.4 LIR no Brasil

Neste momento, o único LIR existente no Brasil é a RNP - Rede Nacional de Pesquisa [RED 89]. Eles designam endereços IPv6 somente para seus clientes, que são aqueles conectados direta-

mente a eles e utilizam suas saídas internet para acesso ao backbone IPv6. A RNP designa 2 faixas de endereço IPv6:

- bloco de teste do 6BONE, que é o 3FFE::/16 [HIN 98a]. O LAS recebeu a seguinte faixa da RNP: 3FFE:2B00:102:100::/64;
- bloco no espaço global *unicast*, que até o final do ano de 2003 era 2001:04A0::/32, obtido com a ARIN. Contudo, este bloco foi devolvido para a ARIN e um novo bloco foi obtido diretamente da LACNIC, que é 2001:12F0::/32.

O Registro.br [REG 03] é responsável pela alocação de endereços IPv4 para organizações no Brasil, pois tem um acordo com a LACNIC para operar como um registro internet local. No entanto, ainda não existe um acordo entre Registro.br e LACNIC para que o primeiro aloque endereços IPv6 a organizações no Brasil. As faixas de endereço IPv4, que são alocadas pelo Registro.br, estão no Apêndice B.

3.5.2 Implementações de IPv6

Existem vários projetos em andamento no mundo, que objetivam prover implementações de pilhas IPv6 e IPSec em plataformas distintas, sendo que muitas destas implementações se tornaram produtos comerciais. Somente algumas serão citadas aqui:

- o Projeto KAME [KAM 98], que é um esforço de seis empresas japonesas, é voltado para sistemas BSD. Por outro lado, o Projeto USAGI [USA 00] é voltado para sistemas Linux;
- a Microsoft [MIC 75], que é voltada para sistemas Windows, provê uma versão da pilha IPv6 e suporte a passagem NAT para aplicativos IPv6, além de um *firewall* IPv6 para proteger a máquina do usuário final contra tráfego IPv6 não solicitado;
- a Apple Computer [APP 03] também disponibilizou um kit de desenvolvimento com IPv6 e IPSec para Mac OS X.

Para obter uma lista mais completa das implementações disponíveis, tanto para máquinas como para roteadores, visite [IPV 02]. Para conhecer as implementações adotadas pelo Laboratório de Administração e Segurança [LAB 04], bem como a configuração utilizada, consultar o Apêndice A.

3.5.3 Projetos de implantação de IPv6

Várias iniciativas, que visam acompanhar a evolução, desenvolvimento e implantação de IPv6 na Internet, estão acontecendo ao redor do mundo. Alguns exemplos de iniciativas são:

- 6REN [PRO 98]: é uma iniciativa americana para promover e encorajar produção de serviços de rede IPv6, objetivando facilitar redes IPv6 de alta qualidade, alto desempenho e operacionalmente robustas;
- 6NET [PRO 02]: é um projeto europeu que objetiva demonstrar que o contínuo crescimento da Internet pode ser acompanhado pela utilização de IPv6;
- 6BONE [PRO 00]: é uma rede de teste IPv6 no mundo.

Para obter uma listagem das iniciativas de implantação disponíveis ao redor do mundo, visite [IPV 99]. Durante a conferência IPv6 *Global Launch Event* organizada pela Comissão Européia em Bruxelas, a Telefônica anunciou que já incorporou IPv6 na sua oferta comercial a empresas e outros operadores, além de estabelecer uma conexão IPv6 entre São Paulo e Madrid. Além disto, operadoras japonesas e coreanas já usam IPv6 em sistemas celular 2,5G e 3G.

3.6 Conclusão

Neste capítulo foram apresentadas algumas características do protocolo IPv6, como o formato de seu cabeçalho, seu espaço de endereçamento e os tipos de endereços existentes. Adicionalmente, foi apresentado o protocolo ICMPv6, o protocolo *Neighbor Discovery* e o processo de Auto-configuração de endereços IPv6. O Registro Internet Regional LACNIC foi explicado, pois é o responsável pelo processo de alocação de endereços IPv6 na América Latina e Caribe. No Capítulo 4 será abordada a questão da segurança nativa provida pelo protocolo IPv6.

Capítulo 4

Segurança em IPv6

Este capítulo apresenta os diversos aspectos relacionados à segurança provida pelo protocolo IPv6, que é disponibilizada de forma nativa. Será abordado o *IP Security* (IPSec), que é uma tentativa para definir uma solução global para o problema de falta de segurança na Internet, assim como será abordado o *Security Neighbor Discovery* (SEND), que é outra tentativa para prover mecanismos de segurança para o protocolo *Neighbor Discovery*.

4.1 O *framework* IPSec - *IP Security*

O *framework* de segurança para o protocolo IP foi formalmente definido e padronizado pelo grupo de trabalho *IP Security Protocol* da IETF na RFC 2401. O IPSec é uma tentativa de habilitar comunicações seguras na camada IP, através da provisão dos seguintes tipos de proteção:

- *integridade sem conexão*: garantia que a mensagem recebida não foi adulterada durante seu trânsito;
- *autenticação da origem dos dados*: garantia da identidade do emissor;
- *proteção contra ataques de replay* (opcional): assegurar que a mesma mensagem não será entregue várias vezes, o que viabiliza ataques que se valem do reenvio de mensagens para ocorrerem;
- *confidencialidade*: impede que o conteúdo da mensagem seja compreensível para qualquer um que a capture, exceto pelo receptor autorizado;

- *proteção contra análise de tráfego* (modo túnel apenas): garante que ninguém conseguirá determinar a identidade das partes envolvidas na comunicação, tampouco a freqüência ou volume de comunicação entre elas;
- *controle de acesso*: o uso de determinados parâmetros de segurança para o estabelecimento de uma comunicação sob a proteção do IPSec está sujeito à concordância com as regras que compõem as políticas de segurança de ambos os extremos.

Os documentos, descrevendo o conjunto de protocolos IPSec, são divididos em sete grupos (Figura 4.1) [THA 98] e descritos na subseção 4.1.1. Assim como, os elementos que compõem o IPSec são descritos na subseção 4.1.2.

4.1.1 Documentos do IPSec

O primeiro documento é o *Architecture* [KEN 98], que amplamente cobre os conceitos gerais, as exigências de segurança, definições e mecanismos definindo a tecnologia IPSec. Os documentos do protocolo ESP e AH cobrem o formato do pacote e as questões gerais relativas aos respectivos protocolos. Também contém valores padrões, tais como conteúdo padrão de *padding* e algoritmos obrigatórios a implementar. O documento *Domain of Interpretation* (DOI) [PIP 98] é parte do mecanismo *IANA Assigned Numbers* e seus valores são bem conhecidos. O conjunto de documentos *Encryption Algorithm* descreve como vários algoritmos de cifragem são usados pelo ESP, exemplo [MADc 98] e [PER 98]. Quando estes ou outros algoritmos de cifragem são usados pelo ESP, o documento DOI deve indicar certos valores, tais como identificador do algoritmo de cifragem, de modo que estes documentos provêem entrada para o DOI. O conjunto de documentos *Authentication Algorithm* descreve os algoritmos de autenticação usados pelos ESP e AH, como o [MAD 98a] e [MAD 98b]. O mesmo acontece com estes ou outros algoritmos quando são usados pelo ESP ou AH, o documento DOI precisa indicar certos valores, como o tipo do algoritmo, de modo que estes documentos provêem entrada para o DOI. Os documentos *Key Management* descrevem os esquemas de gerenciamento de chave dos padrões IETF. Estes documentos também provêem certos valores para o DOI. O documento DOI contém valores necessários para outros documentos se relacionarem entre si, o que inclui algoritmos de cifragem, de autenticação e parâmetros operacionais como tempo de vida das chaves.

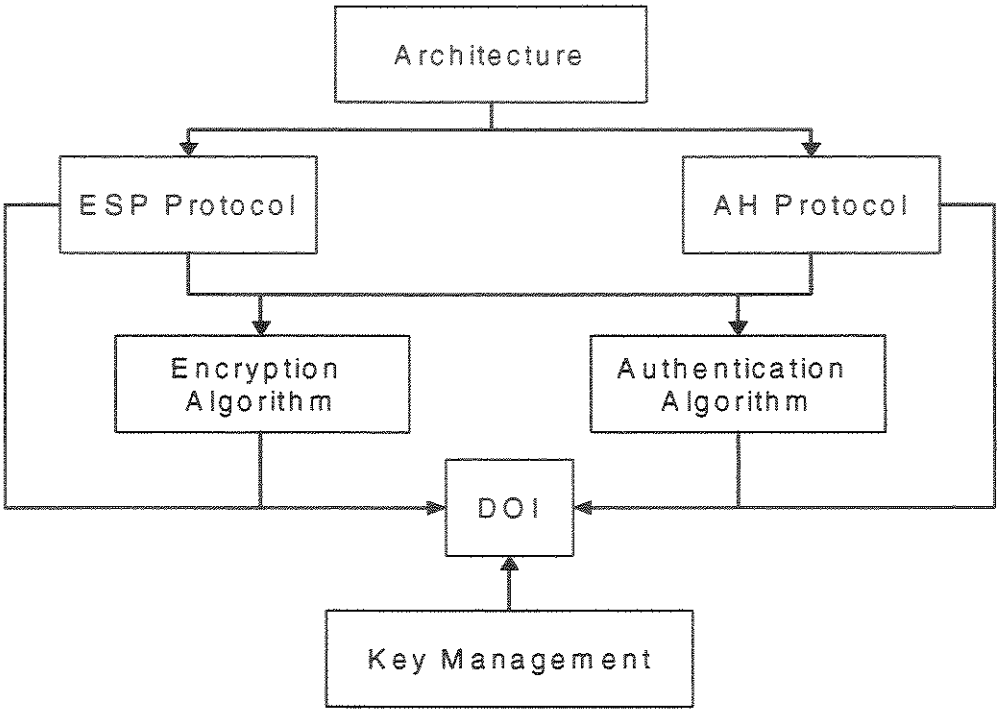


Figura 4.1: Relação entre os Documentos do IPSec.

4.1.2 Elementos do IPSec

O protocolo IPSec é uma adição ao IP, que possibilita o envio e o recebimento de pacotes Internet protegidos criptograficamente. Cabeçalhos especiais IPSec identificam os tipos de proteção criptográficas que serão aplicadas ao pacote e incluem outras informações necessárias à decodificação correta do pacote protegido. O cabeçalho *Encapsulating Security Payload* (ESP) provê privacidade e protege o pacote contra alterações maliciosas, por outro lado, o cabeçalho *Authentication Header* (AH) protege contra alterações maliciosas, sem contudo prover privacidade. Além disso, o protocolo *Internet Key Exchange* (IKE) é um mecanismo que permite a troca de chaves secretas e outros parâmetros relacionados a proteção antes da comunicação propriamente dita entre as partes, sem a intervenção do usuário. As subseções seguintes apresentam os elementos de segurança do *framework* de segurança do IPv6, IPSec, e discute como eles trabalham em conjunto.

4.1.2.1 Associação de Segurança (AS)

Duas entidades em uma comunicação precisam concordar com um conjunto comum de informações, antes que eles possam usar os elementos de segurança de IPv6: quais cabeçalhos de segurança (AH, ESP ou ambos) serão usados, os algoritmos criptográficos a serem usados, as chaves secretas com tamanho e valor, modo de operação (transporte ou túnel), informações para o serviço de proteção contra *replay* e tempo de vida destes parâmetros. Este conjunto de acordos constitui uma Associação de Segurança (AS) entre as duas entidades, pois consiste de todas as informações necessárias para caracterizar e realizar comunicação protegida.

As ASs são unidirecionais, sendo que cada AS é exigida para um tipo específico de proteção: confidencialidade ou autenticação. Deste modo, duas máquinas desejando cifrar e autenticar uma conexão exigem no total quatro ASs, sendo que duas identificam os tipos de proteção exigidas e outras duas identificam os sentidos da proteção durante a comunicação. Logo, é possível que uma troca de pacotes entre duas máquinas tenha parâmetros de proteção distintos em ambos os sentidos, conforme mostra a Figura 4.2, na qual estão alguns possíveis cenários entre duas máquinas.

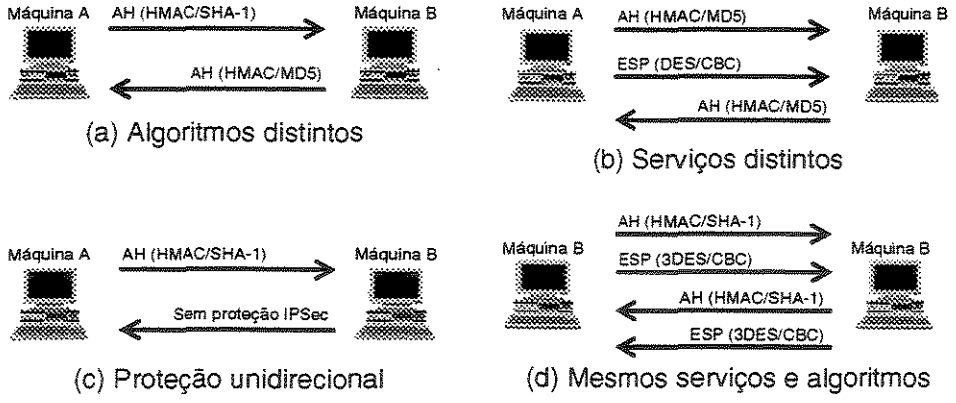


Figura 4.2: Alguns cenários possíveis de ASs entre duas máquinas.

Na Figura 4.2 (a), o tráfego entre as máquinas A e B é protegido pelo cabeçalho AH em ambos os sentidos, no entanto, o algoritmo usado no sentido de A para B é o SHA-1, que é mais seguro que o algoritmo MD5, usado no sentido de B para A. Se tais informações caírem nas mãos de um atacante, ele pode se concentrar em explorar as fraquezas do algoritmo MD5, na tentativa de efetivar algum ataque.

Na Figura 4.2 (b), o tráfego no sentido de A para B está protegido pelos cabeçalhos AH e ESP, contudo, o tráfego no sentido inverso, de B para A, tem somente a proteção do cabeçalho AH, coincidindo o mesmo algoritmo do sentido de A para B. Neste cenário se a confidencialidade é fundamental para a conexão, então o sentido de B para A representa uma falha grave na negociação das ASs, que pode ser facilmente explorada por atacantes.

Na Figura 4.2 (c), somente o tráfego em um dos sentidos, de A para B, está protegido, o que deixa o tráfego do sentido inverso exposto e sujeito a todas as vulnerabilidades conhecidas do protocolo IP.

Na Figura 4.2 (d), o tráfego nos dois sentidos recebe o mesmo tipo de proteção, ou seja, a proteção é aplicada usando os mesmos protocolos e algoritmos, provendo segurança bidirecional ao tráfego. Este cenário é o ideal, já que a proteção foi equilibrada em ambos os sentidos da comunicação.

A máquina destino precisa validar os serviços de um pacote recebido e dar continuidade ao seu processamento através da checagem dos campos que formam a tripla de identificação de cada AS, que precisam estar visíveis. Desta forma, o serviço de confidencialidade do ESP não inclui o SPI, que precisa estar visível.

Cada AS contém vários pedaços de informações que as rotinas de processamento do IPSec podem usar para determinar se uma AS é aplicável a um determinado tipo de tráfego. Estes pedaços, chamados de seletores, incluem:

- *endereços de origem e destino*: podem ser endereços IP únicos (*unicast*, *anycast* ou *multicast*) ou ainda um intervalo de endereços especificado por máscara;
- *nome*: indica o identificador de um usuário ou de um sistema, podendo ser especificado de duas formas: nomes de usuários DNS completamente qualificados ou campo *Distinguished Name* de um certificado X.500;
- *protocolo de transporte*: seleciona o UDP ou TCP;
- *portas de origem e destino*: geralmente é usado para especificar a proteção ao tráfego de um determinado tipo de serviço.

Cada seletor pode ser combinado de acordo com a granularidade desejada em cada AS. Um exemplo de uma AS com uma granularidade grossa pode ser uma AS *host-to-host*, que é uma AS

que se aplica a todo tráfego entre duas máquinas sem levar em conta a aplicação e o usuário. Algumas combinações de seletores são listadas abaixo:

- *orientado à máquina*: quando somente os endereços IP dos pares de uma comunicação são seletores, já que estes seletores governam a comunicação entre os dois sistemas independente de qual usuário ou aplicações estejam envolvidas;
- *orientado à usuário*: quando somente os identificadores de usuários dos pares de uma comunicação são seletores, já que eles governam toda comunicação entre os dois usuários, sem considerar quais sistemas ou aplicações estão envolvidas;
- *orientado à sessão*: quando são utilizados os seletores de portas, origem e/ou destino, em conjunto com o seletor de protocolo de transporte e de endereços IP origem e/ou destino, que protege uma sessão ou instanciação de um tipo particular de tráfego entre duas máquinas específicas.

ASs são administradas em duas bases de dados, chamadas *Security Association Database* (SAD) e *Security Policy Database* (SPD).

O SAD é utilizado para armazenar as ASs ativas de uma máquina num dado momento, ou seja, toda AS estabelecida deve conter uma entrada nesta base de dados, inserida pelo administrador do sistema ou pelo protocolo IKE [HAR 98]. As ASs são identificadas no SAD de cada máquina por triplas compostas dos seguintes valores: endereço de destino, protocolo de segurança e SPI, que é o índice gerado pela máquina destino para identificar uma AS, entre várias que podem estar estabelecidas com a mesma máquina origem para um protocolo específico. Antes de enviar um pacote, o IPSec deve indicar para cada protocolo de segurança utilizado, através desta tripla, a AS que deverá ser utilizada para computar os valores necessários para a composição do cabeçalho correspondente.

O SPD especifica as políticas que determinam a manipulação de todo tráfego IP de um sistema, não apenas de tráfego carregando elementos de cifragem e autenticação. Cada entrada no SPD resulta na criação ou negociação de uma ou mais ASs. Baseado nas características do SPD, para cada pacote IP passando pelo sistema, uma decisão é tomada:

- *descartar o pacote*: certos tipos de tráfego podem ser vistos com inerentemente inseguros e proibidos de serem enviados e recebidos em qualquer situação;
- *aplicar proteção IPSec ao pacote*: exigir que o pacote passe pelo processamento do IPSec;

- *enviar o pacote sem proteção IPSec*: desconsiderar as regras de segurança e permitir a passagem de alguns tipos de pacotes sem aplicar proteção alguma.

A Figura 4.3 mostra um diagrama, que ilustra o processamento de pacotes enviados, em uma plataforma IPSec, bem como a interação existente entre os vários elementos componentes do IPSec.

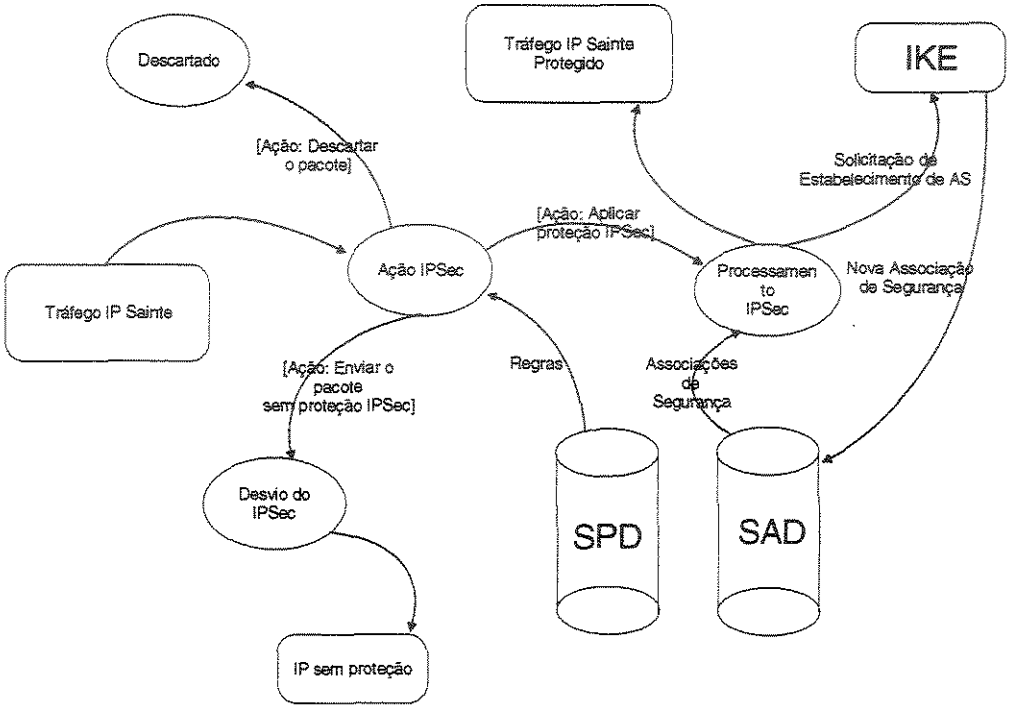


Figura 4.3: Interação entre os vários elementos do IPSec.

Primeiramente, o pacote tráfego IP sainte tem seus campos verificados de acordo com os seletores das regras presentes no SPD, na tentativa de encontrar uma regra que seja compatível. Ocorrendo sucesso na busca da regra, ao pacote será aplicada a ação determinada pela regra do SPD, que será descartar, aplicar proteção ou encaminhar sem proteção. No caso da regra ser aplicar proteção IPSec, as ASs correspondentes à esta regra devem ser recuperadas do SAD para criação e inserção dos cabeçalhos de segurança correspondentes. Contudo, se as ASs necessárias não estiverem no SAD, o protocolo IKE é acionado para que seja dado início ao processo de estabelecimento de novas ASs. Se esta operação ocorrer com sucesso, os parâmetros das ASs cri-

adas são inseridas no SAD pelo IKE, o que permite que o IPSec continue seu processamento. Ocorrendo o inverso, o pacote deve ser descartado. A despeito da especificação determinar que pacotes sem regras associadas sejam descartados, muitas implementações os encaminham para o processamento normal da pilha IP [FRA 01].

Na recepção dos pacotes, o SAD é consultado antes que o SPD. Para cada cabeçalho, AH, ESP ou ambos, presente no pacote, as triplas SPI, endereço de destino e protocolo de transporte são usadas para a recuperação de cada AS com o objetivo de validar e processar os serviços utilizados: autenticação, confidencialidade e/ou integridade. A seguir, é feita uma comparação dos campos do pacote com os seletores que compõem as ASs. Se tais valores forem correspondentes, as ASs usadas na recepção do pacote serão repassadas à segunda etapa do processo de recebimento, onde será verificado se as ASs utilizadas no processamento do pacote estão de acordo com a política de segurança representada pelas regras do SPD. Em caso negativo, o pacote deve ser descartado.

4.1.2.2 Cabeçalho de Autenticação (AH)

Somente autenticação não provê todos os tipos de proteção descritos na seção 5.1, contudo existem aplicações que não precisam de todos os tipos realmente. Por exemplo, informações de roteamento e de *Neighbor Discovery* não são consideradas secretas, porém como uma série de ataques ao sistema de roteamento têm demonstrado, garantir a integridade e a autenticação dos pacotes IP que carregam informações de roteamento é altamente desejável. Adicionalmente, autenticação de pacotes IP provê suficiente prevenção contra ataques populares da Internet, como *IP spoofing*, *DNS spoofing*, *session hijacking* e re-injeção de pacotes (ataques de *replay*) entre outros. Isto ocorre em função da AS estabelecida instruir a implementação do protocolo IP para descartar ou rejeitar todo pacote cujo *checksum* de segurança não possa ser corretamente verificado. Logo, o cabeçalho de Autenticação (*next header* tipo 51) provê integridade e autenticação para toda informação fim-a-fim transportada em um pacote IP.

A Figura 4.4 ilustra o formato do cabeçalho AH, sendo que os cinco primeiros campos têm tamanho fixo, totalizando três palavras de 32-bits e, o sexto campo tem tamanho variável. Segue uma descrição de cada campo:

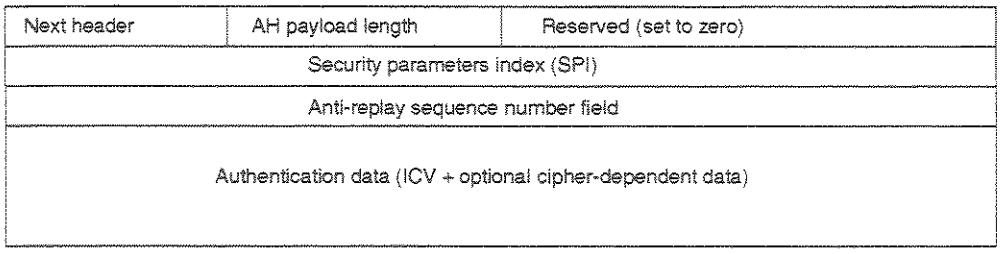


Figura 4.4: Formato do Cabeçalho AH.

- *next header*: identifica o tipo de cabeçalho que vem após o AH, podendo ser outro cabeçalho IPSec (ESP) ou cabeçalhos TCP, UDP, ICMP, IP (se usar o modo de operação túnel) ou cabeçalhos de extensão;
- *payload length*: descreve quantas palavras de 32-bits seguem o campo SPI. A intenção é transmitir o comprimento do dado autenticado, que é um campo variável, para o receptor do pacote. O comprimento do dado autenticado no AH pode diferir dependendo do algoritmo usado;
- *reserved*: é um campo reservado para uso futuro, preenchido com zero;
- *security parameter index (SPI)*: é o índice na base de dados da AS do receptor do pacote e é utilizado para indicar qual algoritmo criptográfico usar;
- *sequence number*: é o número de mensagens enviadas pelo transmissor para o receptor usando a AS atual. Previne ataques de *replay* se o transmissor enviar esta informação para o receptor, o que torna o receptor capaz de realizar esta prevenção, se desejar;
- *autentication data*: é o único campo de tamanho variável. Contém o *Integrity Check Value* (ICV), que é a versão criptográfica do conteúdo da mensagem que pode ser usada pelo receptor para verificar integridade e autenticação da mensagem, e bytes de *padding*, que podem ser inseridos caso seja necessário ajustar o tamanho deste campo aos limites exigidos pelo algoritmo específico, que estiver sendo usado. É um *checksum* seguro criptograficamente gerado a partir da carga útil de dados, de alguns campos do IP e dos cabeçalhos de extensão, concatenado com uma chave secreta negociada entre as partes envolvidas na comunicação, durante o estabelecimento da AS e indexada pelo valor SPI.

O cálculo deste *checksum* seguro criptograficamente, também conhecido como *message digest* ou *hash*, segue as seguintes regras:

- os campos *Version*, *Class* e *Flow label* do cabeçalho IP são excluídos e o campo *Hop limit* é considerado zerado;
- todos os cabeçalhos de extensão, com o bit *change-en-route* setado no *Option Type*, são computados com uma seqüência de bytes zero;
- se o cabeçalho de extensão *Routing* está presente, o valor do campo endereço destino é setado para o endereço do destino final listado no cabeçalho.

O resultado deste cálculo é um *checksum* relativamente curto. Por exemplo, o *checksum* do MD-5 consiste de 128 bits enquanto o *checksum* do SHA-1 consiste de 160 bits. A especificação de IPv6 determina que os algoritmos citados acima, MD-5 e SHA-1, sejam suportados por padrão em cada implementação desenvolvida do IPSec.

Modos AH

Existem dois modos de operação do AH: (1) transporte, que é utilizado para autenticação fim-a-fim entre duas máquinas e (2) túnel, que é usado quando *gateways* de segurança provêem proteção para diversas máquinas na rede. No modo túnel, um cabeçalho adicional externo é colocado no início do pacote com o endereço origem do gateway de segurança, enquanto o cabeçalho interno original tem o endereço origem da máquina interna da rede.

Processamento AH de mensagens saintes

Uma vez determinado que uma mensagem a ser enviada precisa de proteção oferecida pelo AH e a AS referente à comunicação foi encontrada ou negociada, a mensagem é encaminhada para as rotinas de processamento do IPSec, que realizam os seguintes passos:

- insere um molde do cabeçalho AH no local apropriado;
- preenche o campo *Next Header*;
- preenche o campo SPI com o SPI da AS selecionada;
- calcula o campo *Sequence Number*;
- se for uma AS no modo transporte, é preciso alterar o campo *Next Header* do cabeçalho anterior para AH;

- se for uma AS no modo túnel, então o cabeçalho IP adicional externo deve ser construído e adicionado à mensagem. Os endereços origem e destino do cabeçalho externo serão os endereços dos pontos finais do túnel, como especificado pela AS. Além disso, os campos *Version* e *Traffic Class* são copiados do cabeçalho interno para o cabeçalho externo. O campo *Payload Length* é recalculado para o cabeçalho externo, para incorporar o comprimento dos cabeçalhos interno e externo e do AH. O campo *Next Header* é setado para AH ou para o tipo do cabeçalho de extensão que precede o AH. Os próprios cabeçalhos de extensão não são copiados. O *hop limit* é setado para o valor padrão do sistema. Os campos do cabeçalho interno são deixados intactos, com a seguinte exceção: se o endereço origem dos cabeçalhos interno e externo diferirem significa que o pacote interno viajou até chegar ao endereço origem do túnel, o que implica no decremento do campo *Hop Limit*;

- calcular o *authentication data*, que consiste da saída de um *hash* com chave da mensagem. Um algoritmo é usado para obter uma mensagem de qualquer tamanho como entrada e gerar uma saída de tamanho fixo, com a propriedade de ser impraticável modificar a mensagem de qualquer forma que o *hash* resultante da mensagem modificada seja equivalente ao da mensagem original.

- fragmentar a mensagem, se necessário.

Uma observação relevante sobre o cálculo do *authentication data* é que a mensagem completa não é protegida pelo AH, pois o cabeçalho IP pode conter três tipos de dados:

- *dados imutáveis*: que nunca mudam em trânsito;
- *dados mutáveis porém previsíveis*: são dados que podem mudar em trânsito, porém cujo valor final, na chegada ao destino, é previsível;
- *dados mutáveis porém imprevisíveis*: são dados que podem mudar durante o trânsito, porém cujo valor final é imprevisível.

A Figura 4.5 lista os campos do cabeçalho IP em cada uma das três categorias. Apenas os dados da mensagem e os campos do cabeçalho, que não mudam de uma forma imprevisível durante o trânsito, são usados como entrada para o *hash* autenticado, de modo que o receptor do pacote possa verificar o *hash*.

Desta forma, no modo de transporte, os dados da mensagem e os campos previsíveis do cabeçalho IP são protegidos, conforme pode ser observado pela Figura 4.6. No modo túnel, contudo, o cabeçalho original inteiro e os dados da mensagem são protegidos, já que apenas os campos previsíveis do cabeçalho adicionado são protegidos, conforme a Figura 4.7. Logo,

Classes of IP Header Fields

Immutable	Version
	Payload length
	Next header (AH)
	Source address
	Destination address (without routing extension header)
	Destination and hop-by-hop extension headers option type/data length
	Destination and hop-by-hop extension headers option data (option type classified as immutable)
Mutable but Predictable	Destination address (with routing extension header)
	Routing extension header
Mutable Unpredictable	Class
	Flow label
	Hop limit
	Destination and hop-by-hop extension headers: option data (option type classified as mutable)

Figura 4.5: Classes dos Campos IP.

quando um *hash* é calculado, zeros são usados no lugar dos conteúdos não protegidos dos campos do cabeçalho. Uma vez que o *hash* esteja no campo *authentication data*, a mensagem está pronta para ser enviada para seu destino.

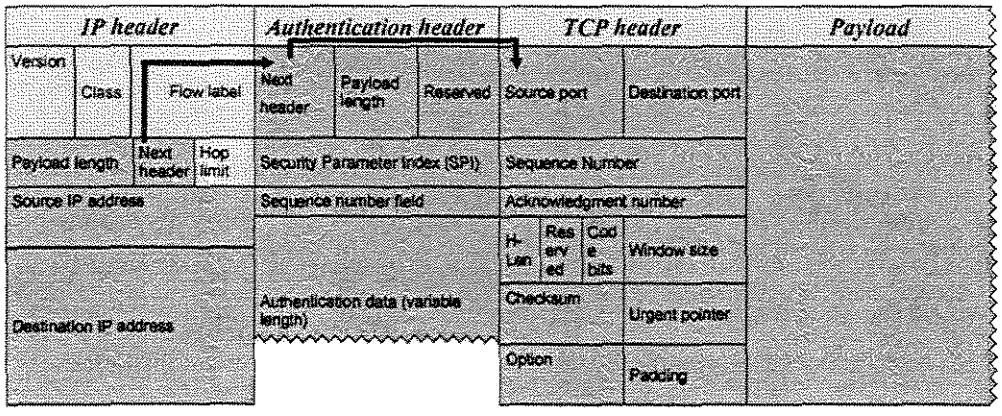


Figura 4.6: Cabeçalho AH no Modo Transporte (campos cinza escuro estão autenticados).

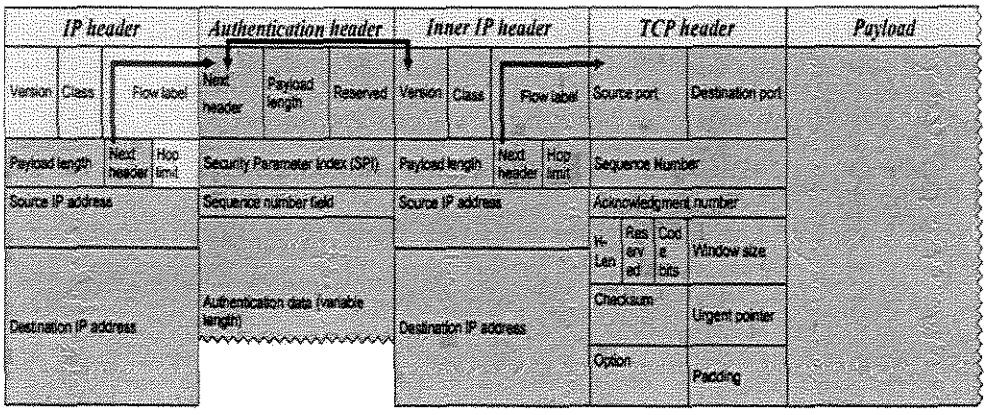


Figura 4.7: Cabeçalho AH no Modo Túnel (campos cinza escuro estão autenticados).

Processamento AH de mensagens entrantes

Quando uma mensagem recebida contém o cabeçalho AH, as rotinas de processamento IP precisam se assegurar que todos os fragmentos da mensagem tenham chegado e reintegrados para formar uma mensagem completa. As rotinas também reiniciam os campos que identificam cada pedaço da mensagem com um fragmento, isto é, o campo *offset* e o flag *"more fragments"* são zerados, de forma que as rotinas não identifiquem erroneamente uma mensagem reintegrada com um fragmento. A mensagem é passada então para as rotinas de processamento do IPSec, que executam os seguintes passos:

- localizar a AS referente a esta comunicação segura no SAD;
- se proteção contra ataques de *replay* é oferecida, é preciso executar a verificação da proteção de *replay*;
- verificar o *authentication data*. O *hash* de autenticação é calculado da mesma forma que foi calculado na origem. Se o cálculo do *hash* não é igual ao encontrado na mensagem, então a mensagem é descartada sem que ocorra nenhum processamento a mais;
- retirar o cabeçalho AH e repetir o processamento IPSec para quaisquer cabeçalhos IPSec restantes.
- verificar o SPD para se assegurar que a proteção IPSec aplicada ao pacote está em conformidade com as políticas exigidas pelo sistema IPSec.

Complicações

A Figura 4.5 mostra que os campos *source address* e *destination address* são considerados imutáveis durante a transmissão, trânsito e recepção do pacote pelos nós que o manipulam. Contudo, a substituição de endereços IPs feita durante o NAT, em razão da rede interna utilizar endereços IP privados, não funcionará com a autenticação no modo de transporte, já que os endereços IP são cobertos pelo *checksum* calculado. Esta questão será abordada no Capítulo 5.

Redução das ameaças

O AH provê vários tipos de proteção na camada de rede. Ele assegura que a mensagem, atravessando a Internet, chegará ao seu destino sem alterações durante o trânsito, que o aparente transmissor da mensagem é o verdadeiro emissor da mensagem e que a mesma não foi errônea ou fraudulentamente retransmitida. No entanto, AH não provê confidencialidade para suas mensagens protegidas, que é função do cabeçalho de segurança ESP, o qual será explicado a seguir.

4.1.2.3 Cabeçalho *Encapsulating Security Payload* (ESP)

O cabeçalho ESP pode ser usado para prover dois conjuntos distintos de proteção, sendo que o primeiro é exclusivo do ESP e o segundo é oferecido também pelo AH. Confidencialidade e proteção contra análise de tráfego são tipos de proteção providos exclusivamente pelo ESP e não pelo AH. Entretanto, integridade sem conexão, autenticação da origem dos dados e proteção contra ataques de *replay* são tipos de proteção providos por ambos os cabeçalhos.

Existe uma distinção entre a autenticação e a integridade providas pelo AH e ESP. No modo de transporte, o AH protege tanto o cabeçalho IP como os dados do pacote, enquanto que o ESP protege apenas os dados do pacote. No modo de túnel, ambos protegem o cabeçalho original, porém apenas o AH protege o cabeçalho externo. Contudo, usar um único cabeçalho para prover múltiplos tipos de proteção reduz tanto o processamento como o tamanho do pacote, o que contribui para aumentar a eficácia e o desempenho da rede. Logo, o ESP é usado para prover confidencialidade e/ou um combinação de integridade sem conexão e autenticação da origem dos dados para as comunicações que são aplicadas. Se confidencialidade é oferecida em modo túnel, proteção contra análise de tráfego pode ser provida também. Finalmente, se integridade e autenticação são providas, então o receptor pode opcionalmente selecionar proteção contra ataques de replay.

Os seletores de ASs são os mesmos para ambos os tipos de cabeçalhos, contudo algumas informações do SAD diferem para entradas AH e entradas ESP em razão do tipo de proteção oferecida ser diferente nos dois cabeçalhos. Três pedaços de informação - SPI, endereço destino e tipo de cabeçalho - são suficientes para identificar com precisão uma AS, de modo que teoricamente o mesmo SPI pode ser usado para identificar uma AS AH e uma AS ESP. Se o cabeçalho ESP é usado para prover confidencialidade, a porção do pacote IP que segue o cabeçalho ESP é cifrada, o que a torna incompreensível para as rotinas de seleção de ASs. Isto significa que os seletores localizados nesta porção do pacote não podem ser usados para distinguir o tráfego protegido ESP. Em particular, o protocolo de transporte (UDP ou TCP) e as portas de origem e destino estão indisponíveis como seletores para pacotes protegidos pelo cabeçalho ESP. Existem outras complicações relacionadas à cifragem dos dados nos protocolos das camadas acima que serão discutidos no Capítulo 5.

A Figura 4.8 ilustra o formato do cabeçalho ESP, constituído de sete campos, sendo que dois campos são opcionais. Segue uma descrição de cada campo:

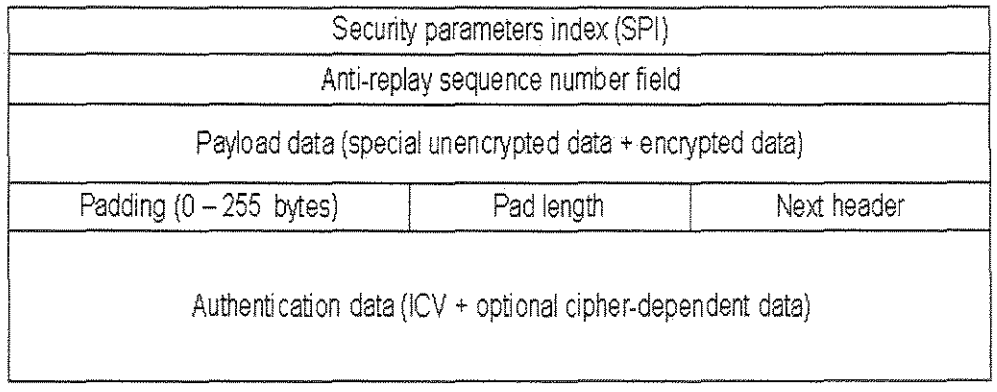


Figura 4.8: Formato do Cabeçalho ESP.

- *SPI*: é o índice na base de dados da AS do receptor do pacote e é utilizado para indicar qual algoritmo criptográfico usar;
- *sequence number*: é o número de mensagens enviadas pelo transmissor para o receptor usando a AS atual. Previne ataques de *replay* se o transmissor enviar esta informação para o receptor, o que torna o receptor capaz de realizar esta prevenção, se desejar;

- *payload data*: se a proteção oferecida para a mensagem for confidencialidade, este campo conterá uma versão cifrada do conteúdo da mensagem, o que substitui a mensagem inicial não cifrada. A parte cifrada também inclui os três campos do cabeçalho ESP seguindo os dados (*padding*, *pad length* e *next header*);
- *padding*: são zeros adicionados ao cabeçalho ESP até alcançar o tamanho desejado;
- *pad length*: número total de bytes de *padding* contido no campo anterior;
- *next header*: identifica o tipo de cabeçalho que segue o ESP, podendo ser cabeçalhos TCP, UDP, ICMP, IP (se usar o modo de operação túnel) ou cabeçalhos de extensão;
- *authentication data*: um campo opcional de tamanho variável que contém o ICV, se a mensagem receber proteção de autenticação e integridade.

O cabeçalho ESP consiste de quatro partes distintas:

- o cabeçalho inicial ESP consiste dos campos SPI e *sequence number*;
- a porção de dados consiste de dados especiais não cifrados (se existir), de quaisquer cabeçalhos de extensão que venham após o ESP, dos cabeçalhos TCP ou UDP e dos dados da mensagem;
- o ESP *trailer* consiste do *padding* (se existir) e dos campos *Pad Length* e *Next Header*;
- o ESP *authentication data* consiste do campo *authentication data* (se existir).

Modos ESP

O cabeçalho ESP também pode ser usado tanto em modo transporte como em modo túnel. No modo transporte, o cabeçalho IP e os cabeçalhos de extensão, até o cabeçalho ESP, não são cifrados e, portanto, não protegidos (Figura 4.9). Cifrar estes cabeçalhos pode tornar todo o mecanismo de roteamento inútil, já que roteadores podem precisar ver, processar e mesmo modificar estes cabeçalhos enquanto o pacote está em trânsito. Desta forma, se cifrar todo o pacote for uma exigência, um túnel deve ser criado empacotando todo o pacote original em um pacote IP externo, cujo conteúdo não é protegido pela cifragem (Figura 4.10).

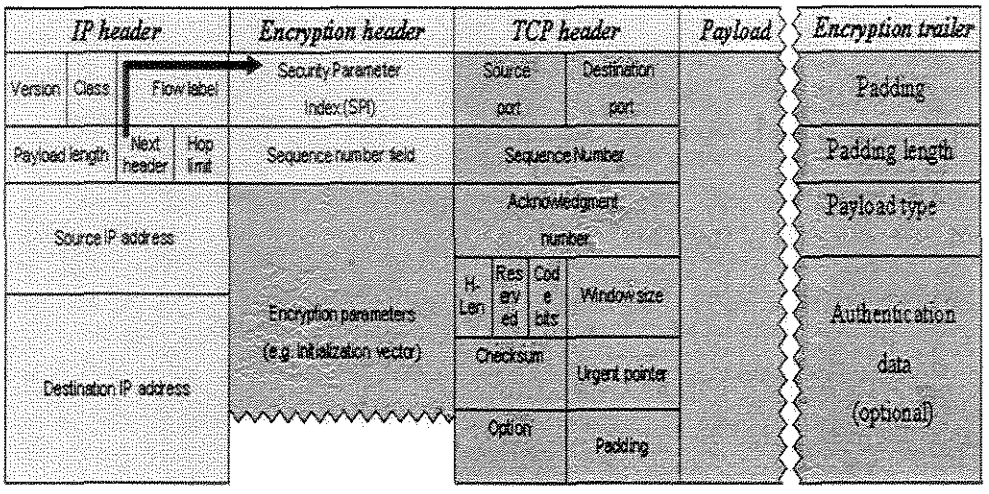


Figura 4.9: Cabeçalho AH no Modo Túnel (campos cinza escuro estão autenticados).

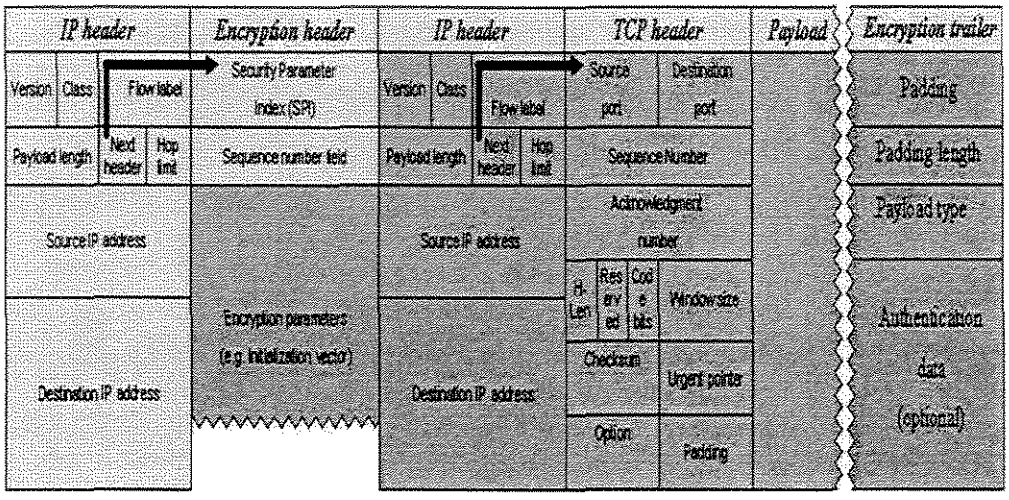


Figura 4.10: Cabeçalho AH no Modo Túnel (campos cinza escuro estão autenticados).

Nenhum ou vários cabeçalhos de extensão (*hop-by-hop*, *routing*, *fragment* ou *destination options*) podem vir antes do cabeçalho ESP, além disto o cabeçalho *destination options* pode seguir o cabeçalho ESP. A posição do cabeçalho *destination options* em relação ao ESP depende do momento de seu processamento, se deverá ocorrer antes ou depois do processamento do ESP. Se o pacote está cifrado, o cabeçalho *destination options* que vier após o ESP não poderá

ser visto por nenhum roteador intermediário e somente será visível após o processamento de decifragem do ESP no destino final.

Processamento ESP de mensagens saintes

Uma vez determinado que uma mensagem precisa da proteção oferecida pelo cabeçalho ESP e a AS que governa está comunicação foi encontrada ou negociada, a mensagem é encaminhada para as rotinas de processamento IPSec, que realizam os seguintes passos:

- insere o molde inicial do cabeçalho ESP no local apropriado;
- preenche o campo SPI com a informação encontrada na AS associada;
- calcula o campo *Sequence Number*;
- se a proteção escolhida for cifragem e os algoritmos de cifragem exigem que dados adicionais especiais não sejam cifrados, então estes dados devem ser adicionados ao cabeçalho. O vetor de inicialização é colocado não cifrado no pacote, de modo que o receptor possa decifrar apropriadamente a mensagem;
- se exigido, adicionar um cabeçalho de túnel;
- anexa os dados restantes do pacote;
- calcula o comprimento de qualquer *padding* (enchimento) exigido e preenche o pacote com o número requisitado de bytes de dados. O conteúdo do *padding* deve ser especificado pelo algoritmo criptográfico ou, se tal especificação não existir, o *padding* deve conter uma série de inteiros com os valores 1, 2, 3, ...
- preencher o campo *Next Header*;
- cifrar a mensagem, se for a proteção escolhida. Os campos de dados, *padding*, *pad length* e *next header* são cifrados. Os algoritmos de cifragem mandatórios para o ESP são DES-CBC e o algoritmo nulo.
- calcula o dado autenticado, se autenticação for especificada pela AS. O processo de autenticação se aplica sobre o cabeçalho ESP inicial e os dados cifrados;
- fragmentar a mensagem, se necessário.

Processamento ESP de mensagens entrantes

Quando uma mensagem, que contém o cabeçalho ESP, é recebida, as rotinas de processamento do IPSec se asseguram que todos os fragmentos da mensagem foram recebidos e reintegrados para formar a mensagem completa. As rotinas também se asseguram que os campos, que identificam cada pedaço da mensagem como um fragmento, sejam reiniciados: o campo *offset* e o flag "*more fragments*" são zerados, de modo que as rotinas de processamento do IPSec não identifiquem de forma errônea a mensagem remontada como sendo um fragmento. Finalmente, as rotinas do IPSec executam os passos seguintes com a mensagem:

- localiza a AS referente à comunicação protegida na base de dados SAD;
- se a proteção contra ataques de *replay* está habilitada, efetua a verificação desta proteção;
- verifica a autenticação dos dados da mensagem. O *hash* é calculado da mesma forma que para uma mensagem sainte. Se o cálculo do *hash* não é igual ao encontrado na mensagem, então a mesma é descartada e não acontece nenhum processamento adicional. É interessante notar que efetuar a verificação de autenticação da mensagem antes da cifragem é eficiente, pois se a mensagem foi alterada não é necessário realizar o processo computacionalmente caro de decifragem dos dados;
- decifrar a porção cifrada do pacote, contudo se a decifragem não ocorrer com sucesso, a mensagem é descartada e não acontece processamento adicional;
- retira o *padding*, se algum foi adicionado;
- retira o cabeçalho ESP e repete o processamento IPSec para quaisquer cabeçalhos IPSec restantes;
- checar o SPD para se assegurar que a proteção aplicada ao pacote entrante se enquadra nas exigências das políticas do sistema IPSec.

Complicações

Embora a cifragem dos cabeçalhos das camadas superiores seja desejável para finalidade de segurança, ela impede campos dos cabeçalhos de transporte, como as portas, de serem seletores de ASs. Também apresenta problemas para usos especializados do tráfego Internet. Um número de campos do cabeçalho de transporte podem ser usados para outros fins que não somente o processamento pela camada de transporte, tais como análise de tráfego, gerenciamento e melho-

ramento do desempenho da rede, detecção a intrusão, filtragem de pacotes, tratamento preferencial para tipos específicos de tráfego, resultando em várias classes de qualidade de serviço (QoS). Existem dois possíveis enfoques: (1) definir um cabeçalho especial, que duplique os campos críticos sem cifragem ou (2) começar a cifragem em um ponto tardio do pacote, deixando os campos desejados dos cabeçalhos sem cifragem. A desvantagem da primeira solução é a possibilidade da segurança ser comprometida, pela provisão de informação não cifrada para potenciais atacantes que também estão cifradas em locais bem conhecidos no pacote. Outro problema é a duplicação da informação, o que resulta no aumento do tamanho do cabeçalho. A segunda solução pode complicar um protocolo já complexo, exigindo processamento especializado adicional.

4.1.2.4 Algoritmos criptográficos obrigatórios

O ESP e o AH provêem mecanismos para proteger os dados enviados sobre uma AS IPSec. Para assegurar a interoperabilidade entre implementações distintas, é necessário especificar um conjunto obrigatório de algoritmos para assegurar que no mínimo um algoritmo estará disponível em todas as implementações. O conjunto básico de algoritmos é:

- HMAC-MD5-96 [MAD 98a] e HMAC-SHA-1-96 [MAD 98b]: algoritmos de autenticação e integridade utilizados pelo AH e, opcionalmente, pelo ESP. Contudo, o *draft* [EAS 04] propõe a utilização do AES-XCBC-MAC-96 [FRA 03a] e do HMAC-SHA1-96;
- DES-CBC [MAD 98c]: algoritmo de cifragem utilizado pelo ESP. O *draft* [EAS 04] propõe a utilização do AES-CBC com chaves de 128 bits [FRA 03b] e do AES-CTR [HOU 03];
- algoritmos nulos de autenticação e cifragem [GLE 98] utilizados pelo ESP.

Considerando que os serviços de autenticação e cifragem do ESP são opcionais, o suporte aos algoritmos nulos é uma exigência para manter a consistência com o modo de negociação destes serviços. Entretanto, os dois serviços não podem ser nulos ao mesmo tempo, já que o ESP deve prover pelo menos um dos seus serviços quando presente na proteção de pacotes. Para saber mais detalhes sobre os vários algoritmos utilizados pelo IPSec, consulte [SEN 02].

4.1.2.5 *Internet Key Exchange* (IKE)

O estabelecimento de ASs baseia-se na existência de chaves secretas conhecidas somente pelos membros da associação. A implementação de segurança depende de um método eficiente de distribuição de chaves, que pode ser manual ou automático. No método manual, o administrador do sistema configura manualmente cada sistema com suas chaves, além de acrescentar as chaves de outras partes integrantes de uma comunicação futura. Contudo, isto é adequado somente para uma quantidade pequena de sistemas. No método automático, a troca de chaves para ASs é sob demanda e sem intervenção humana, o que facilita a utilização de chaves em um sistema distribuído e amplo.

Para estabelecer uma AS entre partes de uma comunicação, as partes precisam primeiro concordar com uma política de segurança comum e um conjunto compatível de algoritmos criptográficos. Para facilitar a troca segura destas informações, elas precisam concordar numa chave ou num segredo compartilhado, que pode ser negociada sobre um meio potencialmente inseguro ou que deve ser baseada em certificados autenticados, através de infra-estrutura de chave pública confiável ou distribuição e verificação de certificados por outros meios.

O *Internet Key Exchange* (IKE) [HAR 98] descreve um protocolo que permite que partes de uma comunicação obtenham material autenticado e gerenciem ASs para o uso de serviços AH e ESP do IPSec de forma segura. O IKE é considerado um protocolo da camada de aplicação do ponto de vista do IPSec e roda na porta 500/UDP. Logo, outros *frameworks* de gerenciamento de chave, além do padrão IKE, podem ser utilizados.

IKE é uma adaptação seletiva de três protocolos mais gerais, descritos a seguir:

- o *Internet Security Association and Key Management Protocol* (ISAKMP) [MAU 98] provê uma estrutura geral para manipulação das ASs e troca de chave;
- o protocolo de determinação de chave *Oakley* [ORM 98] é baseado no Diffie/Hellman. Ele descreve uma série de trocas de chave, chamadas de *modes*, e especifica os serviços providos por cada tipo de chave trocada, tais como proteção de identidade, autenticação e encaminhamento perfeito de chaves secretas (*Perfect Forward Secrecy* - PFS), de modo que mesmo que uma chave seja comprometida chaves posteriores ou dados cifrados não serão prejudicados. IKE não precisa do protocolo Oakley completo, somente de um subconjunto necessário para satisfazer seus objetivos específicos;

- o *Versatile Secure Key Exchange Mechanism for Internet* (SKEME) [KRA 96] descreve uma técnica rápida de troca de chaves que provê anonimato, repúdio e substituição rápida de chave. O IKE também não precisa do protocolo SKEME completo, apenas do método de cifragem de chave pública para autenticação e o conceito de rechaveamento rápido usando uma troca de *tokens* especiais, chamados *nonces*. *Nonces* são números aleatórios usados para adicionar aleatoriedade ao processo de negociação de chave e que provêem proteção limitada contra ataques de *replay*.

Neste momento, é possível definir o IKE como sendo um protocolo de negociação que se utiliza de formatos de dados definidos no ISAKMP para trocar chaves e informações de AS baseadas nos mecanismos de troca de chave Oakley e SKEME.

Funcionamento do IKE

O objetivo de qualquer implementação do IKE é negociar ASs IPSec com pares de uma comunicação, o que é obtido em uma negociação de duas fases. Vale ressaltar que o Oalkley define "modos" e o ISAKMP define "fases". O IKE opera em duas fases:

1. fase 1: estabelece uma AS ISAKMP, que é um canal seguro através do qual a negociação da AS IPSec pode ocorrer. Os diferentes modos de estabelecimento da AS ISAKMP são: *Main Mode*, *Aggressive Mode* ou *Base Mode*. Cada modo é definido como uma série de mensagens, que são trocadas entre o *initiator*, quem envia a primeira mensagem de estabelecimento de uma AS, e o *responder*, quem recebe a mensagem enviada pelo initiator. O *main mode* é uma troca normal, que usa seis mensagens e provê proteção de identidade. O *aggressive mode* usa apenas três mensagens, porém não oferece proteção de identidade. O *base mode* utiliza-se de quatro mensagens e objetiva ser um meio termo entre a segurança do primeiro modo e a eficiência do segundo;

2. fase 2: negocia ASs sobre um canal seguro em benefício do IPSec ou de quaisquer outros serviços, usando *Quick Mode*, que é o método padrão da fase 2 e que usa somente três mensagens. Uma AS ISAKMP é sempre considerada bidirecional após sua conexão, de modo que cada par da comunicação pode iniciar trocas *Quick Mode* a qualquer tempo.

Em uma negociação IKE, é imprescindível que cada participante prove sua identidade para a outra parte. Este processo é chamado de autenticação de pares. Se a identidade dos pares está

em dúvida ou pode ser falsificada, então o processo completo de negociação de AS é sem valor, pois um atacante pode se identificar como sendo um dos pares e conseguir estabelecer uma AS, de modo que estará recebendo o tráfego protegido, quando o tráfego deveria estar sendo protegido dele. Os métodos de autenticação de pares, que podem ser usados no IKE, são:

- segredo pré-compartilhado: os pares usam este segredo para gerar chaves simétricas, que são usadas para cifrar e autenticar mensagens IKE. A cifragem e a decifragem correta das mensagens IKE serve como prova da posse do segredo, que é a única prova de identidade. A troca deste segredo é feita pelo administrador, que deverá inseri-lo manualmente nos sistemas envolvidos na comunicação. Sua grande falha é a ausência de um método escalável e seguro de troca do segredo compartilhado. É útil em ambientes de escala pequena com um número moderado de sistemas, no qual os pares se conhecem antecipadamente. Contudo, se um segredo pré-compartilhado é comprometido, não existe método automático de notificar os pares e estabelecer novo segredo;
- assinaturas digitais ou cifragem com chave pública: estes métodos exigem que cada participante tenha um par de chaves pública e privada. Cada par usa sua chave privada para assinar mensagens a enviar e decifrar mensagens recebidas, enquanto o outro par usa a chave pública correspondente para verificar a identidade das mensagens recebidas e cifrar mensagens a enviar, desta forma a identidade dos pares é provada. Se as chaves públicas são recuperáveis de um repositório seguro, então elas pode ser rapidamente acessadas e atualizadas.

A fase 1 da negociação tem três objetivos:

- negociar parâmetros de segurança: o initiator e o responder devem concordar com valores e características de um número de parâmetros, que governarão o formato das duas últimas mensagens cifradas da fase 1 e de todas as mensagens da fase 2. Além disso, devem negociar qual método os pares usarão para autenticar suas identidades; o tempo de vida máximo da AS da fase 1 e como será mensurado; o método usado para estabelecer o segredo compartilhado que será usado para calcular as chaves secretas e os parâmetros usados para gerar o segredo compartilhado. Todos estes valores coletivamente formam a AS ISAKMP;
- estabelecer um segredo compartilhado: uma troca de mensagens é utilizada para estabelecer o segredo compartilhado, que será usado na geração das chaves secretas;
- autenticar os participantes da comunicação: os pares autenticam suas identidades.

Quando a negociação da fase 1 estiver completa, uma AS ISAKMP, que é um canal protegido, estará estabelecido entre os pares. Esta AS consiste de políticas acordadas e de parâmetros para negociações posteriores, além de chaves secretas simétricas que serão usadas para autenticar e cifrar estas negociações. Ambos os pares podem iniciar negociações posteriores, nas quais a AS ISAKMP é usada para proteger negociações de AS IPSec, que podem ser utilizadas para proteger comunicação IP entre pares em geral. A fase 2 da negociação tem três objetivos:

- negociar parâmetros de segurança: o initiator e o responder devem concordar com valores e características de um número de parâmetros, que governarão a operação da AS IPSec negociada. Além disso, devem negociar o tempo de vida máximo da AS e como será mensurado. Se PFS (*Perfect Forward Secrecy*)[1], que é a garantia da geração de apenas uma chave pela troca Diffie-Hellman e que não tem relação com quaisquer outras chaves usadas entre os pares, é desejado, então eles precisam comunicar os parâmetros usados para gerar o segredo compartilhado, que será usado para calcular o "*keying material*";
- prevenir ataques de *replay*: *hashes* autenticados são trocados e verificados para assegurar que a negociação não é simplesmente o reenvio de uma mensagem envolvida em uma negociação de fase 2 anterior;
- gerar "*keying material*": usando o segredo compartilhado da fase 1, o "*keying material*" para a AS IPSec é gerado.

4.2 Protocolo SEND

O protocolo *Neighbor Discovery* (NDP) [NAR 98] combina o protocolo de resolução de endereços IP em endereços MAC (ARP em IPv4) e mensagens de ICMP para descoberta de roteador (*router discovery*) e redirecionamento (*Redirect*). Além de ser importante no mecanismo de auto-configuração de máquinas IPv6 na rede, já que estas máquinas podem obter informações necessárias para sua configuração IP, usando suas mensagens e sem a necessidade de intervenção direta do administrador. As mensagens do NDP são mensagens ICMPv6, que não usam nenhum tipo de proteção IPSec, o que constitui uma grande vulnerabilidade do sistema de roteamento e auto-configuração na rede IPv6.

---

1. objetiva evitar que o comprometimento do segredo compartilhado de uma AS ISAKMP resulte na fragilização das chaves geradas para as ASs IPSec resultantes.

O protocolo *Neighbor Discovery* (NDP) é sujeito a ataques que podem redirecionar o fluxo dos pacotes IP para lugares inesperados. Tais ataques podem provocar negação de serviço, assim como permitir que um nó da rede intercepte e, opcionalmente, modifique pacotes destinados a outros nós. Um atacante pode alterar rotas, através do envio de mensagens falsas de anúncio de roteadores, fazendo com que todo tráfego dos outros nós passe por ele, além de poder provocar negação de serviço. Ataques de *spoofing* em resolução de endereços podem ser facilmente implementados, a exemplo dos ataques de ARP *spoofing* [CAR 03].

Adicionalmente, o protocolo não possui mecanismos para determinar quais vizinhos são autorizados a enviar um tipo particular de mensagem, por exemplo *Router Advertisements (RA)*. Deste modo, qualquer vizinho pode enviar mensagens de RA, sendo capaz de alterar rotas e, conseqüentemente, negar serviço. No entanto, a especificação do protocolo NDP, em suas considerações de segurança, diz que a troca de pacotes do NDP *podem* ser autenticadas usando o cabeçalho de autenticação (AH), sem detalhar as instruções de como usar o IPSec para proteger NDP.

Portanto, as várias máquinas na rede podem criar ASs com os roteadores, de modo, que possam se utilizar das proteções IPSec durante o processo de inicialização, para garantir integridade e autenticidade das mensagens de auto-configuração. No entanto, surge o problema "do ovo e da galinha" usando o IKE [HAR 98] [ARK 02a], pois neste caso o IPSec pode ser usado somente com a configuração manual das ASs, já que o IKE deveria ser utilizado após a configuração das máquinas pelo NDP e não no estabelecimento de chave a ser usada no NDP (Figura 4.11). A configuração manual torna-se um problema adicional, pois vai contra o princípio básico do NDP, que é permitir a configuração automática, além de não ser uma solução escalável, já que o número de ASs configuradas manualmente necessárias para proteger o NDP pode ser alto [ARK 02b].

Na tentativa de resolver os problemas de segurança e evitar a configuração manual do NDP, o IETF criou o grupo de trabalho chamado *Securing Neighbor Discovery* (SEND), cujo objetivo é definir suporte à segurança no NDP, sem contudo exigir configuração manual. Esse grupo de trabalho publicou três *drafts* até o momento: *SEcure Neighbor Discovery* [ARK 04], *Cryptographically Generated addresses* [AUR 03] e *IPv6 Neighbor Discovery trust models and threats* [NIK 03]. Para proteger as várias funções do NDP, um conjunto de novas opções ND são criadas. A solução proposta contém estes componentes:

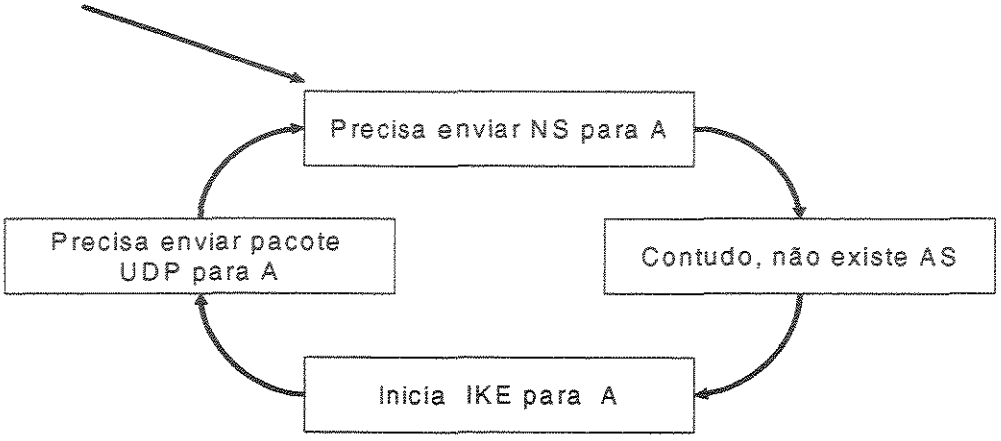


Figura 4.11: Caracterização do problema do "Ovo e da Galinha" com IKE e NDP.

- Cadeias de certificados, apoiados em partes confiáveis, são esperados para certificar a autoridade dos roteadores. Uma máquina e um roteador precisam ter no mínimo uma parte confiável em comum antes que a máquina possa adotá-lo como seu roteador padrão. Mensagens de *Delegation Chain Solicitation* e *Advertisement* são usadas para descobrir uma cadeia de certificados da parte confiável;

- endereços gerados criptograficamente (*Cryptographically Generated Addresses* - CGA) são usados para assegurar que o transmissor de uma NA (*Neighbor Advertisement*) ou RA (*Router Advertisement*) é o dono do endereço reclamado. Um par de chaves pública e privada são necessários em todos os nós, antes que eles reclamem um endereço. A idéia básica é gerar o identificador de interface do endereço IPv6 calculando um *hash* criptográfico da chave pública. O endereço IPv6 resultante é chamado de CGA. Uma nova opção do NDP, chamada opção CGA, é usada para carregar a chave pública e os parâmetros associados;

- uma nova opção NDP, chamada opção *Signature*, é usada para proteger todas as mensagens relativas ao ND (*Neighbor Discovery*) e ao RD (*Router Discovery*). Assinaturas de chave pública são usadas para proteger a integridade das mensagens e para autenticar a identidade dos seus transmissores. A autoridade de uma chave pública é estabelecida tanto pelo processo de delegação de autorização, usando certificados, ou através do mecanismo de prova da propriedade do endereço, usando CGAs. Este estabelecimento depende da configuração e do tipo de mensagem a ser protegida;

- para prevenir ataques de *replay*, duas novas opções do ND são usadas, chamadas *Timestamp* e *Nonce*. Dados que as mensagens RD e ND são enviadas em alguns casos para endereços *multicast*, a opção *Timestamp* oferece proteção *anti-replay* sem qualquer estado estabelecido anteriormente ou números de seqüência. Quando as mensagens são usadas no par *Solicitation - Adversisement*, elas são protegidas usando a opção *Nonce*.

Apenas algumas mensagens do protocolo NDP usam a opção CGA obrigatoriamente, que são as NS (*Neighbor Solicitation*) e NA, além das mensagens de RS enviadas com endereço diferente do *unspecified*. Os outros tipos de mensagens NDP *podem* fazer uso da opção CGA. Se na recepção de qualquer uma destas mensagens, elas estiverem sem a opção CGA, então elas devem ser descartadas.

As mensagens NS, NA, RA e *Redirect* usam a opção *Signature* obrigatoriamente, assim como as mensagens RS enviadas com endereço diferente do *unspecified*. As mensagens recebidas sem esta opção devem ser descartadas.

4.2.1 Funcionamento básico

Vários protocolos, NDP inclusive, permitem que um nó se auto-configure baseado na informação aprendida de sua breve conexão no enlace. É particularmente fácil configurar roteadores num enlace inseguro, porém é particularmente difícil para um nó distiguir entre origens válidas e inválidas da informação, quando um nó precisa desta informação antes de ser capaz de se comunicar com os nós fora do enlace. Considerando que os nós conectados a pouco não podem se comunicar fora do enlace, eles não podem ser responsáveis por pesquisar informação que os ajude a validar os roteadores, contudo, com uma cadeia de certificados assinados apropriadamente, eles podem checar o resultado da pesquisa de algum outro nó e concluir que uma mensagem particular vem de uma fonte autorizada. No caso típico, um roteador, que já se comunica além do enlace, pode, se necessário, comunicar com nós fora do enlace e construir tal cadeia de certificados. O SEND cria duas novas mensagens ICMPv6, chamadas *Delegation Chain Solicitation* (DCS) e *Advertisement* (DCA), que são usadas entre roteadores e máquinas para permitir às máquinas aprender uma cadeia de certificados com o auxílio de um roteador.

Os roteadores precisam de um par de chaves e de um certificado de no mínimo uma autoridade certificadora. O roteador obrigatoriamente descarta qualquer DCS recebida e que não satisfaça todas as checagens de validade [ARK 04]. Uma solicitação que passou pela checagem de

validade é considerada uma *solicitação válida*. Se o endereço origem da solicitação é o endereço *unspecified*, o roteador envia a resposta para o endereço *multicast link-scoped all-nodes*. Se o endereço origem for um endereço *unicast*, o roteador envia a resposta para o endereço *multicast solicited-node* correspondente ao endereço origem. Na resposta, o roteador inclui as opções de certificado apropriadas, de modo que a cadeia de delegação para aquela autoridade certificadora possa ser estabelecida. Se o roteador não encontrar a cadeia para a autoridade certificadora pedida, ele deve enviar a resposta sem nenhum certificado e com a autoridade solicitada. Os roteadores de tempos em tempos enviam uma mensagem DCA para o grupo *multicast all-nodes*, que carrega pelo menos uma autoridade certificadora, no qual algum certificado seja baseado.

As máquinas precisam da chave pública, do nome e de um certificado de no mínimo uma autoridade certificadora, para que possam ser capazes de verificar as assinaturas de certificados de outras máquinas ou roteadores no enlace assinados pela autoridade certificadora. Além disso, elas têm seus próprios pares de chaves, que podem ser assinadas ou não pela mesma autoridade certificadora. Assim como os roteadores fazem testes de sanidade nas mensagens de solicitação recebidas, as máquinas também precisam fazer estes testes em mensagens recebidas de roteadores no enlace [ARK 04]. As máquinas armazenam cadeias de certificados recuperados das mensagens de *Delegation Chain Discovery*, com o objetivo de validarem mensagens RA. Quando estiver solicitando certificados para um roteador, a máquina envia uma mensagem DCS para o endereço *multicast all-routers*, se um roteador padrão ainda não foi escolhido, ou para o endereço IP do roteador padrão, quando o mesmo já foi selecionado.

No entanto, proteger o protocolo NDP com o SEND assegura que um roteador ou nó vizinho pertence ao conjunto de entidades confiáveis, sem contudo assegurar que este roteador não seja um atacante fazendo *spoofing* de outro roteador legítimo. Este é um problema sem solução proposta até o momento.

4.3 Conclusão

Este capítulo apresentou os aspectos relacionados à segurança provida pelo protocolo IPv6, através do seu *framework* de segurança IPSec e do mecanismo de segurança SEND. Os protocolos, que compõem o IPSec, são adições ao IP, que possibilitam o envio e o recebimento de datagramas IP protegidos criptograficamente. Por outro lado, a integridade da rede estará comprometida se os protocolos de roteamento não forem protegidos, o que possibilita ataques de negação de

serviço e alteração de rotas. O mecanismo SEND é proposto para resolver esta fragilidade do protocolo *Neighbor Discovery* e não faz uso do IPSec, como visto na Seção 4.2. As complicações da criptografia fim-a-fim também foram somente enunciadas, contudo serão abordadas de forma mais completa no Capítulo 5.

Capítulo 5

IPv6 e Ambientes Cooperativos Seguros

O objetivo deste capítulo é discutir as implicações da adoção de IPv6 em Ambientes Cooperativos Seguros, implementados com ferramentas de segurança já consolidadas em IPv4. Desta forma, na Seção 5.1 será apresentado um Ambiente Cooperativo Seguro em IPv4, além dos problemas advindos da integração de IPv6 e de seu *framework* de segurança IPSec com as várias ferramentas presentes neste cenário. Na Seção 5.2, são apresentados os possíveis cenários resultantes da adoção de IPv6/IPSec.

5.1 Integração de IPv6 em um Ambiente Cooperativo Seguro

5.1.1 Ambiente Cooperativo Seguro em IPv4

Com o aumento da pervasidade das redes de computadores e equipamentos de comunicação, notadamente através da expansão da Internet, os mecanismos de segurança de redes tiveram de evoluir para adaptar-se aos cenários emergentes. Assim, aos tradicionais *firewalls*, baseados em filtragem de pacotes, incorporam-se outras técnicas como a tradução de endereços de rede (NAT - *Network Address Translation*), *proxies* que verificam o tráfego no nível da aplicação, o uso de Redes Privadas Virtuais (VPNs), a implantação de uma Infra-estrutura de Chave Pública (PKI) e o monitoramento através de Sistemas de Detecção a Intrusões (IDS). Esta complexa configuração de diversos tipos de mecanismos de segurança pode ser denominada de *firewall cooperativo*, podendo também ser definida como um conjunto diverso de *software* e *hardware* que colabo-

ram para aplicar uma determinada política de segurança, seguindo a definição clássica de Bellovin [BEL 99]. O *firewall cooperativo*, mostrado na Figura 5.1 apresenta uma arquitetura que inclui todas as tecnologias de segurança existentes. Ele tem como objetivo tornar mais simples a administração de segurança do ambiente cooperativo, ao integrar e posicionar tecnologias específicas para a proteção do ambiente. O *firewall cooperativo* forma, em conjunto com a rede integrada virtualmente do ambiente cooperativo, o que chamamos de Ambiente Cooperativo Seguro.

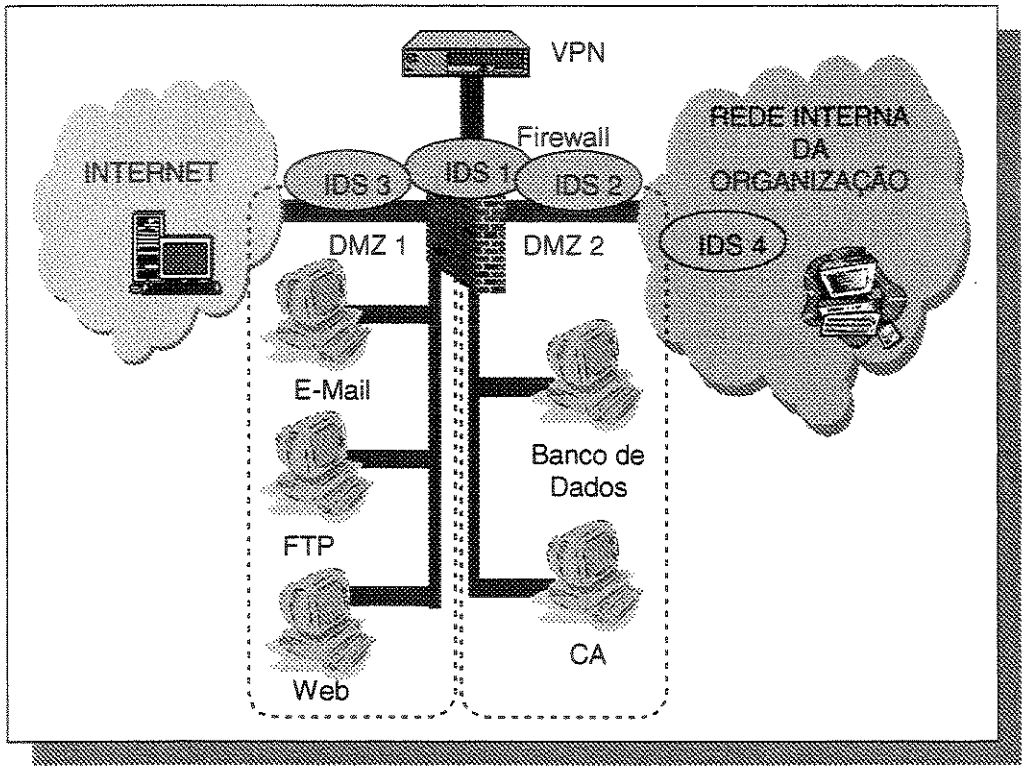


Figura 5.1: A arquitetura de segurança do *firewall cooperativo*

O paradigma fundamental que sustenta a construção de um ambiente seguro como este, isto é, baseado em *firewalls*, consiste na demarcação de um perímetro de segurança, visando estabelecer que a área interna por este delimitada deve ser protegida daquilo que se situa fora de suas fronteiras. Assim, o procedimento é análogo àquele utilizado na segurança de propriedades físicas: barreiras são erguidas no perímetro (muros) para que a travessia seja efetuada de maneira

controlada através de um número reduzido de pontos de conexão supervisionados (portões contendo controle de acesso).

Desta forma, uma premissa básica inerente a esse modelo é a de que tudo aquilo que cruzar as fronteiras definidas pelo perímetro de segurança deve ser inspecionado, a fim de que se possa verificar se tal travessia é efetivamente permitida pela política de segurança. Podemos entrever aqui um conflito com uma característica básica do IPv6: seu suporte nativo à criptografia fim-a-fim (através de seu *framework* IPSec) permitiria transportar um tráfego cifrado entre uma máquina interna e outra externa, o qual não poderia ser verificado pelo sistema de segurança.

De fato, esse conflito ocorre mesmo em IPv4 com a utilização de aplicações que usam criptografia fim-a-fim como o SSH (*secure shell*), pois os dados da aplicação cruzam o *firewall* cifrados, permitindo inclusive o transporte de outros tipos de tráfego por intermédio do túnel criptográfico. Entretanto, com o suporte à criptografia fim-a-fim sendo oferecido pelo nível de rede, como no IPv6, tal situação ganha contornos ainda mais dramáticos.

Para analisar pormenorizadamente tal conflito, passemos, então, a explicitar a relação entre alguns dos principais mecanismos de segurança utilizados em *firewalls* e o IPv6.

5.1.2 Filtragem de pacotes, *proxies* e NAT

A filtragem de pacotes (*packet filtering*), ou escrutínio, é um dos componentes clássicos de um ambiente seguro baseado em *firewalls*. Sua idéia básica é submeter cada um dos pacotes de dados que pretende cruzar o perímetro de segurança a uma verificação baseada num conjunto de regras de filtragem. Cada uma dessas regras especifica uma determinada ação, como aceitar, descartar ou rejeitar, que deve ser tomada caso verifiquem-se algumas características no pacote analisado, que são extraídas dos cabeçalhos dos níveis de rede e transporte - endereços IP de origem e destino, número de portas TCP ou UDP de origem e destino, interface de rede pela qual chega o pacote, entre outras.

Desta forma, é imediatamente notável a dificuldade que a utilização de IPv6 traz para a técnica de filtragem de pacotes: ao cifrar os cabeçalhos de transporte de um pacote, inviabiliza-se a verificação com base nessas características.

A mesma dificuldade ocorre também com os *proxies*, pois estes mecanismos atuam como intermediários entre clientes internos e servidores externos, situando-se também no perímetro da rede, porém efetuando uma verificação do tráfego no nível da aplicação. Logo, com uma cone-

xão cifrada, por intermédio do IPv6, entre cliente e servidor, o *proxy* não poderia nem mesmo ser utilizado.

O mecanismo de tradução de endereços de rede (NAT - *Network Address Translation*), por sua vez, consiste em trocar-se o endereço IP de origem/destino (ou ambos) de um pacote - ou mesmo as portas TCP/UDP de origem/destino - por outros valores, de acordo com a necessidade. Esse mecanismo foi criado inicialmente como uma solução de curto prazo para as restrições de espaço de endereçamento do IPv4. O NAT permite que, dentro de uma rede, um grande número de máquinas utilize endereços internos, não-válidos na Internet - e que, portanto, podem ser usados também por diversas outras redes -, todas compartilhando apenas um número bem menor de endereços válidos para comunicarem-se externamente, estes sim devendo ser únicos na Internet. Desta forma, como o IPv6 possui um espaço de endereçamento muitíssimo maior do que o do IPv4, poder-se-ia supor que o NAT perderia completamente sua razão de ser num ambiente que utilizasse a nova versão do IP.

Entretanto, além do endereçamento, o NAT possui também uma grande aplicação em segurança: ao conferir às máquinas internas endereços não-válidos, esconde-se a topologia da rede interna, uma vez que um observador de fora vê o tráfego como originado apenas daquele pequeno número de endereços válidos, que sobrescrevem aqueles internos na comunicação com a Internet. Logo, um usuário malicioso na rede externa teria maior dificuldade em localizar uma máquina interna e disparar contra ela um ataque, pois o mapeamento entre endereço-porta internos (não-válidos) e endereço-porta válidos é realizado de maneira dinâmica pelo *firewall*, e é extremamente volátil. Apesar de resolver o problema de endereçamento, o IPv6 não proporciona o ocultamento da topologia da rede interna e, assim, os clientes internos que se comunicarem com a Internet através de um endereço IPv6 válido na Internet estarão sujeitos a receber pacotes maliciosos de usuários externos. A utilização de filtros de pacotes poderia minimizar o problema porém, como vimos acima, o IPv6 traz também problemas ao escrutínio. Desta maneira, a exposição das máquinas internas seria aumentada e, assim, também a necessidade de fortificá-las. Isso pode significar uma grande dificuldade em ambientes em que clientes internos são muito heterogêneos, dispersos geograficamente ou em que existem equipamentos antigos que não podem ser atualizados por restrições de *hardware*: um ataque bem-sucedido a qualquer um deles comprometeria a segurança de toda a rede.

Mesmo que o uso de NAT seja, no futuro, completamente abandonado, durante a transição para o IPv6 será ainda necessário levar em conta a integração do IPSec com o NAT, este ainda amplamente utilizado, seja por conta do uso de IPSec sobre IPv4, como também pela operação em redes mistas com IPv6 e IPv4, empregando NATs para garantir a interoperabilidade entre as duas versões. Diversos conflitos surgem do embate entre NAT e IPSec [ABO 03], dos quais podemos destacar dois significativos exemplos: (1) a incompatibilidade entre o AH do IPSec e o NAT: como o cabeçalho AH incorpora os endereços IP de origem e destino, as alterações produzidas por um NAT irão invalidar a verificação de integridade da mensagem; (2) incompatibilidade entre *checksums* e NAT: os *checksums* de TCP e UDP utilizam os endereços IP para o seu cálculo [STE 94], assim o ESP do IPSec só não será afetado pelo NAT quando os protocolos TCP e UDP não estiverem envolvidos (como no modo túnel) ou quando o *checksum* estiver desabilitado como é possível com o UDP do IPv4 (mas não do IPv6).

Recentes esforços de pesquisa para coadunar NAT e IPSec têm utilizado o modo túnel do IPSec para encapsular os pacotes que devem ser protegidos em pacotes UDP [HUT 03].

5.1.3 Redes Privadas Virtuais (VPN)

As Redes Privadas Virtuais (*Virtual Private Network* - VPN) são um componente importante dentro do ambiente cooperativo, principalmente no seu aspecto econômico, ao permitirem que conexões dedicadas e estruturadas de acesso remoto, 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 entre pontos distintos.

Para os usuários que se comunicam através de uma VPN, é como se duas redes fisicamente distintas 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 5.2, onde o túnel VPN é iniciado e finalizado nos *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 5.3, através de um *software* cliente [NAK 03]. Essa solução, na qual o túnel VPN é iniciado no cliente, que se conecta a um provedor de acesso à

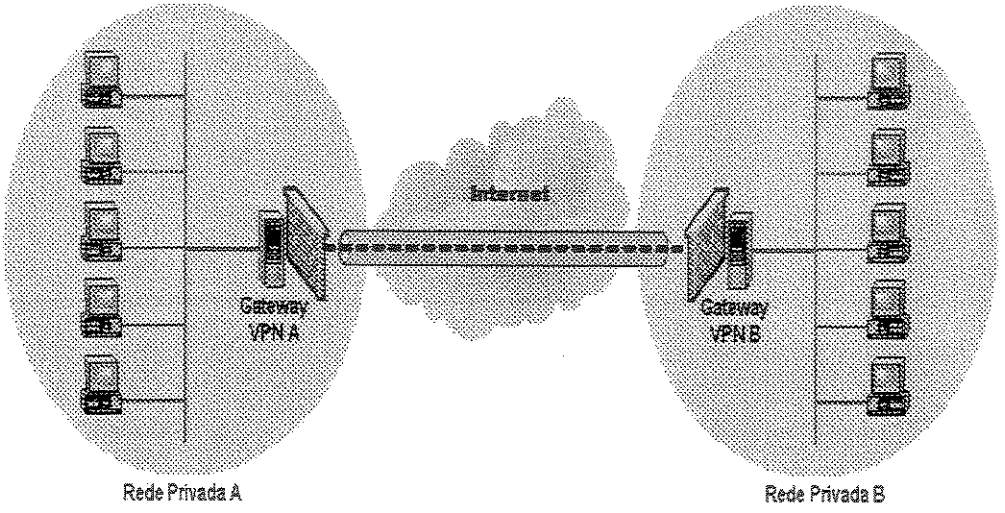


Figura 5.2: *Gateway-to-gateway* VPN.

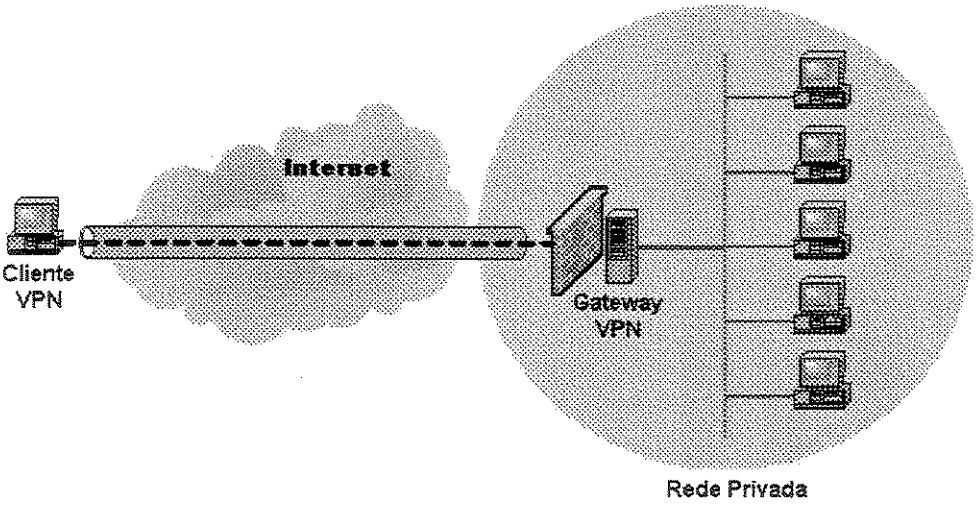


Figura 5.3: *Client-to-gateway* VPN.

Internet (*Internet Service Provider* - ISP), substituindo os acessos remotos diretos, é conhecida como acesso remoto VPN (*remote access 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.

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.

O uso de IPSec, em modo túnel, é uma alternativa que vem sendo padronizada pela grande maioria das soluções VPN, por atender perfeitamente aos requisitos fundamentais acima mencionados [REZ 02]. É importante ressaltar que o termo "Rede Privada Virtual" só se aplica aos cenários onde o IPSec é utilizado em modo túnel. A utilização do protocolo IPSec em modo transporte, para cifragem fim-a-fim, não constitui uma VPN, pois não faz uso de técnicas de tunelamento, uma das principais características das VPNs.

Neste contexto, o impacto causado pelo IPv6 nos cenários atuais de redes privadas virtuais pode seguir duas abordagens, que tomam rumos totalmente opostos: a extinção do uso de VPNs, ou por outro lado, uma enorme difusão desta tecnologia. Isto ocorre porque uma das principais características do protocolo IPv6 é o suporte nativo aos mecanismos de segurança do IPSec.

Em um ambiente onde todas as máquinas podem se comunicar entre si, utilizando a cifragem fim-a-fim oferecida pelo modo transporte do IPSec, a criação de túneis cifrados se tornaria obviamente desnecessária. Sob este ponto de vista, as VPNs poderiam simplesmente cair em total desuso, uma vez que todo o tráfego entre máquinas já estaria sendo previamente protegido, tornando a tecnologia de túneis VPN obsoleta.

No entanto, em um cenário como esse, recaímos nos mesmos problemas de filtragem de pacotes, uso de *proxies* e NAT, apresentados anteriormente. E novamente, nos conflitamos com o modelo clássico de ambiente seguro, enfraquecendo o conceito de perímetro de segurança e movendo boa parte da responsabilidade pela segurança para as máquinas internas.

Isso leva a uma segunda possibilidade, a enorme difusão das VPNs. Se em um ambiente, novamente, todas as máquinas suportam IPSec, a possibilidade de diferentes configurações de túneis cifrados entre pares de máquinas é enorme. Na comunicação entre uma máquina interna, e uma máquina externa, por exemplo, poderíamos ter um primeiro túnel entre a máquina interna e o *firewall*, e um segundo túnel entre este último e a máquina externa. Dessa forma, toda a comunicação entre as duas máquinas seria cifrada, exceto no ponto onde estaria sendo realizada a filtragem de pacotes.

Este seria apenas um dos possíveis cenários. Várias outras topologias de túneis poderiam ser idealizadas, já que todas as máquinas do ambiente seriam potenciais *gateways* VPN.

Apesar desta possibilidade, a princípio, parecer solucionar todos os problemas, é importante notar que a criação de túneis IPSec ainda é um procedimento extremamente complexo e custoso, já que consome muitos recursos dos componentes envolvidos, impondo portanto, em alguns casos, sérias restrições físicas ou mesmo de administração de ambientes.

Além disso, é importante atentar para a possibilidade da existência de túneis aninhados, ou seja, um pacote já tunelado passando por um novo túnel e sendo novamente encapsulado. Além de causar um perigoso overhead no tamanho dos pacotes que trafegam pela rede, pode tornar ainda mais sensível o problema de consumo dos recursos computacionais.

5.1.4 Sistemas de detecção a intrusão (IDS)

O campo de estudo Sistema de Detecção a Intrusão se divide em dois tipos primários [MAT 02]: *Host Based Intrusion Detection System* (HIDS) e *Network-Based Intrusion Detection System* (NIDS). Tradicionalmente, a tecnologia mais comum de detecção é o NIDS [SPI 03]. Estes sistemas trabalham monitorando passivamente o tráfego da rede atrás de atividades suspeitas e não autorizadas. Quando estes sistemas identificam tais atividades, eles geram um alerta. O desafio para NIDS é definir como identificar atividades suspeitas e não autorizadas. Existem várias técnicas de análise, sendo que as mais comuns são: detecção por mau uso e detecção por anomalia [REI 03].

O mecanismo de detecção por mau uso monitora as atividades do sistema em busca de eventos ou conjuntos de eventos, que representam padrões característicos de ataques conhecidos, comumente chamados assinatura de ataque. É considerada uma abordagem bastante eficiente, pois gera um número menor de alarmes falsos. Porém, esta abordagem é capaz apenas de detectar ataques previamente conhecidos e codificados e, dependendo do nível de detalhes das assinaturas, pode também apresentar dificuldade na detecção de variantes de ataques conhecidos. Outro problema é a atualização de novas regras, pois à medida que novos ataques são identificados, novas assinaturas precisam ser adicionados a base de dados. Caso contrário, o NIDS falhará na identificação de novos ataques. O processo de atualizar as assinaturas nunca acabará, assim como os *hackers* nunca deixarão de desenvolver novos ataques. Exemplos de sistemas que utilizam esta técnica: P-BEST, CLIPS, STAT, USTAT, IDIOT.

O mecanismo de detecção por anomalia busca comportamentos anormais. Ele utiliza perfis, que representam o comportamento normal dos usuários, do sistema e da rede. Essa abordagem, que se baseia no comportamento normal do sistema e não em características específicas de ataques, é capaz de detectar novos ataques. Entretanto, as maiores desvantagens dessa abordagem são: (1) geração de um grande número de alarmes falsos, devido ao comportamento imprevisível de usuários e redes; e (2) necessidade de conjuntos extensivos de eventos e de treinamento para caracterizar um perfil de comportamento normal. Exemplos de sistemas que utilizam esta técnica: Tripwire, IDES, Haystack, W&S, TIM, AAFID e EMERALD.

Apesar destes NIDS (mau uso e anomalia) terem características diferentes, eles precisam enfrentar os mesmos desafios [SPI 03]:

- NIDSs tendem a gerar um grande volume de dados, que consomem tempo e recursos para serem analisados e revisados;
- Muitos NIDSs encontram dificuldades em distinguir atividades legítimas de tráfego malicioso, pois compartilham similaridades, o que leva a falsos positivos;
- Os NIDSs também podem falhar na detecção de novos ataques, gerando falsos negativos;
- NIDSs precisam de hardware, que os permita acompanhar as atividades e tráfego da organização. Quanto mais rápida a rede e mais dados tiver, mais robusto o NIDS deverá ser;
- Mais e mais organizações estão adotando a cifragem de seus dados através da adoção de métodos como SSH, SSL e IPSec. Porém, estas tecnologias podem "cegar" o NIDS sobre o que está acontecendo na rede;
- Muitos NIDS não são capazes de analisar e compreender pacotes IPv6, a exemplo do ataque ocorrido em dezembro de 2002, usando tunelamento IPv6 em *honeynets* [THE 03].

A introdução de IPv6 em um ambiente, com um sofisticado NIDS implantado, traz como obstáculo mais importante a utilização de autenticação e cifragem, pois o NIDS desejará, no mínimo, verificar a validade do AH em cada pacote, como também checar o conteúdo do ESP. Este é o problema de canais cifrados e algumas soluções já foram apresentadas: (1) compartilhamento de chave de sessão pelo servidor, para permitir decifragem *on-the-fly*; (2) armazenagem de chaves no lado do servidor para decifrar *off-line* pacotes capturados; e (3) o uso de *ssldump* para decifrar SSL. Contudo, estas soluções implicam no controle das duas pontas do canal para obtenção das chaves de sessão [TRI 03].

O uso de IPv6 estimula a eliminação do critério de detecção por mau uso, pois a definição de milhares de assinaturas torna inviável o funcionamento do NIDS. O número de regras para detecção por anomalia é limitado e conhecido, já que o tráfego autorizado é menor que o tráfego não autorizado, mesmo considerando o tamanho do espaço de endereçamento IPv6 e sua natureza dinâmica.

A implantação de IPv6 pressionará para a mudança do paradigma atual de soluções isoladas e localizadas para um sistema muito mais distribuído. Para o NIDS ser verdadeiramente efetivo, precisa monitorar apropriadamente todo o sistema, estando instalado em cada ponto da rede, já que o tráfego passará cifrado em pontos importantes da rede.

Os NIDS deverão enfrentar estes desafios com a reformulação de seu modelo, que precisa ser distribuído, usar detecção por anomalia, ser pervasivo, além de ter os dados centralizados para permitir uma correlação tão sofisticada quanto possível.

Entretanto, se os NIDS não acompanharem esta tendência, os HIDS podem concentrar todas as funções dos IDSs, já que na verdade, IPv6 é mais compatível com o modo de funcionamento dos HIDS, que tipicamente monitoram eventos e *logs* de segurança no nível do sistema operacional de cada máquina da rede.

5.1.5 Infra-estrutura de chave pública (PKI)

Os serviços básicos oferecidos por uma PKI são autenticação, integridade e confidencialidade. Porém, existem outros serviços que podem ser construídos com a PKI e que se beneficiarão dos seus serviços básicos, que são: comunicação segura, *time stamping* seguro, não-repúdio e gerenciamento de privilégios [ADA 99]. Os exemplos de comunicação segura, relevantes para este capítulo, são:

- correio eletrônico seguro;
- acesso seguro a servidores *web*;
- canais seguros fim-a-fim, como os protocolos IPSec e IKE.

Logo, percebe-se que não existe conflito entre o modo de funcionamento da PKI e do IPSec, ao contrário, eles são complementares, já que a PKI oferece serviços básicos que são essenciais ao IPSec.

IPSec é um típico serviço de rede com políticas de segurança habilitadas, porém as funções de segurança são executadas apropriadamente, somente se, as políticas estão corretamente especificadas e configuradas. As práticas atuais demonstram que as bases de dados de IPSec são configuradas manualmente, o que é razoavelmente ineficiente e sujeito a erros para grandes sistemas de redes distribuídas. Além disto, um número crescente de aplicações e serviços Internet torna a implantação de políticas em IPSec cada vez mais complexa.

Enquanto os padrões básicos para IPSec são considerados estáveis e serão estendidos, principalmente, para permitirem adição de outros algoritmos de cifragem e autenticação, mais trabalho resta a ser feito na área de IKE e no melhoramento de mecanismos de proteção contra análise de tráfego e ataques de negação de serviço.

Portanto, a implantação completa do IPSec depende da disponibilidade de uma PKI amigável, técnica, organizacional e politicamente aceitável, capaz de manipular um grande número de usuários ou certificados [HAG 02].

5.2 Cenários

Como foi possível observar no Capítulo 3, os novos mecanismos incorporados pelo IPv6 visam suprir as deficiências apresentadas pelo IPv4 ao longo dos anos. Sob o ponto de vista da segurança, tornou-se patente a necessidade, cada vez mais urgente, de tecnologias que solucionassem as vulnerabilidades clássicas de segurança do IPv4.

Ao mesmo tempo, as importantes inovações introduzidas pelo IPv6, através do IPSec, fizeram com que fosse cada vez mais difícil estabelecer uma fronteira entre esses dois conceitos. Optar pela adoção do IPv6 sem fazer uso dos recursos de segurança do IPSec seria, sem sombra de dúvidas, um retrocesso.

No entanto, vimos que a adoção de tais recursos de segurança conflita drasticamente com o modo de funcionamento dos principais mecanismos de segurança atualmente utilizados.

A seguir serão apresentados e analisados alguns cenários possíveis de integração IPSec com o modelo de segurança atual.

5.2.1 IPSec de *firewall* a *firewall*

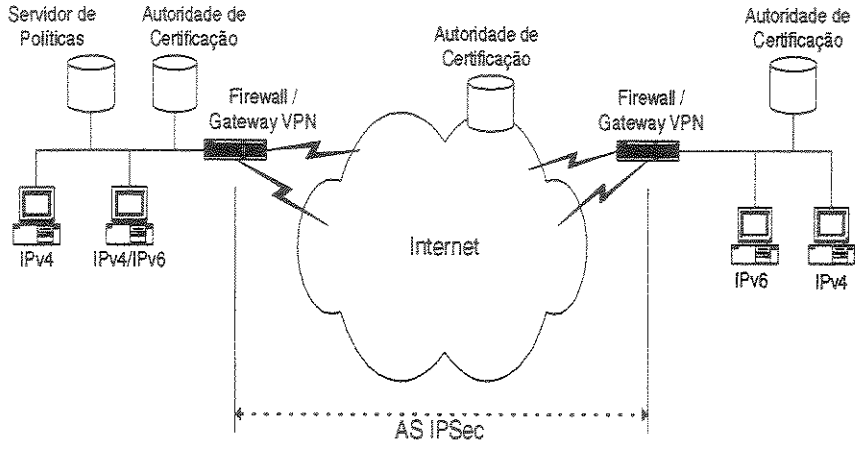


Figura 5.4: IPSec de Firewall a Firewall.

Um cenário inicialmente idealizado seria aquele onde todas as máquinas possuem suporte ao IPv6, porém o uso do IPSec se limitaria à forma tradicional de VPNs *gateway-to-gateway*, como ilustrado na Figura 5.4.

Essa seria uma forma extremamente simples de migração para o IPv6, onde o paradigma de segurança atual não necessitaria de quaisquer alterações. A grande vantagem deste modelo é a forma de integração harmoniosa entre IPv6/IPSec e o modelo clássico de Ambiente Cooperativo Seguro.

É importante ressaltar, que a própria política de segurança da organização pode proibir a utilização de túneis seguros dentro de sua rede, o que impede o monitoramento dos *e-mails* recebidos e enviados por seus funcionários. Assim como impede o monitoramento dos acessos à web efetuados pelos funcionários.

5.2.2 IPSec entre *firewall* e máquina externa

Apesar da simplicidade apresentada no cenário anterior ser uma característica desejável, podemos observar que neste caso existe uma sub-utilização dos recursos de segurança oferecidos pelo IPv6/IPSec, limitando-se ao uso em cenários de VPN já utilizados hoje em IPv4. Um cenário análogo poderia ser obtido estendendo a utilização do IPSec à funcionalidade de acesso remoto

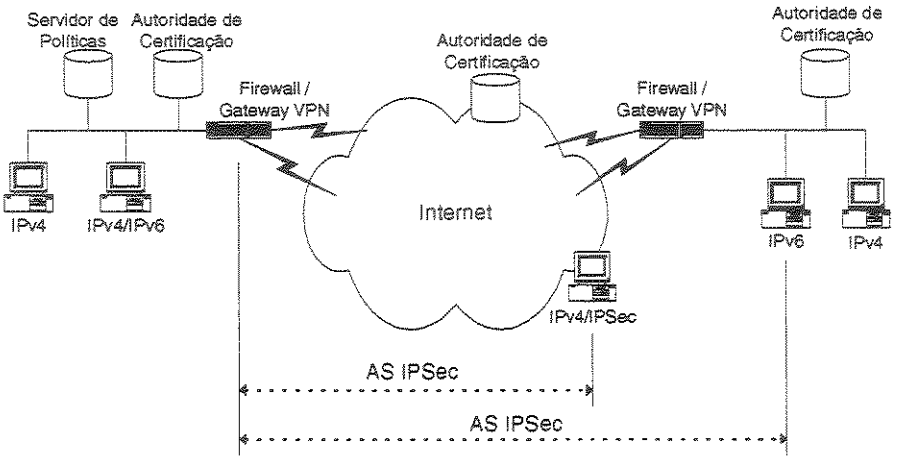


Figura 5.5: IPSec entre Firewall e Máquina Externa.

VPN. Neste novo cenário, o *gateway* VPN de nosso ambiente seguro, representado pela rede mais à esquerda na Figura 5.5, suportaria túneis IPSec não só com outros *gateways* VPN, mas também com clientes remotos.

O grande diferencial deste cenário em relação ao seu correspondente em IPv4, é que agora todos os clientes remotos, por suportarem IPv6/IPSec, possuem a capacidade nativa de acesso remoto VPN. Isso é vantajoso por aumentar a escalabilidade em relação aos cenários atuais, onde um dos problemas existentes é como permitir que sistemas que não suportam nativamente IPSec façam uso do acesso remoto VPN.

5.2.3 IPSec entre máquina interna e máquina externa

Um dos cenários mais flexíveis e desejados de se obter é aquele onde máquinas internas e externas se comunicam fazendo uso do IPSec, seja em modo transporte ou em modo túnel (Figura 5.6).

Contudo, apesar deste ser o modelo mais vantajoso do ponto de vista da segurança da comunicação, os impactos causados no modelo de ambiente seguro atualmente consolidado são enormes.

Este cenário de integração IPv6/IPSec se daria de forma extremamente conflitante com os paradigmas de segurança atuais, incidindo diretamente nos mecanismos de filtragem de pacotes, *proxy*, NAT, IDS e VPNs, como discutido anteriormente.

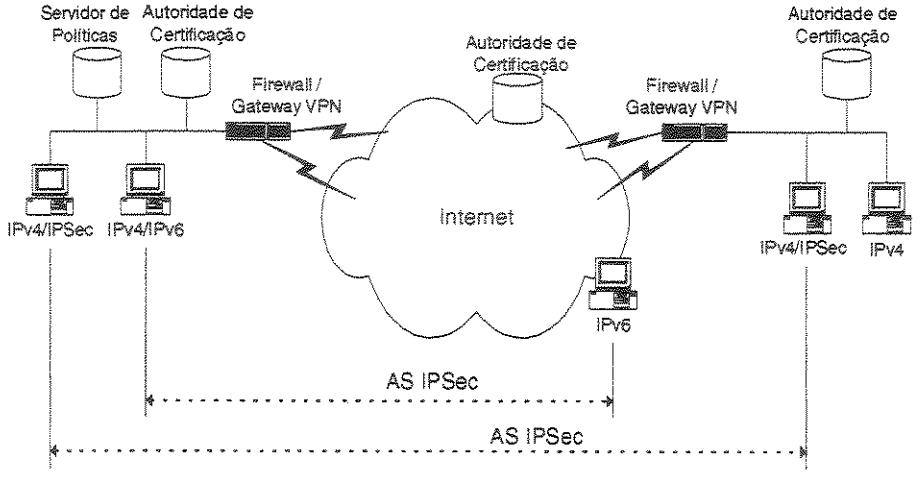


Figura 5.6: IPSec entre Máquina Interna e Máquina Externa.

Além disso, aumentaria sobremaneira o grau de complexidade das tarefas de administração e gerência de ambientes computacionais.

5.2.4 IPSec entre máquina interna e máquina externa com *proxy* de segurança

Uma solução interessante para os problemas surgidos no cenário anterior é a utilização de vários túneis cifrados ao invés de um único. A idéia é que a comunicação entre máquinas internas e externas continue utilizando a proteção do IPSec, fazendo uso, contudo, de um *proxy* de segurança (Figura 5.7).

Neste ambiente, para que clientes remotos possam se comunicar com máquinas internas, eles devem antes estabelecer um túnel cifrado com o *proxy* de segurança, que por sua vez estabelece um túnel cifrado com a máquina interna. Isso permite que mecanismos como filtragem de pacotes, *proxy*, NAT e IDS possam atuar sobre o tráfego de dados no instante em que o *proxy* de segurança repassa as informações de um túnel para o outro.

Esse cenário consiste basicamente de uma extrapolação do uso de VPNs, possibilitada pela integração IPv6/IPSec, e poderia se desdobrar em vários outros cenários, com dois ou até mesmo vários *proxies* de segurança intermediando a comunicação.

Essa possibilidade, apesar de interessante, é no mínimo perigosa do ponto de vista da privacidade dos dados, pois insere um possível ponto de observação das informações. Além do mais,

novamente teríamos uma complexidade significativa nas tarefas de administração do ambiente, e principalmente na gerência dos túneis cifrados, como apresentado anteriormente.

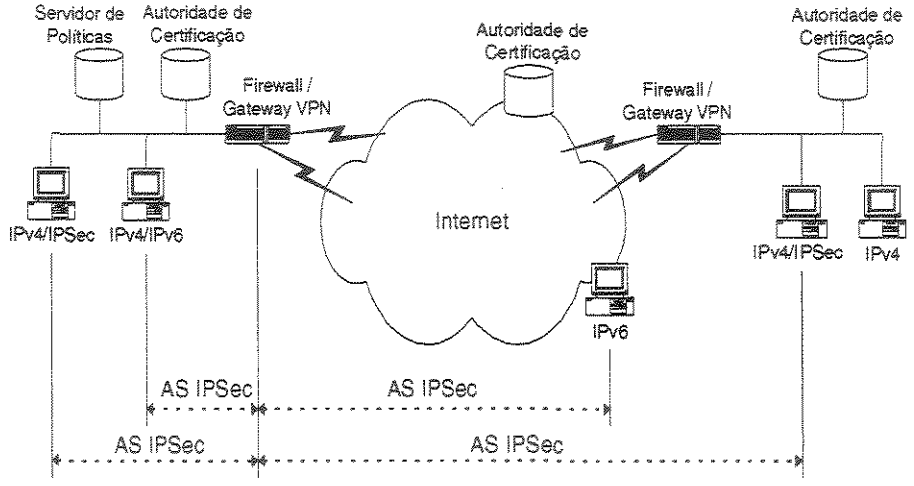


Figura 5.7: IPSec entre Máquina Interna e Máquina Externa com *Proxy* de Segurança.

5.3 *Firewall* Distribuído e Híbrido

Para tentar contornar os problemas de integração entre o IPv6/IPSec e os ambientes seguros, uma abordagem diferente foi proposta por Bellovin [BEL 99]: os *firewalls distribuídos*. A sua abordagem consiste no inverso da empregada pela subseção anterior: ao invés de tentar inserir o IPv6/IPSec em um ambiente seguro IPv4 - baseado, como vimos na constituição de um perímetro de segurança que delimita os escopos interno e externo -, parte-se do novo ambiente, já com a adoção do IPv6/IPSec, para erigir um novo paradigma de segurança que atenda a seus requisitos específicos.

Desta forma, o grande problema que se observa no ambiente IPv6/IPSec é que todas as máquinas tornam-se capazes de estabelecer conexões com associações criptográficas fim-a-fim, as quais deseja-se submeter a uma política. Para tanto, a distribuição dos pontos de aplicação da políticas é proposta com vistas a atender a essa necessidade, de forma que cada máquina efetue a verificação das conexões de que participa - daí o nome de *firewalls distribuídos*. Por outro lado, Bellovin [BEL 99] propõe, ainda, a definição centralizada da política de segurança, com a finalidade de viabilizar a administração e conferir escalabilidade à sua solução.

Para seu funcionamento, o *firewall distribuído* utiliza três componentes básicos [IOA 00]:

- uma linguagem de *definição* da política de segurança, que especifica os tipos de conexões que devem ser permitidos ou bloqueados;
- um mecanismo para *distribuição* das políticas de segurança de forma segura;
- um mecanismo de *aplicação* da política de segurança a pacotes e conexões, que chegam a cada máquina sob a proteção do *firewall* - baseado em algum tipo de autenticação.

Entretanto, a implementação de cada um desses três componentes está longe de ser trivial, e requer pesquisa. Apesar da existência de trabalhos que proponham a linguagem *Keynote* [BLA 99] para definição das políticas de segurança, com esboços do mecanismo de aplicação [IOA 00], os *firewalls distribuídos* são, ainda, uma solução eminentemente conceitual, não possuindo implementação acabada. Há, portanto, amplo espaço para pesquisas nesse campo.

5.4 Integração da rede IPv6 com outras redes

A migração de uma rede IPv4 para IPv6 pode ser feita passo a passo, começando com uma única máquina ou sub-rede, até contemplar todas as máquinas e roteadores da rede de uma organização. Neste capítulo, não foi considerado como ocorre a migração de uma rede IPv4 para IPv6, somente foram analisados os problemas de integração que uma rede IPv6 enfrenta com as ferramentas de segurança consolidadas em IPv4. Logo, uma rede IPv4 migrada para IPv6 precisa ser integrada com as ferramentas de segurança já consolidadas nos Ambientes Cooperativos Seguros, visto que seu *framework* de segurança não resolve todos os problemas de segurança existentes na Internet.

Além disto, esta rede migrada IPv6 precisa continuar se comunicando com outras redes IPv6 ou IPv4 na Internet, o que demanda a necessidade por mecanismos ou técnicas que permitam a interoperabilidade entre redes distintas. Portanto, redes IPv6 também precisam ser integradas a outras redes.

É fato que IPv6 e IPv4 coexistirão por muitos anos, já que a migração de todas as redes IPv4 não ocorrerá simultaneamente. Um grande número de técnicas já foi definido para tornar a coexistência possível e prover uma fácil transição entre redes IPv4 e IPv6. Deste modo, no Capítulo 6 serão apresentadas as várias técnicas e mecanismos de transição existentes entre IPv4 e IPv6, bem como os possíveis cenários de integração e mecanismos aplicáveis.

5.5 Conclusão

Em relação ao conflito existente entre IPv6 e as atuais ferramentas de segurança, recomendam-se dois cenários mais interessantes em termos de compatibilidade. O primeiro cenário seria aquele da Figura 5.4, página 110, que não utiliza a característica de criptografia fim-a-fim do IPSec, preservando o ambiente seguro formado em IPv4 e que é baseado na constituição de um perímetro de segurança que delimita os escopos interno e externo. Este cenário seria utilizado quando a própria política de segurança da organização proibisse a utilização de túneis seguros dentro de sua rede, o que impede seu monitoramento do conteúdo de correio eletrônico e acesso web de seus usuários internos. Pode existir também a necessidade da organização delimitar áreas internas com acesso restrito a poucos funcionários, o que implica na necessidade do estabelecimento de perímetros internos de segurança entre as áreas da organização e que podem ser estabelecidas com o uso de *firewalls tradicionais*. Neste cenário, todas as ferramentas atuais de segurança devem ser adaptadas para suportar IPv6, pois o cabeçalho IPv6 é diferente do cabeçalho IPv4.

O segundo cenário seria a abordagem diferente proposta pelo Bellovin [BEL 99]: os *firewalls distribuídos*, cuja abordagem parte de um novo ambiente, já com a adoção do IPv6/IPSec, para erigir um novo paradigma de segurança que atenda a seus requisitos específicos. Neste cenário, cada máquina é capaz de estabelecer conexões com associações criptográficas fim-a-fim, além de efetuar a verificação das conexões de que participa, ou seja, cada máquina efetua sua própria proteção de acordo com a política definida pela organização. Esta política de segurança é definida de forma centralizada, com a finalidade de viabilizar a administração e conferir escalabilidade à sua solução, contudo, sua aplicação é distribuída. Neste segundo cenário, todas as ferramentas sofrerão adaptações para funcionarem eficientemente no novo ambiente, a exemplo dos NIDS, que trabalham monitorando o tráfego da rede atrás de atividades suspeitas e não autorizadas. Na verdade, os HIDS, que monitoram eventos e *logs* de segurança no nível do sistema operacional de cada máquina da rede, são mais compatíveis com o modo de funcionamento de um *firewall distribuído*. Eles precisarão ser reformulados para detectarem ataques usando assinaturas de ataques às aplicações. Assim como, as demais ferramentas, que trabalham no nível de aplicação, também podem ser adaptadas para desempenharem suas funções em cada máquina da rede, ao invés de trabalharem em um ponto único na borda da rede.

Independentemente do cenário escolhido é indispensável ressaltar a importância da simultaneidade da migração da rede em conjunto com a migração das ferramentas de segurança, pois o inverso deixará a rede exposta a qualquer tipo de ataque.

Capítulo 6

Mecanismos de Transição e Cenários de Comunicação IPv4/IPv6

A IETF criou o Grupo de Trabalho Next Generation Transition (NGTRANS), cujo objetivo era desenvolver ferramentas e mecanismos que permitem a redes e máquinas IPv4 mudarem suavemente para IPv6. Durante o período de dois anos, o Grupo NGTRANS criou e disponibilizou inúmeros esboços (*drafts*), que estabeleceram uma miríade de mecanismos para a integração com IPv6, que vão desde um simples tunelamento a complexos mecanismos como Teredo [HUI 02].

O Grupo NGTRANS, que criou mais de doze ferramentas, foi fechado em fevereiro de 2003, porém suas funções foram transferidas para o Grupo de Trabalho v6ops [IPV 03], cujo finalidade, mais relevante para este capítulo, é refinar o processo de integração de IPv6. Este capítulo tenta identificar a maioria dos mecanismos de transição criados pelo grupo NGTRANS, categorizá-los e explicar brevemente como eles funcionam. Adicionalmente, os cenários de comunicação entre redes IPv4 e IPv6 são mostrados, bem como os mecanismos que se aplicam a cada cenário.

Cada mecanismo de transição pode ser classificado como pertencente a uma das seguintes categorias [MCG 03a] [HAG 02] [SCH 03] [MCG 03b]:

- pilha dupla (*dual stack*);
- tunelamento (*encapsulation* ou *tunnel*);
- tradução (*translation*).

Cada categoria descreve a metodologia básica do mecanismo, já que um mecanismo de transição pode pertencer a mais de uma categoria e, freqüentemente, trabalhar junto com outros mecanismos, assim como sobrepor ou oferecer funções diversas.

6.1 Pilha Dupla

Conceitualmente, é a técnica mais fácil para integrar IPv6 em uma rede IPv4, uma vez que introduz IPv4 e IPv6 no mesmo ambiente e na mesma interface (Figura 6.1). Tanto os roteadores como as máquinas de trabalho precisam ser atualizadas para suportar IPv6 e continuar suportando IPv4, ou seja, o sistema operacional precisa ter as duas pilhas IPv4 e IPv6. Esta técnica exige duas tabelas de roteamento com funções sobrepostas de administração e gerenciamento similar. Um nó pilha dupla tem ambos os endereços configurados em sua interface, sendo que o endereço IPv6 é designado tanto estaticamente quanto dinamicamente, através de configuração *stateless* ou *stateful* [GIL 00].

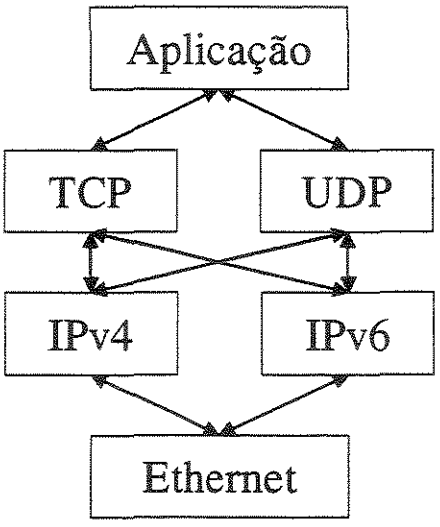


Figura 6.1: Pilha dupla IPv4 e IPv6.

6.2 Tunelamento

Tunelamento é freqüentemente utilizado, quando partes ou toda infra-estrutura de rede não é capaz de prover conectividade IPv6. Portanto, tunelamento permite que o tráfego IPv6 seja carregado sobre a infra-estrutura de rede IPv4.

É o processo pelo qual a informação de um protocolo é encapsulada dentro do pacote de outro protocolo, permitindo que a informação original seja carregada sobre o segundo protocolo. Um exemplo: o pacote IPv6, que é transmitido desta forma, é encapsulado em um pacote IPv4 (usando IP protocolo 41), tunelado até o destino, onde é desencapsulado e o pacote original IPv6 encaminhado.

Este mecanismo pode ser usado quando duas máquinas, usando o mesmo protocolo, desejam se comunicar sobre uma rede que usa outro protocolo de rede. Os métodos de tunelamento disponíveis são:

6.2.1 Túnel configurado

Túnel configurado é definido, na RFC 2893, como tunelamento IPv6 sobre IPv4, onde o endereço IPv4 final do túnel é determinado pela configuração da máquina responsável pelo encapsulamento [GIL 00]. Portanto, o nó encapsulado precisa manter informação sobre todos os endereços finais dos túneis. Este tipo de túnel é ponto-a-ponto e precisa de configuração manual.

6.2.2 *Tunnel Broker*

Ao invés de configurar manualmente cada ponto final de túnel, é possível usar *scripts* executáveis para desempenhar esta tarefa. Esta alternativa automática é chamada de *tunnel broker* e é apresentada em [DUR 01].

Assim como os túneis configurados manualmente, o *tunnel broker* é útil onde um usuário tem uma máquina pilha dupla em uma rede IPv4-only e deseja obter conectividade IPv6. A filosofia básica do *tunnel broker* é permitir a um usuário entrar em contato com o servidor *web*, opcionalmente entrar com detalhes de autenticação e receber de volta um *script* para estabelecer um túnel *IPv6-in-IPv4* até o servidor *tunnel broker*.

O provedor de um serviço *tunnel broker* precisa prover:

- servidor de *web* (disponível sobre IPv4);
- roteador pilha dupla, capaz de aceitar comandos de *setup* para criar novo túneis para clientes finais de túnel.

A operação típica de um serviço *tunnel broker* é ilustrado na Figura 6.2. No passo (1), o usuário se conecta ao servidor de *web* para pedir um túnel. No passo (2), o servidor de *web* retorna

um *script* para que o cliente possa criar um túnel com o servidor de túnel e informa ao servidor de túnel do novo cliente. No passo (3), o cliente ativa o *script* e obtém acesso a rede IPv6 através do servidor de túnel.

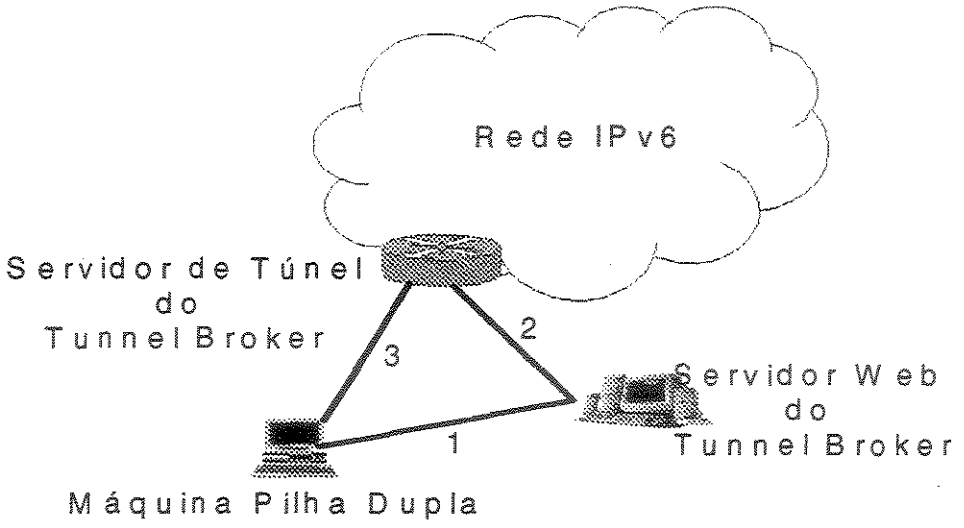


Figura 6.2: Tunnel Broker.

6.2.3 Túnel automático

Este método somente pode ser usado em comunicações *router-to-host* e *host-to-host*, que são esquemas onde qualquer ponto final do túnel também é o receptor dos pacotes. Este tipo de túnel usa endereços IPv6 *IPv4-compatible* nas extremidades do túnel. Em razão do uso de endereços privados, este túnel funciona somente em tunelamento *IPv6 over IPv4*, e não o contrário.

6.2.4 *6to4*

O mecanismo de transição conhecido como *6to4* é uma forma de tunelamento automático *router-to-router*, que usa o prefixo IPv6 2002::/16, para designar uma rede que participa do 6to4. Ele permite que domínios IPv6 isolados se comuniquem com outros domínios IPv6 usando uma configuração mínima [CAR 01].

Um domínio IPv6 isolado, desejando se comunicar com outros domínios IPv6, se designará um prefixo de 2002:V4ADDR::/48, cujo V4ADDR é o endereço IPv4 global configurado na interface apropriada de saída do roteador. Este prefixo tem exatamente o mesmo formato que prefi-

xos normais /48 e, desta forma, permite que um domínio IPv6 use-o como qualquer outro prefixo /48 válido.

No cenário onde domínios *6to4* desejam se comunicar com outros domínios *6to4*, não é necessário configurar o túnel. Pontos finais dos túneis são determinados pelo valor NLA (V4ADDR) do endereço IPv6 de destino contido no pacote IPv6 transmitido, conforme ilustra a Figura 6.3. Contudo, quando domínios *6to4* desejam se comunicar com domínios *IPv6-only*, a conectividade entre os domínios é alcançada através de um roteador *relay*, que tem ao menos uma interface lógica *6to4* e uma interface nativa IPv6. Em [HUI 01] é apresentado o endereço *anycast 6to4*, com o objetivo de simplificar a configuração de roteadores *6to4*.

O uso geral do *6to4* é ser um mecanismo para um roteador de borda IPv6 com apenas conectividade IPv4 externa estabelecer conectividade automática com a Internet pública IPv6. Outros métodos, como ISATAP ou rede nativa IPv6, podem ser usados dentro desta rede.

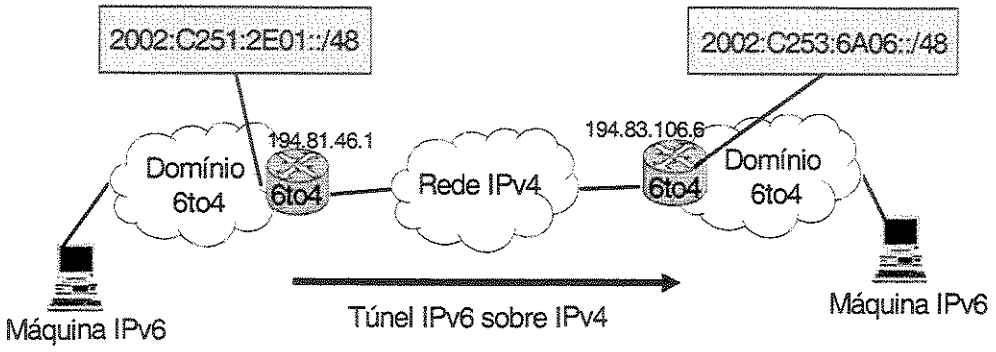


Figura 6.3: 6to4.

6.2.5 *6over4*

A motivação para este método é permitir que máquinas IPv6 isoladas, localizadas num *link* físico sem conectividade direta com roteador IPv6, se tornem máquinas IPv6 completamente funcionais usando um domínio IPv4, que suporte *multicast* IPv4 como seu enlace local virtual. Endereços *multicast* IPv6 são mapeados para endereços *multicast* IPv4 para permitir *Neighbor Discovery*. O método *6over4* está em desuso por várias razões, incluindo a ausência geral de suporte *multicast* IPv4 em várias redes [CAR 99].

6.2.6 ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) é uma alternativa ao *6over4*, já que conecta máquinas e roteadores IPv6 dentro de redes IPv4, sem introduzir impacto no tamanho da tabela de roteamento e exigir serviços especiais IPv4. Cada máquina precisa de um roteador ISATAP no enlace para obter endereço e informação de roteamento [TEM 02].

Pacotes enviados para a Internet IPv6 são roteados através de um roteador ISATAP e, pacotes destinados para outras máquinas na mesma rede são tunelados diretamente para o destino. Clientes ISATAP usualmente efetuam auto-configuração *stateless* de endereço IPv6 com descoberta de roteador ISATAP automática, porém eles também podem opcionalmente usar endereços designados estaticamente, quando exigido por circunstâncias especiais. É um método compatível com mecanismos inter-domínio como *6to4*.

6.2.7 Teredo

Teredo provê um mecanismo de transição, que permite a usuários, em um ambiente IPv4 NAT com endereçamento privado, obter conectividade IPv6. A idéia básica do Teredo é um nó encapsular pacotes IPv6 em UDP IPv4 e tunelá-los para um servidor Teredo na Internet IPv4. É função deste servidor desencapsular e entregar o pacote IPv6 [HUI 02].

O processo de criação do endereço ocorre unicamente através da negociação entre o servidor e o nó Teredo. O cliente Teredo busca, através de um processo de descoberta, encontrar uma porta UDP aberta no gateway NAT existente para alcançar o servidor Teredo. Uma vez encontrado, o cliente pode se comunicar usando IPv6 via o servidor. O protocolo Teredo busca obter um prefixo reservado IPv6 (como *6to4*).

6.2.8 DSTM

Dual Stack Transition Mechanism (DSTM) é uma solução para redes *IPv6-only*, cujas aplicações IPv4 ainda precisam de máquinas pilha dupla na infra-estrutura IPv6 [BOU 01]. É baseado no uso de túneis, para que o tráfego IPv4 seja tunelado sobre o domínio *IPv6-only* até alcançar um *gateway* IPv6/IPv4. O *gateway* tem como funções encapsular e desencapsular o pacote, assim como encaminhá-lo entre os domínios *IPv6-only* e IPv4.

A solução proposta pelo DSTM é transparente para quaisquer tipo de aplicações IPv4 e permite o uso de segurança da camada 3. Contudo, com o esquema usual de tunelamento, um ende-

reço IPv4 é exigido para qualquer máquina que queira se conectar a Internet IPv4. DSTM também reduz esta exigência alocando endereços apenas durante a comunicação, permitindo que várias máquinas compartilhem o mesmo endereço.

DSTM pode ser implementado se a infra-estrutura da rede suportar apenas IPv6. No entanto, alguns nós na rede têm capacidade pilha dupla e aplicações *IPv4-only*. DSTM consiste de três componentes, conforme Figura 6.4:

- um servidor DSTM, que é um servidor de endereço;
- um *gateway* DSTM ou TEP (*Tunnel End Point*);
- um nó pilha dupla, chamado de nó DSTM, que deseja se comunicar usando IPv4.

Os passos, para que ocorra uma comunicação neste cenário, são (Figura 6.4):

1. quando um pacote IPv4 precisa ser enviado, o cliente DSTM pede ao servidor por um endereço IPv4. Os protocolos DHCPv6 [DRO 03], TSP [BLA 02] e RPC já foram propostos para executar esta tarefa;

2. o servidor pede ao *gateway* DSTM para adicionar um TEP para o nó requisitante, já que ele controla o mapeamento de endereço IPv4/IPv6 efetuado pelo *gateway* DSTM. Se o ponto final do túnel é criado com sucesso, de acordo com a mensagem do *gateway*, o servidor DSTM, que gerencia a pilha de endereços IPv4, responde à máquina com as seguintes informações: endereço IPv4 alocado, a duração da alocação e os endereços IPv4 e IPv6 do TEP;

3. estas informações são usadas pelo cliente DSTM para configurar um túnel IPv4 sobre IPv6 (*4over6*) até o *gateway* DSTM. Neste momento, o cliente DSTM tem conectividade IPv4 e, se obteve um endereço IPv4 válido, é capaz de se conectar a qualquer máquina externa.

6.2.9 Classificação dos mecanismos de tunelamento

Esta classificação é útil, pois apesar de todos estes mecanismos pertencerem a uma mesma técnica, tunelamento, cada mecanismo tem características próprias que o distingue do restante. Desta forma, esta classificação visa agrupar os vários mecanismos de tunelamento em sub-classes

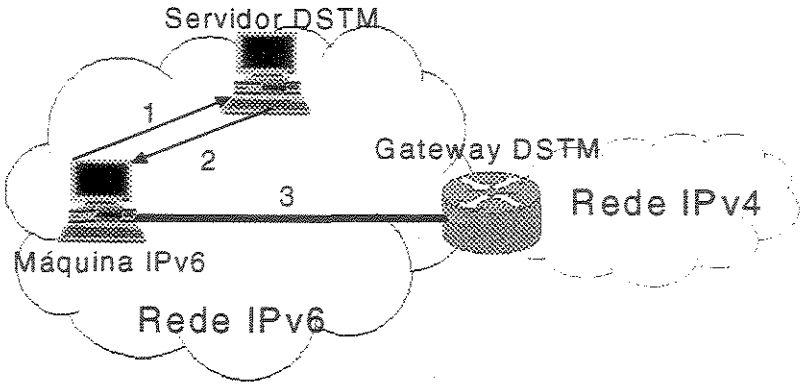


Figura 6.4: DSTM.

com características mais aproximadas. Logo, os mecanismos de tunelamento, explicados anteriormente, podem ser classificados conforme segue abaixo:

- tunelamento via servidor (origem IPv4) - é o método de transição, que estabelece túneis *IPv6-in-IPv4* entre clientes e servidores de túneis. Os mecanismos que fazem parte desta classe são *Tunnel Broker* e Teredo;
- tunelamento via servidor (origem IPv6) - é o mecanismo de transição, que estabelece túneis *IPv4-in-IPv6* entre clientes e servidores de túneis. O único mecanismo que integra esta classe é o DSTM;
- tunelamento *IPv6-over-IPv4* - é o método de transição, que usa endereços IPv4 para automaticamente gerar e configurar o túnel IPv6 sobre redes IPv4. Os mecanismos que integram esta classe são túnel configurado e túnel automático;
- tunelamento interno - é o mecanismo de transição, que usa a infra-estrutura da rede IPv4 como um *link* virtual, já que túneis *IPv6-in-IPv4* são criados automaticamente dentro da rede. Os mecanismos, que compõem esta classe, são ISATAP e *6over4*;
- tunelamento 6to4 - é um método de tunelamento automático *router-to-router*, que usa o prefixo IPv6 2002::/16, para designar uma rede que participa do *6to4*. O mecanismo *6to4* é o único mecanismo desta classe;
- tunelamento 4to6 - é um mecanismo de transição, que estabelece túneis *IPv4-in-IPv6* entre clientes e servidores ou, ainda, entre clientes e clientes.

6.3 Tradução

Mecanismos de Tradução são usados onde dispositivos *IPv6-only* desejam se comunicar com dispositivos *IPv4-only* ou vice-versa. Os mecanismos de tradução disponíveis são:

6.3.1 SIIT *(Stateless IP/ICMP Translation Algorithm)*

O mecanismo de tradução SIIT usa um tradutor localizado na camada de rede da pilha de protocolos. Este tradutor é chamado de tradutor de cabeçalhos e funciona traduzindo cabeçalhos de datagramas IPv4 em cabeçalhos de datagramas IPv6 e vice-versa [NOR 00].

6.3.2 NAT-PT *(Network Address Translation with Protocol Translation)*

É um serviço que permite às máquinas IPv6 e suas aplicações nativas se comunicarem com máquinas IPv4 e suas aplicações, ou vice-versa [TSI 00]. Ele possui uma combinação de tradução de cabeçalho e conversão de endereço. A tradução do cabeçalho é necessária para converter o cabeçalho IPv4 no formato do cabeçalho IPv6 e vice-versa. O resultado é um novo cabeçalho, que é semanticamente equivalente ao cabeçalho original, porém não é igual. A conversão do endereço é útil para máquinas da rede IPv4 saberem identificar as máquinas da rede IPv6, através de endereços de sua própria rede, sendo que o contrário também ocorre. NAT-PT usa um conjunto de endereços, que são dinamicamente designados para datagramas traduzidos. A Figura 6.5 ilustra este mecanismo.

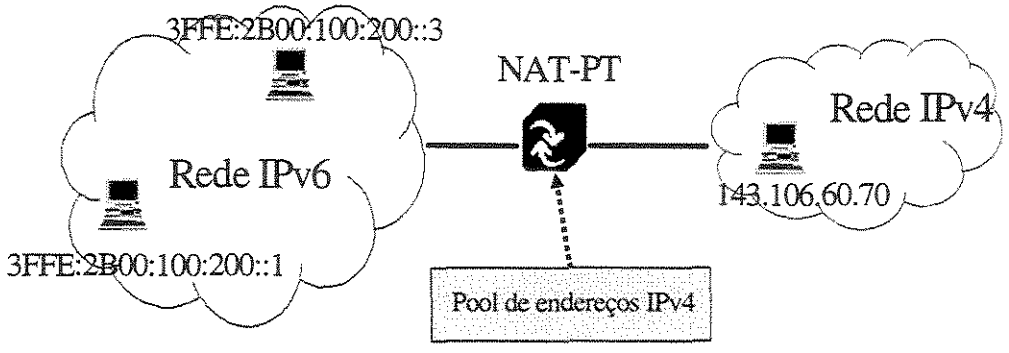


Figura 6.5: NAT-PT.

6.3.3 NAPT-PT *(Network Address Port Translation and Packet Translation)*

Este serviço permite que máquinas IPv6 se comuniquem com máquinas IPv4 transparentemente usando um único endereço IPv4 e vice-versa [TSI 00]. As portas TCP/UDP das máquinas IPv6 são traduzidos em porta TCP/UDP de endereços IPv4 registrados.

A desvantagem do NAT-PT é ter um conjunto de endereços IPv4, que pode ser exaurido, de modo que novas máquinas IPv6 não possam estabelecer novas conexões com a Internet enquanto o conjunto de endereços estiver completamente alocado para outras máquinas.

No entanto, NAPT-PT permite um número máximo de 63K de sessões de TCP e 63K de sessões UDP por endereço IPv4, antes de não ter mais portas para designar.

6.3.4 BIS *(Bump in the Stack)*

É um mecanismo de tradução, similar ao NAT-PT combinado com o SIIT e, implementado na pilha de protocolos do sistema operacional dentro de cada máquina [TSU 00]. Ele assume que a infra-estrutura da rede é IPv6. Enquanto SIIT é uma interface de tradução entre redes IPv6 e IPv4, BIS é uma interface de tradução entre aplicações IPv4 e redes IPv6. O projeto de pilha da máquina, que implementa este mecanismo, é baseado na pilha dupla, com a adição de três módulos (Figura 6.6):

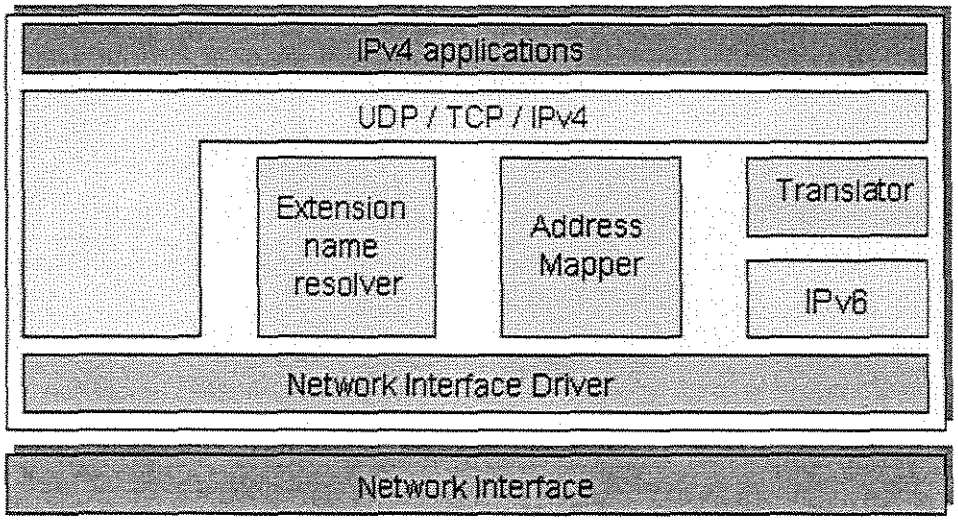


Figura 6.6: BIS.

- *translator*: traduz cabeçalhos IPv4 saintes em cabeçalhos IPv6 e cabeçalhos entrantes IPv6 em cabeçalhos IPv4;
- *extension name resolver*: monitora as perguntas IPv4 de DNS, com o objetivo de criar novas perguntas para resolver registros A e AAAA, enviando o registro A retornado para a aplicação IPv4. Se apenas o registro AAAA é retornado, o resolver pede ao *address mapper* para designar um endereço IPv4 correspondente ao endereço IPv6;
- *address mapper*: mantém um pool de endereços IPv4 e as associações entre endereços IPv4 e IPv6. Ele designará um endereço quando o translator receber um pacote IPv6 da rede para o qual não existe entrada mapeada para o endereço origem. Já que os endereços IPv4 nunca são transmitidos na rede, eles não precisam ser endereços válidos, podendo usar um pool de endereços privados.

As limitações deste mecanismo são: (1) permite comunicação de IPv4 para máquinas IPv6 porém não o contrário, já que não envia tampouco recebe pacotes IPv4 na rede; (2) mesmo que uma aplicação IPv4 tente se comunicar com outra aplicação IPv4 usando BIS, isto não será possível sem mecanismos adicionais de tradução em algum lugar entre as duas aplicações; (3) não funciona para comunicações *multicast*.

6.3.5 BIA *(Bump in the API)*

É um mecanismo similar ao BIS, porém, ao invés de traduzir cabeçalhos entre IPv4 e IPv6, BIA insere um tradutor API entre o *socket* API e os módulos TCP/IP da pilha da máquina [LEE 02]. Desta forma, as funções do *socket* API IPv4 são traduzidas em funções do *socket* API IPv6, e vice-versa. BIA também é baseado na adição de três módulos (Figura 6.7):

- *extension name resolver*: monitora as perguntas IPv4 de DNS, com o objetivo de criar novas perguntas para resolver registros A e AAAA, enviando o registro A retornado para a aplicação IPv4. Se apenas o registro AAAA é retornado, o resolver pede ao address mapper para designar um endereço IPv4 correspondente ao endereço IPv6;
- *function mapper*: mapeia chamadas de *socket* IPv4 em chamadas de *socket* IPv6 e vice-versa. Ele intercepta as chamadas de funções *socket* API IPv4 e invoca as correspondentes chamadas de funções *socket* API IPv6;

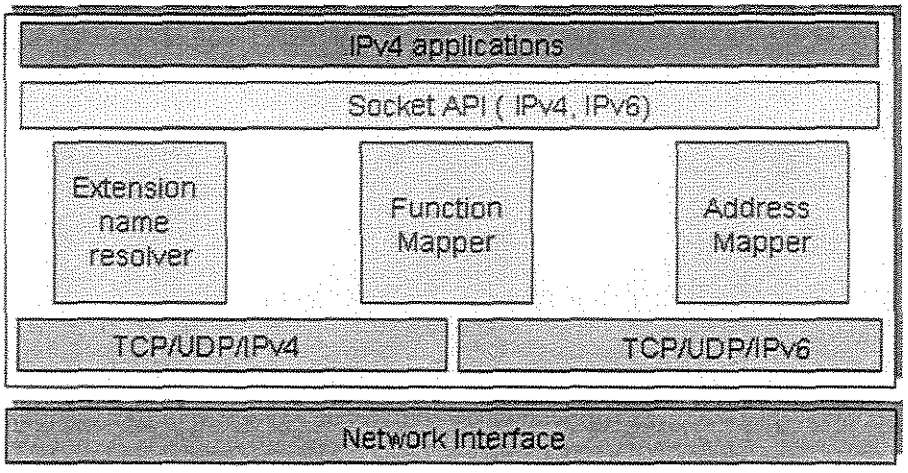


Figura 6.7: BIA.

- *address mapper*: mantém um pool de endereços IPv4 e as associações entre endereços IPv4 e IPv6. Ele designará um endereço quando o translator receber um pacote IPv6 da rede para o qual não existe entrada mapeada para o endereço origem. Já que os endereços IPv4 nunca são transmitidos na rede, eles não precisam ser endereços válidos, podendo usar um pool de endereços privados.

O mecanismo BIA é desenvolvido para sistemas que tem uma pilha IPv6, contudo não tem aplicações que foram atualizadas para IPv6. As vantagens deste mecanismo sobre BIS são: (1) ser independente do driver da interface de rede e (2) não introduzir overhead na tradução dos cabeçalhos dos pacotes. Entretanto, ele apresenta limitações similares ao BIS, como não suporta comunicações *multicast*.

6.3.6 TRT

Um tradutor localizado na camada de transporte é chamado de *transport relay translator*. Ele permite que máquinas *IPv6-only* troquem tráfego (TCP ou UDP) com máquinas *IPv4-only*. Modificações nas máquinas não são exigidas. Um TRT, que roda em uma máquina pilha dupla, pode usar um protocolo quando se comunicar com o cliente e usar outro protocolo quando se comunicar com o servidor da aplicação [HAG 01].

A tradução em TCP inclui recalcular o *checksum*, manter estado necessário sobre qual cliente está conectado com qual *socket* do servidor e remover este estado quando o cliente finalizar a

comunicação. A tradução em UDP inclui recalcular o *checksum* também, pois em IPv6 é obrigatório, porém em IPv4 é opcional. A Figura 6.8 ilustra este mecanismo.

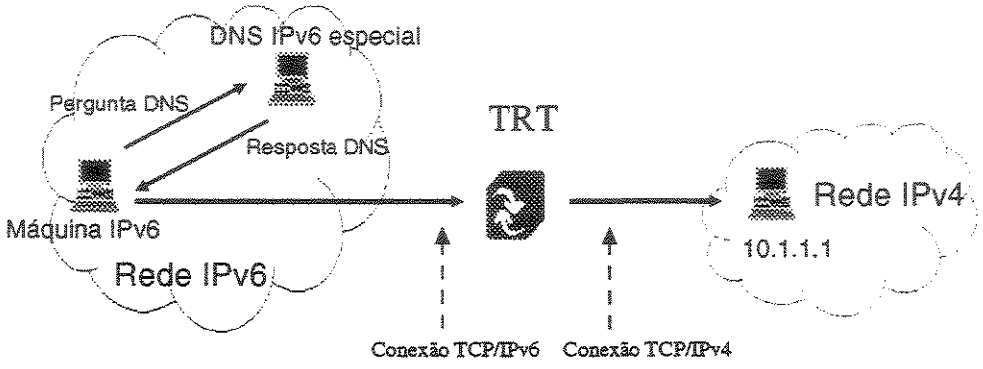


Figura 6.8: TRT.

6.3.7 *SOCKS*

É outro exemplo de um *transport relay*, porém este é usualmente referenciado como um protocolo *proxy* para ambiente cliente/servidor [KIT 01]. É um mecanismo que permite a duas máquinas, cliente e servidor, estabelecerem conexões TCP e UDP via um *proxy*, denominado *Socks Server*. Este *proxy* atua como um *relay* das conexões TCP e UDP.

Quando um cliente deseja se conectar a um servidor de aplicação, ele primeiro configura uma conexão com um bem conhecido e pré-configurado servidor *proxy*, usando um protocolo *proxy* especial. O cliente informa ao *proxy* o endereço IP e o número da porta do servidor de aplicação com quem ele deseja se comunicar. O servidor *proxy* agora é responsável por configurar uma conexão com o servidor de aplicação.

6.3.8 ALG *(Application Layer Gateway)*

É um mecanismo para permitir que usuários, atrás de *firewalls* ou de *gateway* NAT, usem aplicações, que de outro modo não seriam acessíveis. Um exemplo comum de um ALG é um *proxy* de HTTP, como o *squid* ou *wwwoffle*.

O cliente abre uma conexão com o ALG, que, então, estabelece uma conexão com o servidor, agindo como um retransmissor de requisições que saem e, de dados que entram. Em redes *IPv6-only*, a funcionalidade ALG pode ser usada para habilitar máquinas a estabelecer conexões com

serviços em redes IPv4. Isto pode ser obtido configurando ALG em máquinas pilha dupla com conectividade IPv4 e IPv6.

6.3.9 Classificação dos mecanismos de tradução

Os mecanismos de tradução, explicados anteriormente, podem ser distribuídos conforme segue abaixo:

- tradução (rede) - é o método de tradução, que ocorre na camada de rede. Os mecanismos, que fazem parte desta classe são SIIT, NAT-PT e NAPT-PT;
- tradução (transporte) - é o método de tradução, que ocorre na camada de transporte. Os mecanismos, que integram esta classe, são TRT e SOCKS;
- tradução (aplicação) - é o método de tradução, que ocorre na camada de aplicação. O mecanismo, que constitue esta classe, é o ALG;
- tradução (camada adicional) - é o método de tradução, que recebe a adição de uma nova camada na pilha de protocolos. Os mecanismos, que fazem parte desta classe, são BIS e BIA.

6.4 Cenários de comunicação entre redes IPv4 e IPv6

Nesta sub-seção, serão mostrados os vários cenários de comunicação entre redes IPv4 e IPv6, bem como os diversos mecanismos de transição aplicados a eles. O objetivo não é trazer uma lista exaustiva de cenários e sim ilustrar os cenários com maior probabilidade de ocorrência.

6.4.1 Comunicação entre redes IPv4

Neste primeiro cenário são mostradas duas redes IPv4 se comunicando através de redes de trânsito IPv4 e IPv6 (Figura 6.9). O fluxo de ida (1) não precisa de nenhum mecanismo de transição, pois além das redes usarem o protocolo IPv4, a rede de trânsito também usa o mesmo protocolo. O fluxo de volta (2) também não precisa de nenhum mecanismo de transição. Contudo, nos fluxos (3) e (4) é necessário usar algum mecanismo de transição, já que a rede de trânsito usa um protocolo diferente do protocolo das redes envolvidas na comunicação. Os mecanismos a serem usados neste cenário são mostrados na Figura 6.1.

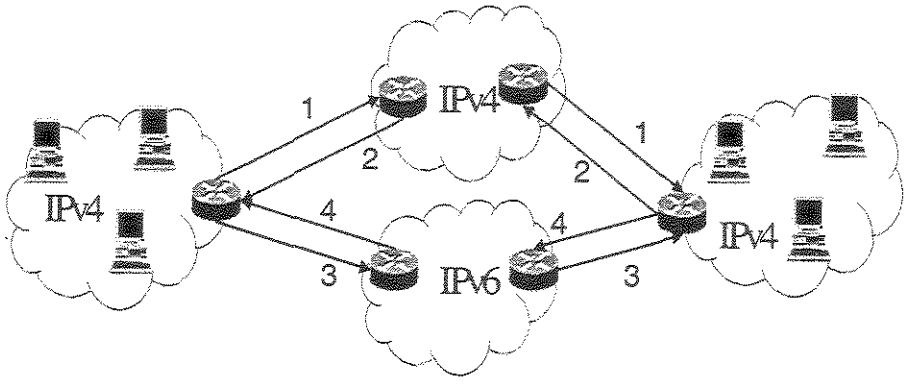


Figura 6.9: Comunicação entre redes IPv4.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv4	IPv4	Não precisa de nenhum mecanismo de transição [1]	Não precisa de nenhum mecanismo de transição [2]
IPv4	IPv4	IPv6	IPv4	IPv4	Tradução (rede, transporte ou aplicação) ou tunelamento 4to6 [3]	Tradução (rede, transporte ou aplicação) ou tunelamento 4to6 [4]

Tabela 6.1: Mecanismos aplicáveis na comunicação entre redes IPv4.

6.4.2 Comunicação entre redes IPv6

Neste segundo cenário é mostrado duas redes IPv6 se comunicando através de redes de trânsito IPv4 e IPv6 (Figura 6.10). Observa-se que esta situação é oposta a do primeiro cenário, já que nos fluxos (3) e (4) não é necessário usar nenhum mecanismos de transição, considerando que todas as redes envolvidas na comunicação utilizam o mesmo protocolo de rede, no caso o IPv6. Os mecanismos a serem usados neste cenário são mostrados na Figura 6.2.

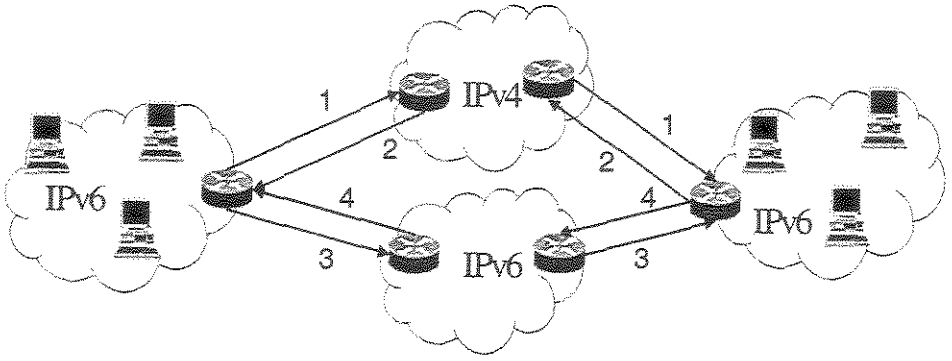


Figura 6.10: Comunicação entre redes IPv6.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv6	IPv6	IPv4	IPv6	IPv6	Tradução (rede, transporte ou aplicação) ou tunelamento (6to4, interno ou IPv6-over-IPv4) [1]	Tradução (rede, transporte ou aplicação) ou tunelamento (6to4, interno ou IPv6-over-IPv4) [2]
IPv6	IPv6	IPv6	IPv6	IPv6	Não precisa de nenhum mecanismo de transição [3]	Não precisa de nenhum mecanismo de transição [4]

Tabela 6.2: Mecanismos aplicáveis na comunicação entre redes IPv6.

6.4.3 Comunicação entre redes IPv4 e IPv6

Neste terceiro cenário é mostrado uma rede IPv4 se comunicando com uma rede IPv6, através de redes de trânsito IPv4 e IPv6 (Figura 6.11). É interessante notar que os fluxos (1), (2), (3) e (4) precisam de mecanismos de transição, que são mostrados na Figura 6.3, em razão da comunicação ocorrer entre redes que usam protocolos distintos.

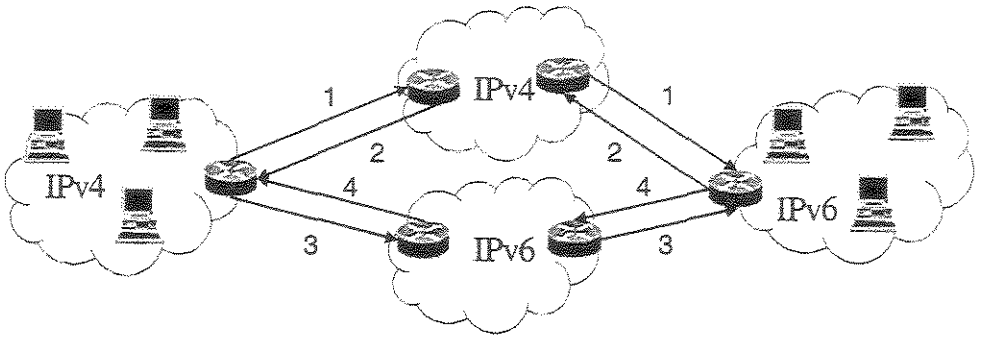


Figura 6.11: Comunicação entre redes IPv4 e IPv6.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv6	IPv6	Tradução (rede, transporte ou aplicação) ou tunelamento via servidor (origem IPv4) [1]	Tradução (rede, transporte ou aplicação) [2]
IPv4	IPv4	IPv6	IPv6	IPv6	Tradução (rede, transporte ou aplicação) ou tunelamento via servidor (origem IPv4) [3]	Tradução (rede, transporte ou aplicação) [4]

Tabela 6.3: Mecanismos aplicáveis na comunicação entre redes IPv4 e IPv6.

6.4.4 Comunicação entre redes IPv4 e IPv6 (aplicação IPv4)

Este quarto cenário mostra uma rede IPv4 se comunicando com uma rede IPv6, através de redes de trânsito IPv4 ou IPv6 (Figura 6.12). Aparentemente, nada de novo em relação ao cenário anterior, porém, a aplicação IPv4, que roda na rede IPv6, ainda não foi migrada para IPv6, o que demanda a utilização de mecanismos específicos para esta situação, conforme mostra a Figura 6.4. A aplicação que roda na máquina é IPv4, no entanto, o pacote que sai da máquina é IPv6.

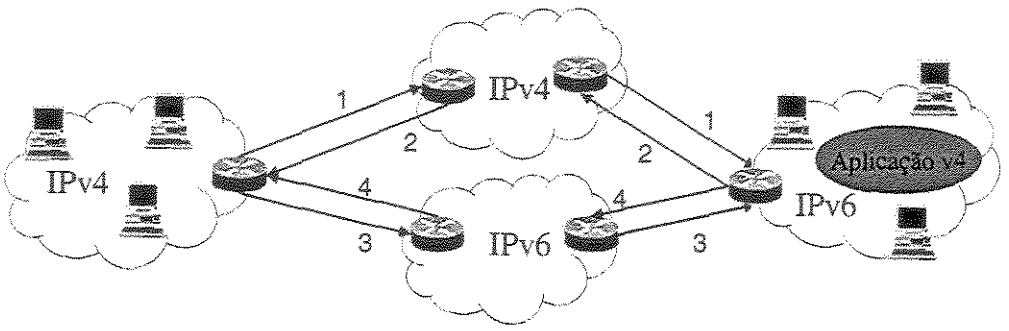


Figura 6.12: Comunicação entre redes IPv4 e IPv6 (aplicação IPv4).

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv4	IPv4	IPv6	IPv4	Tradução (ca) combinada com: - tunelamento via servidor (origem IPv4) ou - tradução (rede, transporte ou aplicação) [1]	Tunelamento via servidor (origem IPv6) [2]
IPv4	IPv4	IPv6	IPv6	IPv4	Tradução (ca) combinada com: - tunelamento via servidor (origem IPv4) ou - tradução (rede, transporte ou aplicação) [3]	Tunelamento via servidor (origem IPv6) [4]

Tabela 6.4: Mecanismos aplicáveis na comunicação entre redes IPv4 e IPv6 (aplicação IPv4).

6.4.5 Comunicação entre redes IPv6 (aplicação origem IPv4)

Este quinto cenário mostra duas redes IPv6 se comunicando, através de redes de trânsito IPv4 ou IPv6 (Figura 6.13). A particularidade deste cenário é ter uma aplicação IPv4 rodando em uma das redes IPv6. Os mecanismos aplicáveis são mostrados na Figura 6.5. Vale a mesma observação

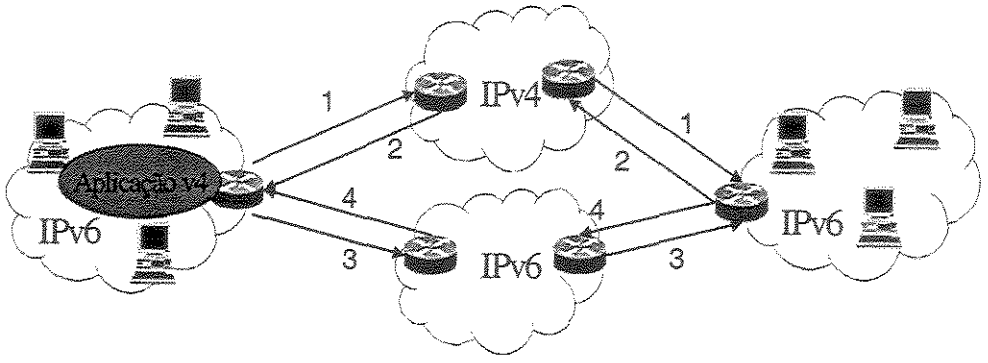


Figura 6.13: Comunicação entre redes IPv6 (aplicação origem IPv4).

anterior: a aplicação que roda na máquina é IPv4, no entanto, o pacote que sai da máquina é IPv6.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv6	IPv4	IPv6	IPv6	Tradução (ca) combinada com: - tunelamento (6to4 ou IPv6-over-IPv4) ou - tradução (rede, transporte ou aplicação) [1]	Tradução (ca) combinada com: - tunelamento (6to4 ou IPv6-over-IPv4) ou - tradução (rede, transporte ou aplicação) [2]
IPv4	IPv6	IPv6	IPv6	IPv6	Tradução (ca) [3]	Tradução (ca) [4]

Tabela 6.5: Mecanismos aplicáveis na comunicação entre redes IPv6 (aplicação origem IPv4).

6.4.6 Comunicação entre aplicações IPv4 em redes IPv6

No último cenário é mostrado duas redes IPv6 se comunicando, através de redes de trânsito IPv4 ou IPv6 (Figura 6.14), no entanto, as duas redes têm aplicações IPv4 que ainda não foram migradas para IPv6. Os mecanismos de transição aplicáveis a este cenário são mostrados na Figura 6.6.

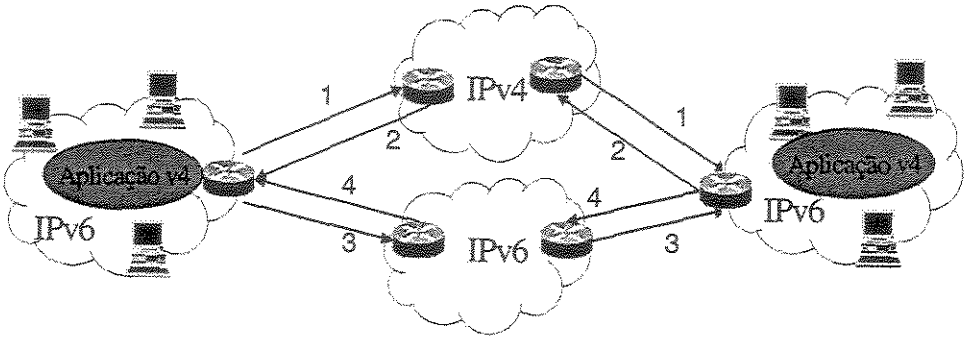


Figura 6.14: Comunicação entre aplicações IPv4 em redes IPv6.

Aplicação Origem	Pacote Origem	Rede Trânsito	Pacote Destino	Aplicação Destino	Método Ida	Método Volta
IPv4	IPv6	IPv4	IPv6	IPv4	Tradução (ca) combinada com: - tunelamento (6to4 ou IPv6-over-IPv4) ou - tradução (rede, transporte ou aplicação) [1]	Tradução (ca) combinada com: - tunelamento (6to4 ou IPv6-over-IPv4) ou - tradução (rede, transporte ou aplicação) [2]
IPv4	IPv6	IPv6	IPv6	IPv4	Tradução (ca) [3]	Tradução (ca) [4]

Tabela 6.6: Mecanismos aplicáveis na comunicação entre aplicações IPv4 em redes IPv6.

6.5 Suporte aos mecanismos de transição

A especificação técnica dos vários mecanismos de transição é tão importante quanto as diversas plataformas existentes suportarem estes mecanismos. Com mais de três anos de desenvolvimento e integração, quase todos os sistemas operacionais suportam mecanismos de transição. A Figura 6.7 mostra uma lista não-exaustiva de plataformas e os mecanismos suportados por cada uma delas, uma lista mais detalhada de implementações é encontrado em [IPV 02]. Os sistemas operacionais Linux usam a pilha IPv6/IPSec do Projeto KAME [KAM 98]. Enquanto, os sistemas operacionais BSD usam a pilha IPv6/IPSec do Projeto USAGI [USA 00].

	Plataformas					
Mecanismos de Transição	Windows XP	Solaris 9.0	HP-UX 11i	Linux (Debian e Red Hat)	BSDs (Free, Open e Net)	Status
Pilha Dupla	yes	yes	yes	yes	yes	RFC2893
Túnel Manual	yes	yes	yes	yes	yes	RFC2893
6over4	yes	no	no	yes	yes	RFC2529
6to4	yes	yes	yes	yes	yes	RFC3056
ISATAP	yes	no	no	experimental	experimental	draft-ietf-ngtrans-isatap-04.txt
Teredo	yes	no	no	no	no	draft-huitema-v6ops-teredo-00.txt
NAT-PT	no	no	no	experimental	experimental	RFC2766
BIA/BIS	no	no	no	no	no	RFC3338/RFC2767
TRT	no	no	no	yes	yes	RFC3142

Tabela 6.7: Plataformas e seus Mecanismos de Transição Suportados.

6.6 Conclusão

A migração de uma rede IPv4 para IPv6 pode ocorrer passo a passo, começando com uma única máquina ou uma sub-rede, ou ainda, com a rede inteira da organização. A integração das máquinas migradas IPv6 com o restante das máquinas IPv4, da Internet ou da rede da organização, é possível com os vários mecanismos de transição.

Esta parte do trabalho apresentou uma compilação detalhada dos diversos mecanismos de transição que permitem a interoperabilidade entre IPv4 e IPv6, considerando que a coexistência entre os dois protocolos ocorrerá durante vários anos. Além disto, forneceu um estudo completo dos cenários de transição com maior probabilidade de ocorrência, bem como dos mecanismos de transição aplicáveis a cada cenário. Este estudo objetiva fornecer subsídios para qualquer organização mapear seu cenário e escolher adequadamente seus mecanismos de transição.

Dentre as três técnicas apresentadas: pilha dupla, tunelamento e tradução, a mais interessante é a pilha dupla, já que é fácil de usar e flexível. Contudo, recomenda-se que ela seja utilizada somente em uma rede interna controlada por uma organização. Agora, quando a organização precisa interagir com outras redes IPv6 na Internet, não é possível garantir que as redes intermediárias ou *backbones* usem IPv6. Neste caso, a técnica mais interessante é o tunelamento, pois

permite que o tráfego IPv6 se beneficie da infraestrutura de conectividade e roteamento, em funcionamento, de IPv4.

Recomenda-se a combinação das duas técnicas em um cenário de transição, pilha dupla internamente na rede e tunelamento na borda da rede, de modo que, este cenário aproveitará as vantagens das duas técnicas, sendo fácil de implementar e independente das redes externas.

A técnica tradução apresenta como vantagem permitir que máquinas IPv6 se comuniquem diretamente com máquinas IPv4, porém as desvantagens são: não suporta características avançadas de IPv6 como segurança fim-a-fim; impõe limitações à topologia da rede, pois as respostas de qualquer mensagem enviada pelo roteador de tradução devem retornar para o mesmo roteador de tradução, além do roteador de tradução ser um ponto único de falha. Em razão destas desvantagens, esta técnica não é recomendável, ou melhor, deve ser usada apenas quando nenhuma outra técnica for possível e deve ser vista como uma solução temporária até outra qualquer ser implementada.

Capítulo 7

Conclusão

O IPv4, versão atual do protocolo IP, não antecipou e, conseqüentemente, não contempla as necessidades atuais da Internet. O problema mais evidente é o crescimento exponencial da Internet e resultante ameaça de exaustão do espaço de endereçamento IPv4. Logo, técnicas como NAT e CIDR foram desenvolvidas para resolver paliativamente este problema.

Aliado ao problema de endereçamento IP, a necessidade de configuração simplificada, a ausência de mecanimos de segurança mais robustos e a necessidade de suporte melhorado para entrega de dados em tempo-real estimularam a *Internet Engineering Task Force* (IETF) a desenvolver um conjunto de protocolos e padrões conhecido como IP versão 6 (IPv6). É interessante observar que o projeto de IPv6 objetiva causar o mínimo impacto nos protocolos das camadas acima e abaixo do modelo TCP/IP, eliminando a adição aleatória de novas características. Além de suportar um espaço de endereçamento de 128 bits e conter uma estrutura mais simples e eficiente, o IPSec foi incluído como parte integrante e obrigatória na sua estrutura.

Do ponto de vista lógico, este trabalho pode ser dividido em duas partes principais. A primeira parte (representada pelos Capítulos 2, 3, 4 e 5) está relacionada ao impacto da adoção de IPv6, principalmente de seu modelo de segurança IPSec, em um Ambiente Cooperativo Seguro.

Esta parte do trabalho caracterizou um Ambiente Cooperativo Seguro, acompanhando a evolução dos vários cenários de rede, e apresentou algumas tecnologias, técnicas e conceitos de segurança disponíveis, chegando ao conceito de *firewall cooperativo*. Logo a seguir, apresentou também os conceitos básicos relativos ao protocolo IPv6, analisando o impacto de sua implementação em ambientes que utilizam técnicas de segurança comuns atualmente. Após a verificação detalhada dos pontos de conflito entre o IPv6 e alguns mecanismos individualmente, uma

visão mais geral das conseqüências do emprego do IPv6 em diferentes cenários de utilização foi apresentada. Constata-se que, da implantação do IPv6, eclodem vários desafios técnicos no que concerne à sua interoperabilidade com as atuais ferramentas de segurança de redes.

O painel traçado nessa parte do trabalho pretende, dessa forma, ter fornecido parâmetros consistentes para que, amparado nas análises aqui empreendidas, se possa antecipar problemas e avaliar soluções relativas à integração de IPv6 em ambientes seguros, de acordo com as necessidades específicas de cada cenário.

A segunda parte lógica do trabalho, representada pelo Capítulo 6, é um estudo sobre a coexistência de uma rede IPv4 migrada para IPv6 com outras redes, que tanto podem ser IPv4 ou IPv6. Esta necessidade existe em função dos cabeçalhos IPv4 e IPv6 não serem interoperáveis entre si, o que implica que um roteador ou máquina precisa implementar ambos os protocolos para conseguir reconhecer e processar seus cabeçalhos. Desta forma, vários mecanismos de transição foram desenvolvidos para permitir a coexistência tranqüila entre redes que se utilizam de protocolos distintos.

Uma rede IPv4 migrada para IPv6 precisa ser integrada com as ferramentas de segurança já consolidadas nos Ambientes Cooperativos Seguros, visto que seu *framework* de segurança IPSec não resolve todos os problemas de segurança existentes na Internet. Além disto, esta rede migrada IPv6 precisa continuar se comunicando com outras redes IPv6 ou IPv4 na Internet, o que torna essencial conhecer os mecanismos de transição e seus possíveis cenários de aplicação.

Este trabalho teve como contribuições gerais:

- estudo dos impactos do novo protocolo: impactos de integração de IPv6 em um Ambiente Cooperativo Seguro, considerando que a migração das ferramentas deve acompanhar a migração dos protocolos de rede;
- identificação de possíveis problemas e limitações: buscamos identificar os problemas advindos da característica de criptografia fim-a-fim do *framework* de segurança IPSec com as várias ferramentas de segurança já consolidadas;
- definição de estratégias de adoção do novo protocolo: a rede analisada já possui suporte a IPv6, porém são apresentadas várias técnicas de transição, que permitem uma adoção suave do novo protocolo em outras redes que não possuem suporte a IPv6;
- criação de cultura a respeito da utilização do protocolo: através da divulgação e da apresentação de minicursos [SAN 03b] sobre o protocolo.

7.1 Trabalhos futuros

A continuidade deste trabalho envolve o desenvolvimento de uma metodologia de migração, que estabeleça critérios bem definidos para a ocorrência da migração, tanto no nível de conectividade da rede como da adaptação das aplicações cooperativas. Esta metodologia pode seguir as orientações do *draft* [LIN 03] e das publicações do Projeto 6NET [PRO 02].

Um trabalho vislumbrado é a definição de um novo mecanismo de transição baseado em máquinas virtuais, com aplicação em dois cenários definidos: (1) rede IPv4 com uma aplicação crítica e tentativa de adquirir experiência com o protocolo IPv6 sem comprometer o estado da rede atual e (2) rede IPv6 migrada com uma aplicação proprietária, que ainda não migrou para IPv6, precisa de uma rede paralela para rodar exclusivamente esta aplicação. Este mecanismo é baseado na idéia da criação de uma rede paralela à nativa e que rode um protocolo diferente ao da rede nativa.

Outra sugestão para pesquisa futura seria estudar o *draft* do SEND e pesquisar soluções para o problema do *spoofing* de um roteador legítimo, já que o SEND assegura somente que o roteador ou nó vizinho pertence ao conjunto de entidades confiáveis e não que ele seja quem diz.

Seguindo a linha de pesquisa de mecanismos de auto-configuração, outro trabalho interessante a ser pesquisado é sobre como um nó pode conseguir informação do servidor DNS. O nó poderia conseguir informações de DNS de um servidor DHCPv6, contudo o método de auto-configuração *stateless* se tornou mais popular que o DHCPv6, o que implica na obtenção das mesmas informações por outros métodos. Existem vários métodos propostos, porém todos têm vantagens e desvantagens, o que torna difícil a tarefa de escolha.

Outro trabalho seria estudar o DNSSec com o objetivo de propor soluções para integração de IPSec e DNSSec. DNSSec poderia ser um substituto à altura de uma PKI, no que concerne às informações criptográficas necessárias para o funcionamento do IPSec.

Outra sugestão para pesquisa posterior seria criar uma ferramenta para aplicação prática do conhecimento reunido neste trabalho, cujo objetivo será possibilitar o mapeamento de redes de organizações nos cenários apresentados e a análise, de forma automática, destes cenários para determinar os mecanismos de transição a serem utilizados.

Bibliografia

[ABO 03] ABOBA, B.; DIXON, W. IPSEC Working Group. Internet Draft. *IPSec-NAT Compatibility Requirements*. October 20, 2003. http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-reqts-06.txt

[ADA 99] ADAMS, C.; LLOYD, S. *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*. New Riders Publishing. 1999.

[APN 93] APNIC - Asia Pacific Network Information Centre. http://www.apnic.net. 30/01/04.

[APP 03] APPLE Computer. Developer Connection for Mac OS X. http://developer.apple.com/macosx. 30/01/04.

[ARI 97] ARIN - American Registry for Internet Numbers. http://www.arin.net. 30/01/04.

[ARK 02a] ARKKO, J. Network Working Group. Internet Draft. *Effects of ICMPv6 on IKE and IPSec Policies*. June 23, 2002. http://www.rnp.br/ietf/internet-drafts/draft-arkko-icmpv6-ike-effects-01.txt

[ARK 02b] ARKKO, J; NIKANDER, PEKKA; KIVINEN, TERO. Network Working Group. Internet Draft. *Manual SA Configuration for IPv6 Link Local Messages*. June 23, 2002. http://archive.cert.uni-stuttgart.de/in-drafts/draft-arkko-manual-icmpv6-sas-01.txt

[ARK 04] ARKKO, J; KEMPF, J.; SOMMERFELD, B.; ZILL, B.; NIKANDER, P. Secure Neighbor Discovery Working Group. Internet Draft. *SEcure Neighbor Discovery (SEND)*. January 24, 2004. http://www.ietf.org/internet-drafts/draft-ietf-send-ndopt-03.txt

[AUR 03] AURA, T. Secure Neighbor Discovery Working Group. Internet Draft. *Cryptografhically Generated Addresses (CGA)*. December 2003. http://www.ietf.org/internet-drafts/draft-ietf-send-cga-04.txt

[BEL 99] BELLOVIN, S. M. *Distributed Firewalls*. ;login: magazine, special issue on security, 1999.

[BHA 01] BHANSALI, B. B. SANS Institute. GIAC practical repository. *Man-In-the-Middle Attack - A Brief.* February 16, 2001. 30/01/04. http://www.giac.org/practical/gsec/Bhavin_Bhansali_GSEC.pdf

[BLA 99] BLAZE, M.; FEIGENBAUM, J.; IOANNIDIS, J.; KEROMYTIS, A. Network Working Group. Request for Comments 2704. *The KeyNote Trust-Management System Version 2.* September 1999. http://www.ietf.org/rfc/rfc2704.txt

[BLA 02] BLANCHET, M. NGTRANS Working Group. Internet Draft. *DSTM IPv4 over IPv6 tunnel profile for Tunnel Setup Protocol (TSP).* February 22, 2002. http://www.viagenie.qc.ca/en/ipv6/ietf/draft-blanchet-ngtrans-tsp-dstm-profile-00.txt

[BOU 01] BOUND, J.; TOUTAIN, L.; DUPONT, F.; MEDINA, O.; AFIFI, H.; DURAND, A. NGTRANS Working Group. Internet Draft. *Dual Stack Transition Mechanism (DSTM).* November 2001. http://www.ietf.org/proceedings/01dec/I-D/draft-ietf-ngtrans-dstm-05.txt

[CAR 03] CARNUT, M. A.; GONDIM, J. J. C. Artigo submetido ao SSI-2003 – Simpósio sobre Segurança em Informática 2003. *ARP Spoofing Detection on Switched Ethernet Networks: a Feasibility Study.* Novembro, 2003.

[CAR 01] CARPENTER, B.; MOORE, K. Network Working Group. Request for Comments 3056. *Connection of IPv6 Domains via IPv4 Clouds.* February 2001. http://www.ietf.org/rfc/rfc3056.txt

[CAR 99] CARPENTER, B.; JUNG, C. Network Working Group. Request for Comments 2529. *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.* March 1999. http://www.ietf.org/rfc/rfc2529.txt

[CHA 00] CHAPMAN, D. Brent.; ZWICHY, Elizabeth D.; COOPER, S. *Building Internet Firewalls.* Second Edition. O'Reilly & Associates, Inc. 2000.

[CHE 94] CHESWICK, William R.; BELLOVIN, Steven M. *Repelling the Wily Hacker.* Addison-Wesley. 1994, April.

[COM 95] Comitê Gestor da Internet no Brasil. http://www.cg.org.br. 30/01/04.

[CON 98] CONTA, A.; DEERING, S. Network Working Group. Request for Comments 2463. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.* December 1998. http://www.ietf.org/rfc/rfc2463.txt

[DEE 98] DEERING, S.; HINDEN, R. Network Working Group. Request for Comments 2460. *Internet Protocol, Version 6 (IPv6), Specification.* December 1998. http://

www.ietf.org/rfc/rfc2460.txt

[DRO 03] DROMS, R.; BOUND, J.; VOLZ, B.; LEMON, T.; PERKINS, C.; CARNEY, M. Network Working Group. Request for Comments 3315. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* July 2003. http://www.ietf.org/rfc/rfc3315.txt

[DUR 01] DURAND, A.; FASANO, P.; GUARDINI, I.; LENTO, D. Network Working Group. Request for Comments 3053. *IPv6 Tunnel Broker.* January 2001. http://www.ietf.org/rfc/rfc3053.txt

[EAS 04] EASTLACK, D. E. Internet Protocol Security Working Group. Internet Draft. *Cryptographic Algorithm Implementation Requirements for ESP and AH.* January 2004. http://www.ietf.org/internet-drafts/draft-ietf-ipsec-esp-ah-algorithms-01.txt

[FEN 97] FENNER, W. Network Working Group. Request for Comments 2236. *Internet Group Management Protocol, Version 2.* November 1997. http://www.ietf.org/rfc/rfc2236.txt

[FRA 01] FRANKEL, S. *Desmystifying the IPSec Puzzle.* Artech House. 2001.

[FRA 03a] FRANKEL, S.; HERBERT, H. Network Working Group. Request for Comments 3566. *The AES-XCBC-MAC-96 Algorithm and Its Use With IPSec.* September 2003. http://www.ietf.org/rfc/rfc3566.txt

[FRA 03b] FRANKEL, S.; GLENN, R.; KELLY, S. Network Working Group. Request for Comments 3602. *The AES-CBC Cipher Algorithm and Its Use With IPSec.* September 2003. http://www.ietf.org/rfc/rfc3602.txt

[GIL 00] GILLIGAN, R.; NORDMARK, E. Network Working Group. Request for Comments 2893. *Transition Mechanisms for IPv6 Hosts and Routers.* August 2000. http://www.ietf.org/rfc/rfc2893.txt

[GLE 98] GLENN, R.; KENT, S. Network Working Group. Request for Comments 2410. *The NULL Encryption Algorithm and Its Use With IPSec.* November 1998. http://www.ietf.org/rfc/rfc2410.txt

[GUL 01] GULKER, C. *The Kevin Mitnick/Tsutomu Shimomura Affair.* September 2001. http://www.gulker.com/ra/hack

[HAB 03] HABERMAN, B. Network Working Group. Request for Comments 3590. *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol.* September 2003. http://www.ietf.org/rfc/rfc3590.txt

[HAG 01] HAGINO, J.; YAMAMOTO, K. Network Working Group. Request for Comments 3142. *An IPv6-to-IPv4 Transport Relay Translator*. June 2001. http://www.ietf.org/rfc/rfc3142.txt

[HAG 02] HAGEN, S. *IPv6 Essencials*. O'Reilly. 2002, July.

[HAR 98] HARKINS, D.; CARREL, D. Network Working Group. Request for Comments 2409. *The Internet Key Exchange (IKE)*. November 1998. http://www.ietf.org/rfc/rfc2409.txt

[HIN 98a] HINDEN, R.; FINK, R.; POSTEL, J. Network Working Group. Request for Comments 2471. *IPv6 Testing Address Allocation*. December 1998. http://www.ietf.org/rfc/rfc2471.txt

[HIN 98b] HINDEN, R.; DEERING, S. Network Working Group. Request for Comments 2375. *IPv6 Multicast Address Assignments*. July 1998. http://www.ietf.org/rfc/rfc2375.txt

[HIN 03a] HINDEN, R.; DEERING, S. Network Working Group. Request for Comments 3513. *Internet Protocol Version 6 (IPv6) Addressing Architecture*. April 2003. http://www.ietf.org/rfc/rfc3513.txt

[HIN 03b] HINDEN, R.; DEERING, S.; NORDMARK, E. Network Working Group. Request for Comments 3587. *IPv6 Global Unicast Address Format*. August 2003. http://www.ietf.org/rfc/rfc3587.txt

[HOU 03] HOUSLEY, R. Internet Protocol Security Working Group. Internet Draft. *Using AES Counter Mode With IPSec ESP*. July 2003. http://www.rnp.br/ietf/internet-draft/draft-ietf-ipsec-ciph-aes-ctr-05.txt

[HUI 01] HUITEMA, C. Network Working Group. Request for Comments 3068. *An Anycast Prefix for 6to4 Relay Routers*. June 2001. http://www.ietf.org/rfc/rfc3068.txt

[HUI 02] HUITEMA, C. NGTRANS Working Group. Internet Draft. *Teredo: Tunneling IPv6 over UDP through NATs* . February 19, 2002. http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-ngtrans-shipworm-05.txt

[HUI 98] HUITEMA, C. *IPv6: The New Internet Protocol*. Prentice Hall PTR. 1998, January.

[HUT 03] HUTTUNEN, A.; SWANDER, B.; STENBERG, M.; VOLPE, V.; DIBURRO, L. IPSEC Working Group. Internet Draft. *UDP Encapsulation of PSec Packets*. October 2003. http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-07.txt

[IAN 03] IANA - Internet Assigned Numbers Authority. http://www.iana.org. 30/01/04.

[IET 86] IETF - Internet Engineering Task Force. http://www.ietf.org. 30/01/04.

[IOA 00] IOANNIDIS, S.; KEROMYTIS, A. D.; BELLOVIN, S. M.; SMITH, J. M. ACM Conference on Computer and Communications Security. *Implementing a Distributed Firewall.* Athens, Greece: ACM, 2000.

[IPV 03] IPv6 Operations Working Group (v6ops). http://www.ietf.org/html.charters/v6ops-charter.html. 30/01/04.

[IPV 02] IPv6 Implementations. http://playground.sun.com/ipv6/ipng-implementations.html. 30/01/04.

[IPV 99] IPv6 Forum. http://www.ipv6forum.com. 30/01/04.

[JOH 03] JOHNSON, D.; PERKINS, C.; ARKKO, J. IETF Mobile IP Working Group. Internet Draft. *Mobility Support in IPv6.* June 2003. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-24.txt

[KAM 98] KAME Project. http://www.kame.net. 30/01/04.

[KEN 98] KENT, S.; ATKINSON, R. Network Working Group. Request for Comments 2401. *Security Architecture for the Internet Protocol.* November 1998. http://www.ietf.org/rfc/rfc2401.txt

[KIT 01] KITAMURA, H. Network Working Group. Request for Comments 3089. *A SOCKS-based IPv6/IPv4 Gateway Mechanism.* April 2001. http://www.ietf.org/rfc/rfc3089.txt

[KOS 98] KOSIUR, D. *Building and Managing Virtual Private Networks.* John Wiley & Sons, Inc. 1998.

[KRA 96] KRAWCZYK, H. IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security. *SKEME: A Versatile Secure Key Exchange Mechanism for Internet.* IEEE, 1996.

[LAB 04] Laboratório de Administração e Segurança. http://www.las.ic.unicamp.br. 30/01/04.

[LAC 02] LACNIC. http://www.lacnic.net. 30/01/04.

[LEE 02] LEE, S.; SHIN, M-K.; KIM, Y-J.; NORDMARK, E.; DURAND, A. Network Working Group. Request for Comments 3338. *Dual Stack Hosts using "Bump-In-the-API" (BIA).* October 2002. http://www.ietf.org/rfc/rfc3338.txt

[LIN 03] LIND, M.; KSINANT, V.; PARK, D.; BAUDOT, A. IPv6 Operations Working Group.

Internet Draft. *Scenarios and Analysis for Introducing IPv6 into ISP Networks.* December 2003. http://www.ietf.org/internet-drafts/draft-ietf-v6ops-isp-scenarios-analysis-00.txt

[MAD 98a] MADSON, C.; GLENN, R. Network Working Group. Request for Comments 2403. *The Use of HMAC-MD5-96 within ESP and AH.* November 1998. http://www.ietf.org/rfc/rfc2403.txt

[MAD 98b] MADSON, C.; GLENN, R. Network Working Group. Request for Comments 2404. *The Use of HMAC-SHA-1-96 within ESP and AH.* November 1998. http://www.ietf.org/rfc/rfc2404.txt

[MAD 98c] MADSON, C.; DORASWAMY, N. Network Working Group. Request for Comments 2405. *The ESP DES-CBC Cipher Algorithm with Explicit IV.* November 1998. http://www.ietf.org/rfc/rfc2405.txt

[MAT 02] MATHEW, D. SANS Institute. GSEC practical v1.4 b. *Choosing an Intrusion Detection System that Best Suits your Organization.* 2002. 30/01/04. http://www.sans.org/rr/papers/5/82.pdf

[MAU 98] MAUGHAN, D.; SCHERTLER, M.; SCHNEIDER, M.; TURNER, J. Network Working Group. Request for Comments 2408. *Internet Security Association and Key Management Protocol (ISAKMP).* November 1998. http://www.ietf.org/rfc/rfc2408.txt

[MCG 03a] MCGEHEE, B.; RICH, Y. *A Discussion on IPv6 Transition Mechanisms Part 1: From Dual Stack to 6to4 and ISATAP.* August 2003. 30/01/04. http://www.ipv6style.jp/en/building/20030820/index.shtml

[MCG 03b] MCGEHEE, B.; RICH, Y. *A Discussion on IPv6 Transition Mechanisms Part 2: Teredo, NAT-PT, BIS and MPLS.* August 2003. 30/01/04. http://www.ipv6style.jp/en/building/20030822/index.shtml

[MIC 75] Microsoft. http://www.microsoft.com. 30/01/04.

[NAR 98] NARTEN, T.; NORDMARK, E.; SIMPSON, W. Network Working Group. Request for Comments 2461. *Neighbor Discovery for IP Version 6 (IPv6).* December 1998. http://www.ietf.org/rfc/rfc2461.txt

[NAK 03] NAKAMURA, E. T.; GEUS, P. L. *Segurança de Redes em Ambientes Cooperativos.* Segunda Edição. Editora Futura. 2003.

[NIC 89] NIC-MX. http://www.nic.mx. 30/01/04.

[NIK 03] NIDANDER, P.; KEMPF, J.; NORDMARK, E. Secure Neighbor Discovery Working

Group. Internet Draft. *IPv6 Neighbor Discovery trust models and threats.* October 15, 2003. http://www.ietf.org/internet-drafts/draft-ietf-send-psreq-04.txt

[NOR 00] NORDMARK, E. Network Working Group. Request for Comments 2765. *Stateless IP/ ICMP Translation Algorithm (SIIT).* February 2000. http://www.ietf.org/rfc/ rfc2765.txt

[ORM 98] ORMAN, H. Network Working Group. Request for Comments 2412. *The OAKLEY Key Determination Protocol.* November 1998. http://www.ietf.org/rfc/rfc2412.txt

[PAR 93] PARTRIDGE, C.; MENDEZ, T.; MILLIKEN, W. Network Working Group. Request for Comments 1546. *Host Anycasting Service.* November 1993. http://www.ietf.org/rfc/ rfc1546.txt

[PER 98] PEREIRA, R.; ADAMS, R. Network Working Group. Request for Comments 2451. *The ESP CBC-Mode Cipher Algorithms.* November 1998. http://www.ietf.org/rfc/ rfc2451.txt

[PIP 98] PIPER, S. Network Working Group. Request for Comments 2407. *The Internet IP Security Domain of Interpretation for ISAKMP.* November 1998. http://www.ietf.org/ rfc/rfc2407.txt

[PRO 02] Project 6NET: Large-Scale International IPv6 Pilot Network. http://www.6net.org. 30/01/04.

[PRO 98] Project 6REN: IPv6 Research & Education Network. http://www.6ren.net. 30/01/04.

[PRO 00] Project 6BONE: Testbed for Deployment of IPv6. http://www.6bone.net. 30/01/04.

[RED 89] Rede Nacional de Ensino e Pesquisa (RNP). http://www.rnp.br. 30/01/04.

[REG 03] Registro.br. http://registro.br. 30/01/04.

[REI 03] REIS, M. A. Tese de Mestrado – Campinas : IC/UNICAMP. *Forense Computacional e sua aplicação em Segurança Imunológica.* Fevereiro, 2003.

[REK 95] REKHTER, Y.; LI, T. Network Working Group. Request for Comments 1887. *An Architecture for IPv6 Unicast Address Allocation.* December 1995. http://www.ietf.org/rfc/ rfc1887.txt

[REZ 02] REZENDE, E. R. S.; GEUS, P. L. Artigo submetido ao SSI-2002 – Simpósio sobre Segurança em Informática 2002. *Análise de Segurança dos Protocolos utilizados para Acesso Remoto VPN em Plataformas Windows.* Novembro, 2002.

[RIP 97] RIPE NCC - Réseaux IP Européens Network Coordination Centre. http://www.ripe.net. 30/01/04.

[SAN 03a] Sans Institute. *Intrusion Detection FAQ [Version 1.80].* June 13, 2003. 30/01/04. http://www.sans.org/resources/idfaq/index.php

[SAN 03b] SANTOS, C. R.; GEUS, P. L. Minicurso ministrado no SSI-2003 – Simpósio sobre Segurança em Informática 2003. *Integração de IPv6 em Ambientes Seguros.* Novembro, 2003.

[SCH 03] SCHILD, C.; STRAUF, T. Project 6NET. Deliverable D2.3.2. *Initial IPv4 to IPv6 transition cookbook for end site networks/universities.* February 2003. http://www.6net.org/publications

[SCO 98] SCOTT, C.; WOLFE, P.; ERWIN, M. *Virtual Private Networks.* Second Edition. O'Reilly and Associates, 1998.

[SEN 02] SENA, J. C. Tese de Mestrado – Campinas : IC/UNICAMP. *Um modelo para proteção do tráfego de serviços baseado em níveis de segurança.* Maio, 2002.

[SPI 03] SPITZNER, L. SecurityFocus. *Honeypots: Simple, Cost-Effective Detection* April 30, 2003. 30/01/04. http://www.securityfocus.com/infocus/1690

[SRI 01] SRISURESH, P.; EGEVANG, K. Network Working Group. Request for Comments 3022. *Tradicional IP Network Address Translator (Traditional NAT).* January 2001. http://www.ietf.org/rfc/rfc3022.txt

[STE 94] STEVENS, W. R. *TCP/IP Illustrated, Volume 1: The Protocolos.* Addison-Wesley professional computing series. 1994.

[TEM 02] TEMPLIN, F.; GLEESON, T.; TALWAR, M.; THALER, D. NGTRANS Working Group. Internet Draft. *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).* January 30, 2002. http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-ngtrans-isatap-03.txt

[THA 98] THAYER, R.; DORASWAMY, N.; GLENN, R. Network Working Group. Request for Comments 2411. *IP Security Document Roadmap.* November 1998. http://www.ietf.org/rfc/rfc2411.txt

[THE 03] The Honeynet Project. Scan of the Month. *Scan 28 - Italian blackhats break into a Solaris server then enable IPv6 tunneling for comunications.* May 30, 2003. 30/01/04. http://www.honeynet.org/scans/scan28

[THO 98] THOMSON, S.; NARTEN, T. Network Working Group. Request for Comments 2462. *IPv6 Stateless Address Autoconfiguration*. December 1998. http://www.ietf.org/rfc/rfc2462.txt

[TRI 03] TRIULZI, A. Proceedings of the Conference Security and Protection of Information 2003. *Intrusion Detection Systems and IPv6*. March 2003.

[TSI 00] TSIRTSIS, G.; SRISURESH, P. Network Working Group. Request for Comments 2766. *Network Address Translation - Protocol Translation (NAT-PT)*. February 2000. http://www.ietf.org/rfc/rfc2766.txt

[TSU 00] TSUCHIYA, K.; HIGUCHI, H.; ATARASHI, Y. Network Working Group. Request for Comments 2767. *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*. February 2000. http://www.ietf.org/rfc/rfc2767.txt

[USA 00] USAGI Project. http://www.linux-ipv6.org. 30/01/04.

Apêndice A

Configuração de IPv6 no Laboratório de Administração e Segurança (LAS)

Neste apêndice será apresentado o trabalho de configuração de IPv6 nas máquinas do Laboratório de Administração e Segurança (LAS) do Instituto de Computação (IC) da Unicamp [LAB 04].

A.1 Topologia da rede

O roteador gate6.ipv6.las.ic.unicamp.br (Figura A.1) tem o sistema operacional FreeBSD 4.8 [FRE 95] instalado com os pacotes de desenvolvedor - traz os códigos fontes do kernel - para que o kernel possa ser compilado. O FreeBSD 4.8 foi compilado com o kernel do Projeto KAME [KAM 98], que é um esforço unificado de seis empresas japonesas para prover uma pilha gratuita IPv6 e IPSec para variantes BSD no mundo. O roteador desempenha somente as funções de *firewall* e ponto inicial do túnel com a Rede Nacional de Pesquisa - RNP [RED 89]. Nele está rodando o IPFW - interface de linha de comando do IPFIREWALL -, que é o utilitário mais comum e popular para implementar a filtragem de pacotes IP e controle de tráfego no FreeBSD, após a compilação do kernel, já que ele inicialmente vem desabilitado a nível de kernel. No roteador está rodando também o IP6FW - interface de linha de comando do IPV6FIREWALL -, após a compilação do kernel pelas mesmas razões acima.

O servidor shadowfax.ipv6.las.ic.unicamp.br (Figura A.1) tem o sistema operacional Linux, distribuição Red Hat 9.0 [REDa 03], compilado com o kernel do Projeto USAGI (UniverSAl playGround for Ipv6) [USA 00]. Este projeto objetiva contribuir com a comunidade do Linux e

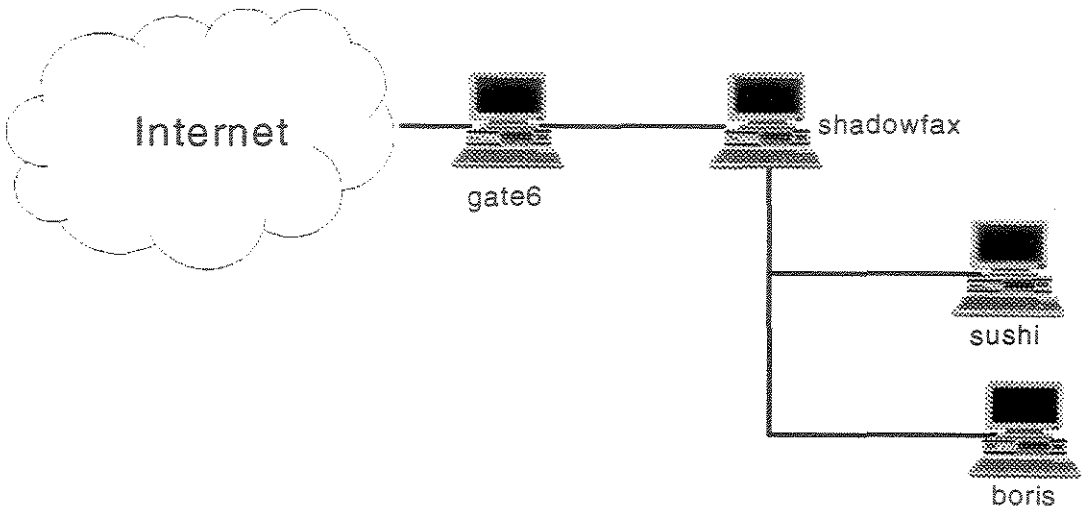


Figura A.1: Topologia da Rede IPv6 do Laboratório de Administração e Segurança.

de IPv6 através da produção, com qualidade, da pilha de protocolos IPv6 e IPSec para o sistema Linux.

As estações de trabalho, sushi.ipv6.las.ic.unicamp.br e boris.ipv6.las.ic.unicamp.br, foram instaladas na máquina shadowfax no sistema de máquinas virtuais VMware [VMW 98]. Elas também rodam Linux, distribuição Red Hat 9.0, contudo não foram compiladas, somente tiveram o módulo de IPv6 carregado na hora do boot.

A.2 Configuração FreeBSD 4.8

A.2.1 Compilar *kernel*

O kernel do FreeBSD foi compilado usando o kernel do KAME (ftp://ftp.kame.net/pub/kame/snap/kame-20030616-freebsd48-snap.tgz). A compilação seguiu os passos abaixo [HAM 95] [CHE 95]:

- O kernel do KAME foi baixado no diretório /usr/local
- O arquivo foi descompactado usando o tar :
  - #tar -zxvf kame-20030616-freebsd48-snap.tgz
  - #cd kame

- usar o comando abaixo para criar os links simbólicos do kernel a ser compilado
  - #make TARGET=freebsd4 prepare
- backup do kernel antigo
  - #cp /kernel /kernel.previous
  - #cd /usr
  - #mkdir include.clean
  - #cd include.clean
  - #(cd ../include; tar Bpcf - .) | tar Bpxf -
- edição do arquivo de configuração do kernel
  - #cd /kame/freebsd4/sys/i386/conf
  - #cp GENERIC.KAME IPFW-IP6FW-NAT
  - #ee IPFW-IP6FW-NAT
- construção do kernel
  - #/usr/sbin/config IPFW-IP6FW-NAT
  - #cd ../../compile/IPFW-IP6FW-NAT
  - #make depend
  - #make
- instalação do kernel
  - #make install
- construção de aplicativos
  - #cd kame/freebsd4
  - #make includes
  - #make install-includes
  - #make install
- boot do sistema
  - #fastboot

O arquivo de configuração do kernel IPFW-IP6FW-NAT foi adicionado as linhas a seguir:

pseudo-device gif 5 #IPv6 and IPv4 tunneling; representa o número de interfaces virtuais que a máquina terá

```
#IPv4 firewall
options "IPFIREWALL"
options "IPFIREWALL_VERBOSE"
options "IPFIREWALL_VERBOSE_LIMIT=100"
options "IPFIREWALL_DEFAULT_TO_ACCEPT"
#NAT
options "IPDIVERT"
#IPv6 firewall
options "IPV6FIREWALL"
options "IPV6FIREWALL_VERBOSE"
options "IPV6FIREWALL_VERBOSE_LIMIT=100"
options "IPV6FIREWALL_DEFAULT_TO_ACCEPT"
```

A.2.2 Configurar arquivo /etc/rc.conf

A configuração do arquivo /etc/rc.conf é apresentada a seguir [CHE 95]:

```
#configuração das informações específicas da máquina
hostname="gate6.ipv6.las.ic.unicamp.br"
gateway_enable="YES"
################ Interfaces IPv4 ####################
network_interfaces="fxp0 de0 lo0"
ifconfig_fxp0="inet 143.106.60.70 netmask 255.255.255.192"
ifconfig_de0="inet 143.106.60.97 netmask 255.255.255.240"
ifconfig_de0_alias0="inet 10.1.1.80 netmask 255.255.255.0"
default_router="143.106.60.65"
################ Interfaces IPv6 ###################
ipv6_enable="YES"
ipv6_network_interfaces="fxp0 de0 lo0"
ipv6_gateway_enable="YES"
ipv6_ifconfig_fxp0="3ffe:2b00:500:6::2 prefixlen 126"
```

ipv6_ifconfig_de0="3ffe:2b00:100:102:0:1::2 prefixlen 80"

##

#enable ipfw

firewall_enable="YES"

firewall_type="simple"

#Os tipos de políticas de firewall válidas são:

open - não existem regras para filtrar o tráfego (equivalente a compilar o kernel com a opção IPFIREWALL_DEFAULT_TO_ACCEPT no arquivo de configuração do kernel)

client - protege somente esta máquina

simple - protege toda a rede

closed - desabilita totalmente serviços IP, exceto via interface lo0

UNKNOWN - desabilita a carga das regras do firewall

filename - carrega as regras de um dado arquivo (path completa é exigida)

firewall_script="/etc/ipfw.rules" # carrega as regras, que estão no arquivo, na hora do boot

#enable natd

natd_enable="YES"

natd_interface="fx0"

natd_flags="-m" #se possível, preservar o número de porta

#enable ip6fw

ipv6_firewall_enable="YES"

ipv6_firewall_type="simple"

ipv6_firewall_script="/etc/ip6fw.rules" #carrega as regras, que estão no arquivo, na hora do boot

A.2.3 Configurar túnel com a RNP

A configuração do túnel com a RNP é feita também no arquivo /etc/rc.conf e será apresentada a seguir [KAP 95]:

endereço da RNP = 200.136.100.141 e endereço da gate6 = 143.106.60.70

#configuração da interface virtual gif0

```
gif_interfaces="gif0"
gifconfig_gif0="143.106.60.70 200.136.100.141"
```

A.2.4 Configurar as regras do *firewall*

O IPFIREWALL [PAL 95] [TRA 03] é um *firewall* para filtragem de pacotes padrão no FreeBSD, sendo que o IPFW e o IP6FW são suas interfaces de linha de comando. O conteúdo dos arquivos de configuração é listado abaixo:

IPv4 - /etc/ipfw.rules

```
#!/bin/sh
#Setup system for firewall service.
#
# Regras específicas para o cenário do LAS
# interfaces
EXT_IF="fxp0"
INT_IF="de0"
#endereços das interfaces
EXT_IP="143.106.60.70" # máscara 255.255.255.192
INT_IP="143.106.60.97" # máscara 255.255.255.224
# redes e máscaras
EXT_NET="143.106.60.64"
EXT_MASK="255.255.255.192"
INT_NET="143.106.60.96"
INT_MASK="255.255.255.224"
#path do comando ipfw
fwcmd="/sbin/ipfw"
#limpar todas as regras existentes
${fwcmd} -f flush
#regras para interface LOOPBACK - padrao FreeBSD
${fwcmd} add 1 pass all from any to any via lo0
${fwcmd} add 2 deny all from any to 127.0.0.0/8
${fwcmd} add 3 deny ip from 127.0.0.0/8 to any
```

```
# regras anti IP SPOOFING
${fwcmd} add 4 deny all from ${INT_NET}:${INT_MASK} to any in via ${EXT_IF}
${fwcmd} add 5 deny all from ${EXT_NET}:${EXT_MASK} to any in via ${INT_IF}
#parar redes da RFC1918 no interface externa
${fwcmd} add 8 deny all from any to 10.0.0.0/8 via ${EXT_IF}
${fwcmd} add 9 deny all from any to 172.16.0.0/12 via ${EXT_IF}
${fwcmd} add 10 deny all from any to 192.168.0.0/16 via ${EXT_IF}
# parar redes draft-manning-dsua-03.txt (1 may 2000) (inclui RESERVED-1, DHCP auto-configuração, NET-TEST, MULTICAST (class D), e class E) na interface externa
${fwcmd} add 21 deny all from any to 0.0.0.0/8 via ${EXT_IF}
${fwcmd} add 22 deny all from any to 169.254.0.0/16 via ${EXT_IF}
${fwcmd} add 23 deny all from any to 192.0.2.0/24 via ${EXT_IF}
${fwcmd} add 24 deny all from any to 224.0.0.0/4 via ${EXT_IF}
${fwcmd} add 25 deny all from any to 240.0.0.0/4 via ${EXT_IF}
# NAT - local deliberado
${fwcmd} add 26 divert natd all from any to any via ${EXT_IF}
# impede tráfego RFC1918 entrando pela interface interna
${fwcmd} add 27 deny all from 10.0.0.0/8 to any via ${EXT_IF}
${fwcmd} add 28 deny all from 172.16.0.0/12 to any via ${EXT_IF}
${fwcmd} add 29 deny all from 192.168.0.0/16 to any via ${EXT_IF}
# parar redes draft-manning-dsua-03.txt (1 may 2000) (inclui RESERVED-1, DHCP auto-configuração, NET-TEST, MULTICAST (class D), e class E) na interface externa
${fwcmd} add 31 deny all from 0.0.0.0/8 to any via ${EXT_IF}
${fwcmd} add 32 deny all from 169.254.0.0/16 to any via ${EXT_IF}
${fwcmd} add 33 deny all from 192.0.2.0/24 to any via ${EXT_IF}
${fwcmd} add 34 deny all from 224.0.0.0/4 to any via ${EXT_IF}
${fwcmd} add 35 deny all from 240.0.0.0/4 to any via ${EXT_IF}
#ping
# gate6 - internet
${fwcmd} add 41 pass icmp from ${EXT_IP}:${EXT_MASK} to any icmptypes 8 keep-state via ${EXT_IF}
```

```
# internet - gate6
${fwcmd} add 42 pass icmp from any to ${EXT_IP}:${EXT_MASK} icmptypes 8 keep-state via
${EXT_IF}
# rede interna - internet
${fwcmd} add 43 pass icmp from ${INT_NET}:${INT_MASK} to any icmptypes 8 keep-state in
via ${INT_IF}
# gate6 - rede interna
${fwcmd} add 44 pass icmp from ${INT_NET}:${INT_MASK} to any icmptypes 8 keep-state out
via ${INT_IF}
#traceroute
# permite sair tráfego udp
${fwcmd} add 51 pass udp from ${INT_NET}:${INT_MASK} to any in via ${INT_IF}
# permite chegar tráfego icmp tipo "time exceed during transit"
${fwcmd} add 52 pass icmp from any to ${INT_NET}:${INT_MASK} icmptypes 11
# conexões tcp estabelecidas - permite continuar a conexão se tcp syn (setup) ocorreu com
sucesso
${fwcmd} add 61 pass tcpl from any to any established
# ssh
# máquina tigre do IC - gate6
${fwcmd} add 71 pass tcp from 143.106.7.16 to ${EXT_IP} 22 in via ${EXT_IF} keep-state setup
# gate6 - rede interna
${fwcmd} add 72 pass tcp from ${INT_IP} to ${INT_NET}:${INT_MASK} 22 out keep-state setup
# rede interna - internet
${fwcmd} add 73 pass tcp from ${INT_NET}:${INT_MASK} to ANY 22 keep-state setup
# gate6 - internet
${fwcmd} add 74 pass tcp from ${EXT_IP}:${EXT_MASK} to any 22 out via ${EXT_IF} keep-
state setup
#túnel (gate6 - RNP)
${fwcmd} add 81 pass ip from ${EXT_IP}:${EXT_MASK} to ${RNP_IP} out via ${EXT_IF} keep-
state
```

```
${fwcmd} add 82 pass ip from ${RNP_IP} to ${EXT_IP}:${EXT_MASK} in via ${EXT_IF} keep-
state
#http
# rede interna - internet
${fwcmd} add 91 pass tcp from ${INT_NET}:${INT_MASK} to any 80,443 keep-state setup
# fragmentos
${fwcmd} add 101 pass all from any to any frag
# Política padrão: ACEITA tudo!, por isto a última regra é para negar TUDO!
${fwcmd} add 110 deny all from any to any

IPv6 - /etc/ip6fw.rules
#!/bin/sh
#Setup system for IPv6 firewall service.
#$FreeBSD: src/etc/rc.firewall6,v 1.1.2.11
# Regras específicas para o cenário do LAS
# interfaces
EXT_IF_GIF0="gif0"
INT_IF="de0"
#endereços das interfaces
EXT_IP_GIF0="3FFE:2B00:500"
INT_IP="3FFE:" # máscara /80
# redes e máscaras
INT_NET="3FFE:2B00:"
INT_PREF="80"
#path do comando ipfw
fw6cmd="/sbin/ip6fw"
#limpar todas as regras existentes
${fw6cmd} -f flush
#regras para interface LOOPBACK - padrao FreeBSD
${fw6cmd} add 1 pass all from any to any via lo0
# ND
```

```
# DAD
${fw6cmd} add 2 pass ipv6-icmp from :: to ff02::/16
# RS, RA, NS, NA, redirect...
${fw6cmd} add 3 pass ipv6-icmp from fe80::/10 to fe80::/10
${fw6cmd} add 4 pass ipv6-icmp from fe80::/10 to ff02::/16
# trafego de 3ffe:: e fe80 são conhecidos e permitidos
${fw6cmd} add 5 pass all from ${INT_NET}/${INT_PREF} to any in via ${INT_IF}
${fw6cmd} add 6 pass all from fe80::/12 to any via ${INT_IF}
# regras anti IP SPOOFING
${fw6cmd} add 7 deny all from ${INT_NET}/${INT_PREF} to any in via ${EXT_IF_GIF0}
${fw6cmd} add 8 deny all from any to any in via ${INT_IF}
#parar site-local na interface externa
${fw6cmd} add 9 deny all from fec0::/10 to any via ${EXT_IF_GIF0}
${fw6cmd} add 10 deny all from any to fec0::/10 via ${EXT_IF_GIF0}
# impedir endereços "internos" no cabo
${fw6cmd} add 11 deny all from :ffff:0.0.0.0/96 to any via ${EXT_IF_GIF0}
${fw6cmd} add 12 deny all from any to :ffff:0.0.0.0/96 via ${EXT_IF_GIF0}
# impedir pacotes para prefixos compatíveis IPv4 maliciosos
${fw6cmd} add 13 deny all from ::224.0.0.0/100 to any via ${EXT_IF_GIF0}
${fw6cmd} add 14 deny all from any to ::224.0.0.0/100 via ${EXT_IF_GIF0}
${fw6cmd} add 15 deny all from ::127.0.0.0/104 to any via ${EXT_IF_GIF0}
${fw6cmd} add 16 deny all from any to ::127.0.0.0/104 via ${EXT_IF_GIF0}
${fw6cmd} add 17 deny all from ::0.0.0.0/104 to any via ${EXT_IF_GIF0}
${fw6cmd} add 18 deny all from any to ::0.0.0.0/104 via ${EXT_IF_GIF0}
${fw6cmd} add 19 deny all from ::255.0.0.0/104 to any via ${EXT_IF_GIF0}
${fw6cmd} add 20 deny all from any to ::255.0.0.0/104 via ${EXT_IF_GIF0}
${fw6cmd} add 21 deny all from ::0.0.0.0/96 to any via ${EXT_IF_GIF0}
${fw6cmd} add 22 deny all from any to ::0.0.0.0/96 via ${EXT_IF_GIF0}
# impedir pacotes para prefixos 6to4 maliciosos
${fw6cmd} add 31 deny all from 2002:e000::/20 to any via ${EXT_IF_GIF0}
${fw6cmd} add 32 deny all from any to 2002:e000::/20 via ${EXT_IF_GIF0}
```

```
${fw6cmd} add 33 deny all from 2002:7f00::/24 to any via ${EXT_IF_GIF0}
${fw6cmd} add 34 deny all from any to 2002:7f00::/24 via ${EXT_IF_GIF0}
${fw6cmd} add 35 deny all from 2002:0000::/24 to any via ${EXT_IF_GIF0}
${fw6cmd} add 36 deny all from any to 2002:0000::/24 via ${EXT_IF_GIF0}
${fw6cmd} add 37 deny all from 2002:ff00::/24 to any via ${EXT_IF_GIF0}
${fw6cmd} add 38 deny all from any to 2002:ff00::/24 via ${EXT_IF_GIF0}
${fw6cmd} add 39 deny all from 2002:0a00::/24 to any via ${EXT_IF_GIF0}
${fw6cmd} add 40 deny all from any to 2002:0a00::/24 via ${EXT_IF_GIF0}
${fw6cmd} add 41 deny all from 2002:ac10::/28 to any via ${EXT_IF_GIF0}
${fw6cmd} add 42 deny all from any to 2002:ac10::/28 via ${EXT_IF_GIF0}
${fw6cmd} add 43 deny all from 2002:c0a8::/32 to any via ${EXT_IF_GIF0}
${fw6cmd} add 44 deny all from any to 2002:c0a8::/32 via ${EXT_IF_GIF0}
${fw6cmd} add 45 deny all from ff05::/16 to any via ${EXT_IF_GIF0}
${fw6cmd} add 46 deny all from any to ff05::/16 via ${EXT_IF_GIF0}
#ping
${fw6cmd} add 47 pass ipv6-icmp from any to any icmptypes 128,129
# permite icmpv6 destination unreach
${fw6cmd} add 48 pass ipv6-icmp from any to any icmptypes 1
# permite NS/NA/toobig
${fw6cmd} add 49 pass ipv6-icmp from any to any icmptypes 2,135,136
# conexões tcp estabelecidas - permite continuar a conexão se tcp syn (setup) ocorreu com
sucesso
${fw6cmd} add 61 pass tcpl from any to any established
# ssh
# gate6 - rede interna
${fw6cmd} add 71 pass tcp from ${INT_IP} to ${INT_NET}/${INT_PREF} 22 out via ${INT_IF}
setup
# rede interna - internet
${fw6cmd} add 72 pass tcp from ${INT_NET}/${INT_PREF} to any 22 via ${INT_IF} setup
# gate6 - internet
${fw6cmd} add 73 pass tcp from ${EXT_IP_GIF0} to any 22 out via ${EXT_IF_GIF0} setup
```

```
# http
#rede interna - internet
${fw6cmd} add 74 pass tcp from ${INT_NET}/${INT_PREF} to any 80,443 in via ${INT_IF} setup
${fw6cmd} add 75 pass tcp from ${INT_NET}/${INT_PREF} to any 80,443 out via ${EXT_IF_GIF0} setup
# Política padrão: ACEITA tudo!, por isto a última regra é para negar TUDO!
${fw6cmd} add 110 deny ipv6 from any to any
```

A.3 Configuração Linux Red Hat 9.0

A.3.1 Compilar *kernel*

O kernel do Red Hat foi compilado usando o kernel do USAGI (ftp://ftp.linux-ipv6.org/pub/usagi/stable/kit/usagi-linux24-stable-20030214.tar.bz2). A instalação do kit do USAGI seguiu os passos abaixo [REDb 03]:

- O kernel do USAGI foi baixado no diretório /usr/src/
- O arquivo foi descompactado usando o bzip2 e o tar :
  - #bzip2 -cd usagi-linux24-stable-20030214.tar.bz2 | tar xvf -
  - #cd usagi
    - ou
  - #bzip2 -cd usagi-linux24-stable-20030214.tar.bz2
  - #tar -xvf usagi-linux24-stable-20030214.tar
  - #cd usagi
- usar o comando abaixo para criar os links simbólicos do kernel a ser compilado
  - #make prepare TARGET=$(TARGET)
    - onde $(TARGET) pode ser linux22 ou linux24, o que for mais apropriado para o sistema onde será instalado o kit USAGI
- configure o kernel
  - cd kernel
  - cd $(TARGET)

  - make mrproper
  - make menuconfig ou make config ou make xconfig
    - estes comandos são equivalentes e permitem que o arquivo de configuração do kernel seja configurado
- construir o kernel e os módulos
  - make dep
  - make bzImage
  - make modules
- instala o kernel e os módulos
  - make install
  - make modules_install
- edite o arquivo do boot loader lilo ou grub, para contemplar este novo kernel. [REDc 03]

A.3.2 Configurar DNS

O programa utilizado para configurar DNS com suporte a IPv6 foi o BIND 9 [INT 94]. A rede do LAS tem uma alocação SLA/64 3FFE:2B00:100:102::/64. Os arquivos de configuração do DNS são [INT 00]:

```
/etc/named.conf - arquivo de configuração do name server
acl "ns-trusted-hosts" {
        143.106.60.15;
};
acl "internal-hosts" {
        143.106.60.178;
        143.106.60.170;
        10.1.2.2;
        10.1.2.3;
        10.1.1.75;
        143.106.60.114;
};
options {
        directory "/var/named"; //localização dos arquivos do named
```

```
    // statements de IPv4
        allow-transfer { ns-trusted-hosts;  }; //especifica quem pode pedir blocos de dados de sua zona
    allow-recursion { internal-hosts;  }; //o named desta maquina faz recursão em beneficio de clientes listados
        transfer-format one-answer; //influencia o modo como os registros do dns são replicados para os slaves
    // statements de IPv6
        listen-on-v6 { any; };
    };
    zone "localhost" IN {
        type master;
        file "localhost.zone";
    };
    //Arquivos de zone para IPv4
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "localhost.zone";
    };
    zone "60.106.143.in-addr.arpa" IN {
        type master;
        file "143.106.60";
    };
    //Arquivo de zone para IPv4 e IPv6
    zone "ipv6.las.ic.unicamp.br" IN {
        type master;
        file "ipv6.las.zone";
```

```
};
//Arquivos de zone para IPv6
//dominio IPv6
//endereco loopback IPv6
zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.int" IN {
        type master;
        file "localhost.zone";
};
zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
       file "localhost.zone";
};
//reverse lookup zones
// SLA ID - 3ffe:2b00:100:102::/64
zone "2.0.1.0.0.0.1.0.0.0.b.2.e.f.f.3.ip6.int" IN {
        type master;
        file "3ffe.2b00.100.102";
};
zone "2.0.1.0.0.0.1.0.0.0.b.2.e.f.f.3.ip6.arpa" IN {
        type master;
        file "3ffe.2b00.100.102";
};

/etc/resolv.conf - arquivo de configuração do resolver

/var/named:
      - localhost.zone
;Arquivo: localhost.zone, loopback de IPv4 e IPv6
;Dominio IPv6 do LAS
$TTL    86400
@                   IN SOA      shadowfax.ipv6.las.ic.unicamp.br. root.ipv6.las.ic.unicamp.br. (
```

```
                                20030801                ; serial
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1D )            ; minimum
                        IN NS       @
                        IN A        127.0.0.1
;ipv4
localhost.              IN A        127.0.0.1
;1.0.0.127.in-addr.arpa     IN PTR      localhost.
;ipv6
localhost.              IN A6       ::1
;1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.int. IN PTR      localhost.
```

– ipv6.las.zone

```
;Arquivo: end-ipv6.zone
;Dominio IPv6 do LAS
$TTL    86400
@                   IN SOA  shadowfax.ipv6.las.ic.unicamp.br. root.ipv6.las.ic.unicamp.br. (
                                20030802        ; serial
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1D )            ; minimum
                    IN NS   shadowfax.ipv6.las.ic.unicamp.br.
                    IN MX   10 shadowfax.ipv6.las.ic.unicamp.br.
;Nomes de Redes
;SLA-ipv6               IN A6       3ffe:2b00:100:102::
;Hosts locais
shadowfax           IN A            143.106.60.98
;shadowfax          IN AAAA         3ffe:2b00:100:102:0:1:0:3
```

```
shadowfax          IN A6   0      3ffe:2b00:100:102:0:1:0:3
;shadowfax         IN A6   64     ::0:1:0:3       teste
gate6              IN A           143.106.60.70
;gate6             IN AAAA        3ffe:2b00:100:102:0:1:0:2
gate6              IN A6   0      3ffe:2b00:100:102:0:1:0:2
;gate6             IN A6   64     ::0:1:0:2       teste
;proxy
www                IN CNAME       shadowfax.ipv6.las.ic.unicamp.br.
proxy              IN CNAME       shadowfax.ipv6.las.ic.unicamp.br.
ftp                IN CNAME       shadowfax.ipv6.las.ic.unicamp.br.
```

- named.ca
  - arquivo que contém informação dos servidores de nome da raiz. Seu conteúdo não é listado aqui, pois é o mesmo para IPv4 e IPv6, já que ainda não existem servidores da raiz exclusivamente IPv6.

- 143.106.60

```
;Arquivo: 143.106.60
;Dominio IPv6 do LAS
$TTL    86400
@               IN SOA    shadowfax.ipv6.las.ic.unicamp.br. root.ipv6.las.ic.unicamp.br. (
                          20030801        ; serial
                          3H              ; refresh
                          15M             ; retry
                          1W              ; expiry
                          1D )            ; minimum

@                 IN NS     shadowfax.ipv6.las.ic.unicamp.br.
70                IN PTR    gate6.ipv6.las.ic.unicamp.br.
98                IN PTR    shadowfax.ipv6.las.ic.unicamp.br.
```

```
        – 3ffe:2b00:100:102
;Arquivo: 3ffe:2b00:100:102
;Dominio IPv6 do LAS
$TTL    86400
@               IN SOA    shadowfax.ipv6.las.ic.unicamp.br. root.ipv6.las.ic.unicamp.br. (
                          20030801  ; serial
                          3H        ; refresh
                          15M       ; retry
                          1W        ; expiry
                          1D )      ; minimum

@                                   IN NS     shadowfax.ipv6.las.ic.unicamp.br.
2.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0    IN PTR    gate6.ipv6.las.ic.unicamp.br.
3.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0    IN PTR    shadowfax.ipv6.las.ic.unicamp.br.
```

A.4 Referências

[CHE 95] CHERN, L. FreeBSD Handbook. Chapter 19 Advanced Networking. *19.13 Network Address Translation*. 1995. 30/01/04. http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-natd.html

[FRE 95] FreeBSD Project. http://www.freebsd.org. 30/01/04.

[HAM 95] HAMBY, J.; MOCK, J. FreeBSD Handbook. *Chapter 9 Configuring the FreBSD Kernel.* 1995. 30/01/04. http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/kernelconfig.html

[INT 94] Internet Systems Consortium, Inc. (ISC). http://www.isc.com. 30/01/04.

[INT 00] Internet Systems Consortium, Inc. (ISC). *BIND 9 Administrator Reference Manual.* 2000. 30/01/04. http://www.bind9.net/Bv9ARM.html

[KAM 98] KAME Project. http://www.kame.net. 30/01/04.

[KAP 95] KAPLAN, A.; RHODES, T. FreeBSD Handbook. Chapter 19 Advanced Networking. *19.16 IPv6*. 1995. 30/01/04. http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-ipv6.html

[LAB 04] Laboratório de Administração e Segurança. http://www.las.ic.unicamp.br. 30/01/04.

[PAL 95] PALMER, G.; NASH, A. FreeBSD Handbook. Chapter 10 Security. *10.8 Firewalls* 1995. 30/01/04. http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html

[RED 89] Rede Nacional de Ensino e Pesquisa (RNP). http://www.rnp.br. 30/01/04.

[RED 03a] Red Hat. http://www.redhat.com. 30/01/04.

[RED 03b] Red Hat Documentation. Red Hat Linux 9: Red Hat Linux Customization Guide. *Appendix A. Building the Kernel.* 30/01/04. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-custom-kernel-modularized.html

[RED 03c] Red Hat Documentation. Red Hat Linux 9: Red Hat Linux Customization Guide. *30.6. Verifying the Boot Loader.* 30/01/04. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-kernel-bootloader.html

[TRA 03] TRACANELLI, P.; GOTO, M. Documentação FreeBSD. *Capítulo 8 IPFIREWALL/IPFW.* 2003. 30/01/04. http://free.bsd.com.br/~eksffa/freebsd/ipvw.php

[USA 00] USAGI Project. http://www.linux-ipv6.org. 30/01/04.

[VMW 98] VMware. http://www.vmware.com. 30/01/04.

Apêndice B

Alocação de endereços IP no Brasil e no Mundo

B.1 Faixas IPv4 a serem alocadas no Brasil

O Registro.br é o responsável pela alocação de endereços IPv4 para organizações no Brasil. Nesta subseção serão apresentadas as faixas IPv4 a partir das quais o Registro.br faz suas alocações.

% Copyright LACNIC lacnic.net
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to AS and IP numbers registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2003-09-12 17:15:11 (BRT -03:00)

owner: Comite Gestor da Internet no Brasil
ownerid: BR-CGIN-LACNIC
responsible: Frederico A C Neves
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR

phone: +55 11 9119-0304 []
owner-c: CGB
created: 20020902
changed: 20030603

nic-hdl: CGB
person: Comite Gestor da Internet no Brasil
e-mail: blkadm@NIC.BR
address: Av. das Nações Unidas, 11541, 7° andar
address: 04578-000 - São Paulo - SP
country: BR
phone: +55 19 9119-0304 []
created: 20020902
changed: 20020902

aut-num: 22548
inetnum: 200.17/16
inetnum: 200.18/15
inetnum: 200.20/16
inetnum: 200.96/13
inetnum: 200.128/9
inetnum: 201.0/12

B.2 Alocação de endereços IPv6 no mundo

As alocações já feitas pela IANA são mostradas na Figura B.1. Quando um RIR alocou quase completamente seu bloco, ele pode solicitar novo bloco [IAN 04].

Prefixo IPv6	Valores Binários sub-TLA	Alocação para	Data
2001:0000::/23	0000 000x xxxx x	IANA	Jul 99
2001:0200::/23	0000 001x xxxx x	APNIC	Jul 99
2001:0400::/23	0000 010x xxxx x	ARIN	Jul 99
2001:0600::/23	0000 011x xxxx x	RIPE NCC	Jul 99
2001:0800::/23	0000 100x xxxx x	RIPE NCC	May 02
2001:0A00::/23	0000 101x xxxx x	RIPE NCC	Nov 02
2001:0C00::/23	0000 110x xxxx x	APNIC	May 02
2001:0E00::/23	0000 111x xxxx x	APNIC	Jan 03
2001:1000::/23	0001 000x xxxx x	designação futura	
2001:1200::/23	0001 001x xxxx x	LACNIC	Nov 02
2001:1400::/23	0001 010x xxxx x	RIPE NCC	Feb 03
2001:1600::/23	0001 011x xxxx x	RIPE NCC	Jul 03
2001:1800::/23	0001 100x xxxx x	ARIN	Apr 03
2001:1A00::/23	0001 101x xxxx x	RIPE NCC	Jan 04
...	...		
2001:FE00::/23	1111 111x xxxx x	designação futura	

Figura B.1: Alocação de Endereços IPv6.

B.3 Referências

[IAN 04] IANA - IPv6 Top Level Aggregation Identifier Assignments. http://www.iana.org/assignments/ipv6-tla-assignments. 30/01/04.

Glossário

alocação: significa distribuir espaço de endereçamento a Registros Internet (IR) com o propósito de subseqüente distribuição feitas por eles.

Ambiente Cooperativo: é o ambiente no qual as várias organizações (matrizes, filiais, parceiros comerciais, distribuidores, clientes, etc) trocam informações técnicas, comerciais e financeiras através de uma rede integrada virtualmente.

Ambiente Cooperativo Seguro: é definido como sendo a rede integrada virtualmente utilizada pelas várias organizações, que compõem o ambiente cooperativo para trocarem informações de vários tipos, combinada com o firewall cooperativo, cujo objetivo é proteger o ambiente formado.

aplicação IPv4: a aplicação que roda em uma máquina usa somente o protocolo IPv4, não estando apta a reconhecer um endereço IPv6. Contudo, a máquina pode ter conectividade de rede IPv4 e/ou IPv6. Uma das possíveis razões para a aplicação não reconhecer IPv6 é a fato de programadores ainda não terem portado a aplicação para IPv6.

***backbone*:** É um conjunto de caminhos disponíveis para as redes locais ou regionais conseguirem interconecção a longas distâncias com outras redes.

cabeçalho AH: é um dos cabeçalhos IPSec que protege contra alterações maliciosas, provendo proteção de integridade e autenticação para toda informação fim-a-fim transportada em um pacote IP.

cabeçalho ESP: é o segundo cabeçalho IPSec que provê privacidade e protege o pacote contra alterações maliciosas.

cabeçalhos IPSec: são cabeçalhos especiais que identificam os tipos de proteção criptográficas, que serão aplicadas ao pacote e incluem outras informações necessárias à decodificação correta do pacote protegido.

CGA: *Cryptographically Generated Addresses*. São endereços gerados criptograficamente para assegurar que o transmissor de uma mensagem *Neighbor Advertisement* ou *Router Advertisement* é o dono do endereço reclamado.

cifragem: é o processo pelo qual uma mensagem (chamada de texto claro) é transformada em outra (chamada de texto cifrado), através da aplicação de uma função matemática (chamada de algoritmo de cifragem) e de uma senha especial de cifragem (chamada de chave).

designação: significa delegar espaço de endereçamento para um ISP ou usuário final, para um uso específico dentro da infraestrutura Internet que ele opera. Designações devem ser feitas somente para um propósito específico e documentado para uma específica organização e não deve ser sub designado para outras partes.

detecção a intrusão: pode ser definida como o processo de monitoramento dos eventos ocorridos em um sistema computacional ou rede, em busca de sinais que indiquem problemas de segurança.

firewall: um *firewall* consiste na demarcação de um perímetro de segurança, visando estabelecer que a área interna por este delimitada deve ser protegida daquilo que se situa fora de suas fronteiras.

***firewall* cooperativo:** é um conjunto diverso de software e hardware, que colaboram para aplicar uma determinada política de segurança. Ele apresenta uma arquitetura que inclui todas as tecnologias de segurança existentes.

framework: conjunto de recursos disponibilizados que permitem uma certa funcionalidade ou uma certa função operarem em alto nível.

IDS: *Intrusion Detection System*. Um sistema de detecção a intrusão é um sistema que automatiza o processo de monitoramento dos eventos ocorridos em um sistema computacional ou rede, em busca de sinais que indiquem problemas de segurança.

IKE: *Internet Key Exchange*. É um mecanismo que permite a troca de chaves secretas e outros parâmetros relacionados a proteção antes da comunicação propriamente dita entre as partes, sem a intervenção do usuário.

initiator: é o responsável pelo envio da primeira mensagem de estabelecimento de uma Associação de Segurança.

IPSec: é uma tentativa para definir uma solução global para o problema de falta de segurança na Internet, habilitando comunicações seguras na camada IP.

IPv6: um novo conjunto de protocolos e padrões desenvolvido pelo *Internet Engineering Task Force* (IETF) para a camada de rede. Seu objetivo é atualizar o protocolo IPv4, causando o mínimo impacto nos protocolos das camadas acima e abaixo.

LACNIC: *Latin American and Caribbean Internet Addresses Registry*. É a organização responsável pela administração do espaço de endereçamento IP, Números de Sistemas Autônomos (ASN), resolução reversa e outros recursos para a região da América Latina e Caribe em nome da comunidade Internet.

LIR: *Local Internet Registry*. É responsável basicamente pela designação de espaço de endereçamento para os usuários dos serviços de rede fornecidos. LIR são geralmente Provedores de Serviço Internet (ISP), cujos clientes são basicamente usuários finais e possivelmente outros Provedores de Serviços (ISP).

mecanismo de transição: é um mecanismo que permite a redes e máquinas IPv4 migrarem ou adotarem o protocolo de rede IPv6 de forma suave e tranqüila. Estes mecanismos são divididos em três classes: pilha dupla, tunelamento e tradução.

mecanismo de tunelamento: é o mecanismo de transição frequentemente utilizado quando partes ou toda infra-estrutura de rede não é capaz de prover conectividade IPv6. Ele permite que o tráfego IPv6 seja carregado sobre a infra-estrutura de rede de IPv4.

mecanismo de tradução: é um mecanismo usado onde dispositivos, que usam somente IPv6, desejam se comunicar com dispositivos que usam somente IPv4.

mecanismo pilha dupla: este mecanismo permite integrar facilmente IPv6 em uma rede IPv4. uma vez que introduz IPv4 e IPv6 no mesmo ambiente e na mesma interface. Tanto os roteadores como as máquinas de trabalho precisam ser atualizadas para suportar IPv6 e continuar suportando IPv4, ou seja, o sistema operacional precisa ter as duas pilhas IPv4 e IPv6.

NAT: *Network Adress Translation*. Mecanismo de tradução de endereços de rede consiste em trocar o endereço IP de origem/destino (ou ambos) de um pacote - ou mesmo as portas TCP/UDP de origem/destino - por outros valores, de acordo com a necessidade.

ND: *Neighbor Discovery*. Este protocolo combina o protocolo de resolução de endereços IP em endereços MAC e mensagens de ICMP para descoberta de roteador e redirecionamento. É também importante no mecanismo de auto-configuração de máquinas IPv6 na rede, já que estas máquinas podem obter informações necessárias para sua configuração IP usando as mensagens do protocolo *Neighbor Discovery* e sem a necessidade de intervenção direta do administrador.

NDP: *Neighbor Discovery Protocol*. É a sigla do protocolo *Neighbor Discovery*. Ele consiste de cinco mensagens ICMP: um par de mensagens *Router Solicitation* (RS) e *Router Advertisement* (RA), um par de mensagens *Neighbor Solicitation* (NS) e *Neighbor Advertisement* (NA) e uma mensagem de ICMP *redirect*.

PFS: *Perfect Forward Secrecy*. É a garantia da geração de apenas uma chave pela troca Diffie-Hellman e que não tem relação com quaisquer outras chaves usadas entre os pares.

proxy: é um mecanismo que atua como intermediário entre clientes internos e servidores externos, situando-se também no perímetro da rede, porém efetuando verificação do tráfego no nível de aplicação.

RD: *Router Discovery*. É o processo de descoberta do roteador padrão de um enlace. Este processo usa dois tipos de mensagens: *Router Advertisement* (RA) e *Router Solicitation* (RS). As

mensagens de RA são enviadas pelos roteadores em intervalos regulares para anunciarem o prefixo para um enlace, seus endereços de enlace e o MTU usado no enlace. As mensagens de RS são enviadas pelas máquinas para solicitarem RA dos roteadores do enlace.

rede IPv4: é uma rede de computadores cujo protocolo de rede corrente é o IPv4, ou seja, todos os computadores usam somente IPv4 para se comunicarem com outras máquinas da rede.

rede IPv6: é uma rede de computadores cujo protocolo de rede corrente é o IPv6, ou seja, todos os computadores usam o IPv6 para obter conectividade de rede.

***responder*:** é quem recebe a mensagem enviada pelo initiator com o objetivo de estabelecer uma Associação de Segurança.

RFC: *Request for coments*. Um documento técnico que define ou formaliza um padrão dentro da rede Internet.

RIR: Registro Internet Regional. São estabelecidos e autorizados pela respectiva comunidade regional e reconhecidos pela IANA para servir e representar extensas regiões geográficas. A principal regra de um RIR é gerenciar e distribuir espaço de endereçamento Internet público em suas respectivas regiões. O LACNIC é o registro Internet para a região da América Latina e Caribe.

SAD: *Security Association Database*. É utilizado para armazenar as Associações de Segurança ativas de uma máquina num dado momento, ou seja, toda Associação de Segurança estabelecida deve conter uma entrada nesta base de dados, inserida pelo administrador ou pelo protocolo IKE.

SEND: *Secure Neighbor Discovery*. É um grupo de trabalho criado pelo IETF para definir suporte à segurança no protocolo *Neighbor Discovery*, sem contudo exigir configuração manual.

SPD: *Security Policy Database*. Especifica as políticas que determinam a manipulação de todo tráfego IP de um sistema, não apenas de tráfego carregando elementos de cifragem e autenticação. Cada entrada no SPD resulta na criação ou negociação de uma ou mais Associações de Segurança.

SPI: *Security Parameter Index*. É o índice na base de dados da Associação de Segurança do receptor do pacote e é utilizado para indicar qual algoritmo criptográfico usar.

VPN: *Virtual Private Network*. As redes virtuais privadas são um componente importante dentro do ambiente cooperativo ao permitirem que conexões dedicadas e estruturadas de acesso remoto, 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 entre pontos distintos.