Implementação do protocolo IPV6 com segurança: Uma análise sobre os desafios e riscos para os administradores de redes internet

Anderson Luiz Coan[1]

[1]EACH-USP – School of Arts, Sciences, and the Humanities of the University of São Paulo, Av. Arlindo Béttio, 1000, CEP 03828-000, São Paulo, SP

{anderson.coan}@usp.br

Resumo. *Uma das grandes preocupações que assolam os profissionais de TI na atualidade é a grande preocupação com a segurança na comunicação utilizando a internet. Técnicas paliativas como a utilização dos serviços NAT*[1]*já vem sendo utilizadas, mas começa a apresentar seus limites. O novo protocolo IPV6 vem sendo estudado e implementado gradativamente por instituições acadêmicas e profissionais e, entre outras características, visa oferecer maior segurança através de serviços como o IPSec. Com isso, passa a se tornar interessante apresentar uma análise dos desafios e riscos que os administradores de internet vão ter pela frente a tomar a decisão dessa transição IPV4 para IPV6 com segurança. Essa é a proposta desse artigo.*

Abstract. *A major concern plaguing IT professionals today is the great concern about security in communication using the internet. Palliative techniques such as the use of NAT services already being used, but beginning to show its limits. The new protocol IPv6 has been studied and implemented gradually by academic institutions and professional, among other characteristics, aims to offer enhanced security through services such as IPSec. With this, goes on to become interesting to present an analysis of the challenges and risks that administrators of Internet will have ahead to make the decision that IPV4 to IPV6 transition safely. That is the purpose of this article.*

1. Introdução

Desde o início dos estudos da implementação do protocolo IPV6, muito se foi discutido a respeito da segurança. Antes, termos como encriptação e autenticação, termos desconhecido na versão do IPV4, agora passam a fazer parte do protocolo IPV6, permitindo assim disponibilizar para qualquer par de dispositivos com conexão fim a fim, caminhos que proporcionam níveis mais elevados de segurança (SANTOS 2010).

Desde seu surgimento até os dias atuais, a comunicação na internet vem aumentando cada vez mais, tanto nas residências quanto nas empresas, se tornando assim, um fator

[1] Network Address Translation (NAT) é um protocolo que faz a tradução dos endereços IP´s e portas TCP da rede local para a internet.

preocupante, estimulando pesquisadores a cada vez mais aprofundar seus conhecimentos na implementação de uma segurança mandatária. Isso se começou a tornar possível ao encontrar recursos no protocolo IPV6 que trata especificamente segurança.

Atualmente muitos dados estão trafegando na internet sujeitos a capturas por programas específicos, usados de forma maliciosa. O protocolo que atualmente está trafegando e gerenciando a rede da internet é o protocolo IPV4 (*Internet Protocol Version 4*), que não previa, desde a ampla implementação do uso da Internet, esse grande avanço na troca das informações, se tornando assim, um protocolo vulnerável (JUNIOR 2005).

Serviços como, por exemplo, o IPSec, já vem sendo estudado por muitas instituições acadêmicas e profissionais, tornando cada vez mais interessante a sua referência de segurança.

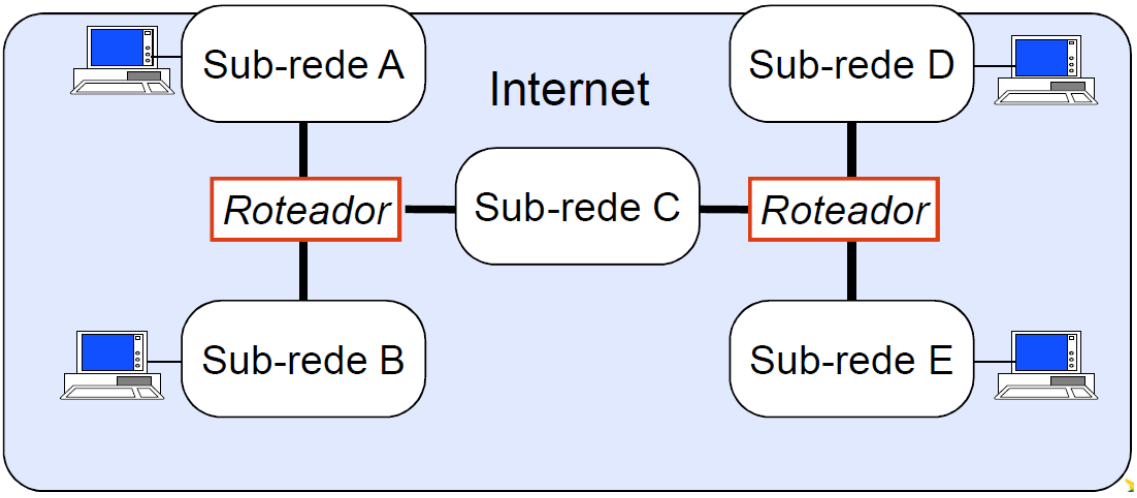
Outras possibilidades são implementações de uma boa política de distribuição de redes IPV6, agregado com outras políticas internas a essas instituições e legislações, a fim de se tentar tornar cada vez mais suave a transição do protocolo IPV4 para o IPV6 e também a segurança dos dados trafegados.

Esse artigo tem a proposta de apresentar algumas análises sobre os desafios e riscos para os administradores de internet na transição do IPV4 para o IPV6, assim como a segurança que esse protocolo irá propor aos dados trafegados, baseado em informações já amplamente estudados por autores citados aqui. O trabalho está dividido da seguinte maneira: O capítulo 2 apresenta um breve histórico da Internet, para que o leitor possa entender como toda essa necessidade aconteceu. No capítulo 3, é apresentado um breve estudo sobre o funcionamento do IPV6. Já no capítulo 4 é apresentado alguns dos principais desafios discutidos por instituições acadêmicas e profissionais a respeito da transição do IPV4 para o IPV6 e também a implementação da segurança na troca das informações. E por fim, no capítulo 5, as considerações finais sobre esse trabalho.

2. Histórico

Na figura 1 abaixo, é apresentado uma visão geral de como funciona um sistema de interconexão de redes distintas trafegando dados pela internet.

Figura 1: A interconexão de duas ou mais redes se dá pela funcionalidade do roteador



A internet surgiu a partir de pesquisas militares nos períodos áureos da Guerra Fria, na década de 60. Na perspectiva do governo americano de sofrer um ataque do inimigo, trazendo a público informações sigilosas e podendo torna-los vulneráveis, começou-se a idealizar um modelo de troca e compartilhamento de informações que permitisse a descentralização das mesmas. Assim, se o Pentágono fosse atingido, as informações armazenadas ali não estariam perdidas. Era preciso, portanto, criar uma rede. Assim, surgiu a ARPANET[2].

A ARPANET funcionava através de um sistema conhecido como chaveamento de pacotes, que é um sistema de transmissão de dados em rede de computadores no qual as informações são divididas em pequenos pacotes, que por sua vez contém trecho dos dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original. Sem perceber, o Departamento de Defesa dos Estados Unidos dava início ao maior fenômeno midiático do século 20, a Internet.

Já na década de 1970, o governo dos EUA permitiu que pesquisadores que desenvolvessem, nas suas respectivas universidades, estudos na área de defesa pudessem também entrar na ARPANET. Com isso, a ARPANET começou a ter dificuldades em administrar todo este sistema, devido ao grande e crescente número de localidades universitárias contidas nela.

Estudos então desenvolveram um sistema técnico denominado Protocolo de Internet (*Internet Protocol*) que permitia que o tráfego de informações fosse encaminhado de uma rede para outra. Todas as redes conectadas pelo endereço IP na Internet comunicam-se para que todas possam trocar mensagens. Através da *National Science Foundation*, o governo norte-americano investiu na criação de backbones (que significa espinha dorsal, em português), que são poderosos computadores conectados por linhas que tem a capacidade de dar vazão a grandes fluxos de dados, como canais de fibra óptica, elos de satélite e elos de transmissão por rádio. Além desses backbones, existem os criados por empresas particulares. A elas são conectadas redes menores, de forma mais ou menos anárquica. É basicamente isto que consiste a Internet, que não tem um dono específico. Em 1992, o cientista Tim Berners-Lee, do CERN, criou a *World Wide Web* (WWW). Já a empresa norte-americana Netscape criou o protocolo HTTPS (*HyperText Transfer Protocol Secure*), possibilitando o envio de dados criptografados para transações comercias pela internet.

Com muitos diferentes métodos de redes, alguma coisa era necessária para a unificação dos mesmos. Em 1973, foi trabalhado uma reformulação fundamental, onde as diferenças entre os protocolos de rede eram escondidas pelo uso de um protocolo inter-redes comum, tornando os hospedeiros (conhecidos como *hosts*) responsáveis.

Com o papel da rede reduzida ao mínimo, ficou possível a junção de praticamente todas as redes. O DARPA[3] concordou em financiar o projeto de desenvolvimento do software. Decorrentes das primeiras espacificações do TCP

---

[2] Criada pela ARPA (Advanced Research Projects Agency), uma rede para interligar equipamentos com o objetivo de descentralizar informações.

[3] DARPA (Defense Advanced Research Projects Agency, Agência de Projetos de Pesquisa Avançada de Defesa) foi criada em fevereiro de 1958 (como ARPA) por militares e pesquisadores americanos com o objetivo original de manter a superioridade tecnológica dos EUA. Era ARPA até 1993, depois voltou a ser DARPA em 1996.

(*Transfer Control Protocol*) em 1974, TCP/IP (*Transfer Control Protocol/Internet Protocol*) emergiu em meados do final de 1978, em forma quase definitiva. Em 1981, os padrões associados foram publicados como RFCs 791, 792 e 793 e adotado para uso. O DARPA patrocinou e incentivou o desenvolvimento de implementações TCP/IP para vários sistemas operacionais e depois programou uma migração de todos os hospedeiros de todas as suas redes de pacotes para o TCP/IP. Em 1º de janeiro de 1983, data conhecida como *Flag Day*, o protocolo TCP/IP se tornou o único protocolo aprovado pela ARPANET (Histórico da Internet 2013).

Com todo esse desenvolvimento acontecendo de forma muito rápida, não foi possível se dar conta de que em algum momento, a segurança das informações trocadas nessa grande rede ganharia destaque. Além disso, o crescimento acelerado trouxe outro agravante: o problema da falta de endereçamentos lógicos, ou seja, do endereço IP, disponível a todos os usuários da rede. Uma hora, ele acabaria.

A versão atual do IP é a 4, porém algumas características desta versão estão deixando a desejar, pois, nos últimos anos, a Internet teve um crescimento surpreendente e com este crescimento surgiram problemas que não estavam previstos. Assim, devido a grande quantidade de máquinas conectadas a Internet, os endereços IP começaram a se tornar escassos e, além disso, o surgimento de novas tecnologias, como, por exemplo, serviços em tempo real que utilizam sons e vídeos, não é suportado de maneira eficiente pelo atual protocolo.

Na época, a versão 4 do protocolo IP mostrou-se muito robusta, e de fácil implantação e interoperabilidade, entretanto, seu projeto original não previu alguns aspectos como:

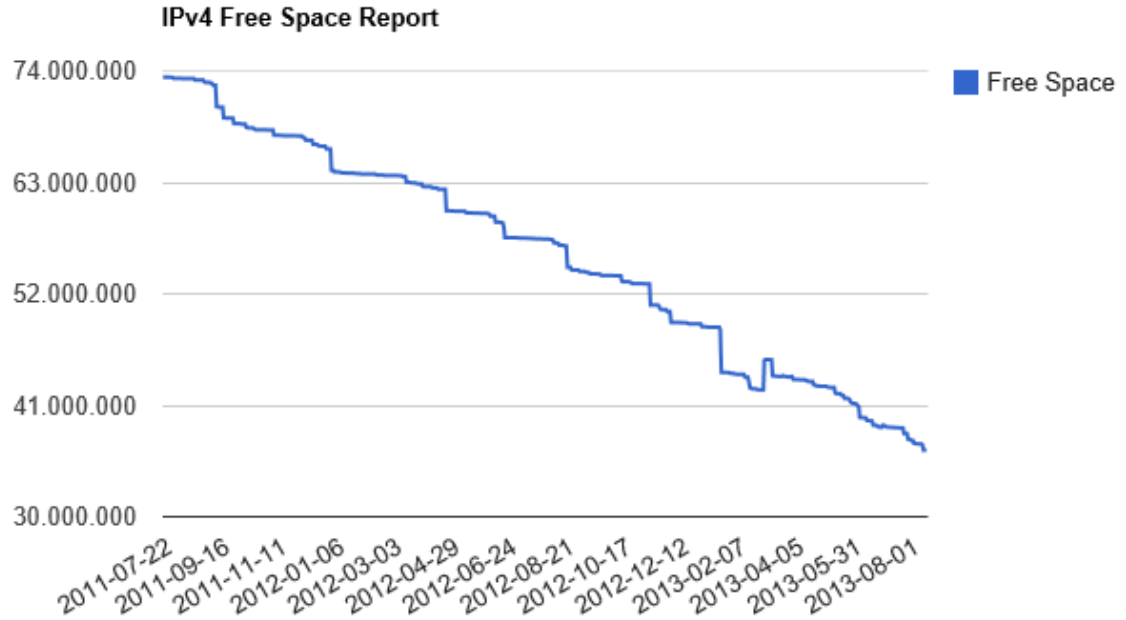
- O crescimento das redes e um possível esgotamento dos endereços IP;
- O aumento da tabela de roteamento;
- Problemas relacionados à segurança dos dados transmitidos;
- Prioridade na entrega de determinados tipos de pacotes.

Por isso a necessidade de criação de um novo protocolo começou a tomar maiores proporções. Sendo assim, em 1990 o IETF (*Internet Engineering Task Force*) iniciou o desenvolvimento de uma nova versão do protocolo, o IPv6 (MARTINI 2003).

A figura 2 abaixo redobra a tese que a internet, por se popularizar muito nos últimos anos, vem esgotando os endereços IPV4.

Figura 2: Esgotamento do IPv4 em nossa região (LACNIC).

Fonte: http://labs.lacnic.net/stats/reports/



3. O protocolo IPV6

O protocolo IPV6 foi originalmente oficializado em 6 de junho de 2012, resultado do esforço do IETF para criar a "nova geração do IP" (*IPng: Internet Protocol next generation*).

O protocolo está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada de "*pilha dupla*" ou "*dual stack*", por algum tempo. A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de 2^{32} = 4.294.967.296 de endereços IP, contra cerca de 2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços do novo protocolo.

O assunto é tão relevante que alguns governos têm apoiado essa implantação. O governo dos Estados Unidos, por exemplo, em 2005, determinou que todas as suas agências federais deveriam provar ser capazes de operar com o protocolo IPv6 até junho de 2008. Em julho de 2008, foi liberada uma nova revisão das recomendações para adoção do IPv6 nas agências federais, estabelecendo a data de julho de 2010 para garantia do suporte ao IPv6. O governo brasileiro recomenda a adoção do protocolo no documento e-PING, dos Padrões de Interoperabilidade de Governo Eletrônico.

O aumento na capacidade de endereçamento é uma das principais inovações do IPv6, que quadruplicou o número de octetos em relação ao IPv4, visto que o tamanho do endereço passou de 32 bits, divididos em 4 octetos, para 128 bits, contendo 16 octetos (MARTINI 2003).

Além de ampliar o espaço de endereçamento, dar segurança na conectividade, o IPv6 acrescenta novas funcionalidades ao IPv4 e altera algumas características, que são (JUNIOR 2005):

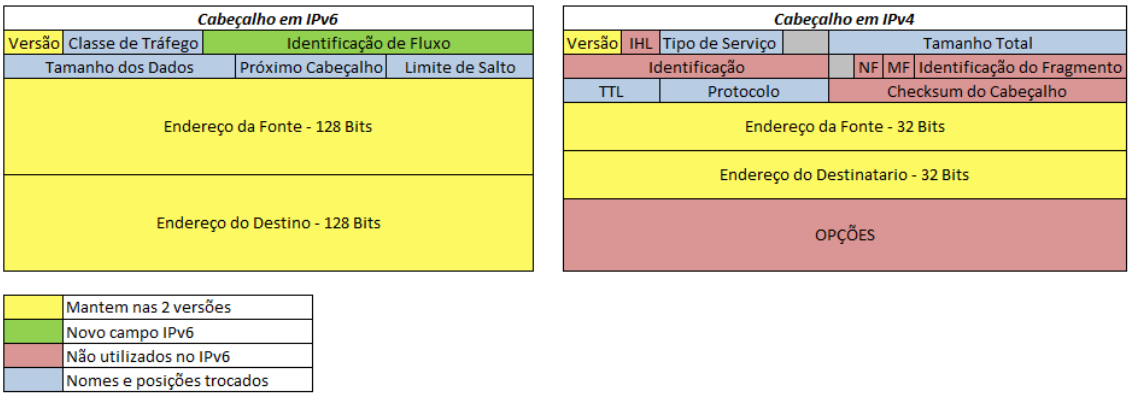
- Simplificação do cabeçalho: vários campos presentes no IPv4 foram suprimidos e outros tornaram–se opcionais. Um cabeçalho mais simplificado implica em menos processamento para cada pacote, sendo extremamente útil para redes de alta velocidade;
- Cabeçalhos de extensão: são inseridos ao cabeçalho base para prover alguns serviços importantes, porém irrelevantes para uma simples troca de informações entre hosts. A forma flexível com que esse cabeçalho foi implementado permite que sejam incluídas novas funcionalidades no futuro;
- Novo formato de endereço: o IPv4 agrupa seus bits em octetos e os representam em decimal, enquanto que o IPv6 agrupa seus bits em oito hexatetos em hexadecimal;
- Rota definida na origem: no IPv4 a rota que era definida durante o envio, na nova versão, passa a ser definida na origem, o que diminui os custos de processamento dos roteadores;
- Suporte a autoconfiguração: permite atribuir automaticamente um endereço IP a um host, o que elimina a necessidade de se configurar manualmente os equipamentos conectados a rede;
- Suporte a endereços *anycast*[4]: no IPv6 foi inserido o endereço *anycast*, que se assemelha a uma junção dos endereços multicast e unicast;
- Roteamento: tem a função de determinar a rota que os pacotes irão percorrer para alcançar seu destino. Essa rota é definida na origem, diminuindo a carga de trabalho dos roteadores intermediários.

Ao observar a figura 3 abaixo, é possível traçar um comparativo entre os dois cabeçalhos, fazendo uma análise das diferenças entre eles, permitindo assim as diversas vantagens apresentadas pelo protocolo IPV6 em relação ao IPV4.

---

[4] Um dos três tipos de endereços definidos no IPV6. O anycast identifica um conjunto de interfaces. Um pacote encaminhado a um endereço anycast é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos. Os outros dois tipos de endereços definidos no IPV6 são: Unicast e Multicast. O Broadcast deixou de existir no IPV6.

Figura 3: Comparando os 2 cabeçalhos.
Imagem retirada de: http://rafaelantunesavila.files.wordpress.com/2011/03/image.png



Para que o protocolo IPv6 alcance a eficiência e a flexibilidade propostas, além do cabeçalho básico, demonstrado na figura 3, foram elaborados cabeçalhos de extensão. Informações opcionais são codificadas nesses cabeçalhos, que são colocados em um pacote entre o cabeçalho IPv6 e o cabeçalho da camada superior (COMER 1998).

Também existem diferenças de funcionamento da fragmentação entre os protocolos.

No IPv4, quando o tamanho do datagrama é maior que o MTU (*Maximum Transfer Unit*) da rede, este é dividido em novos datagramas, copiando-se para o conteúdo do cabeçalho do datagrama original. No cabeçalho das cópias o valor do campo identificação permanece inalterado, identificando os fragmentos do datagrama dividido. Uma observação importante é que os fragmentos trafegam como datagramas isolados até o destino final, sendo que o datagrama é remontado quando todos atingem o destino.

No IPv6, a fragmentação é realizada na própria máquina origem, ao contrário do IPv4 que permitia a fragmentação durante o envio do datagrama. Assim, antes de enviar o datagrama pela rede o IPv6 executa uma técnica de descoberta prévia do caminho identificando a MTU mínima até o destino. A máquina origem fragmenta o datagrama, fazendo com que o mesmo tenha fragmentos de tamanho inferior a MTU identificada.

Esta fragmentação é chamada fim-a-fim, pois nenhuma fragmentação ocorrerá nos roteadores intermediários, havendo uma redução no overhead dos roteadores, possibilitando que os mesmos atendam um número maior de datagramas por unidade de tempo. Quando for necessária uma fragmentação a máquina origem insere um cabeçalho de extensão após o cabeçalho básico (COMER 1998).

No processo de roteamento, também existe uma diferença significante. No protocolo IPv4, quando uma máquina deseja enviar um datagrama, o protocolo encapsula o datagrama e envia ao roteador com menor ou melhor caminho, este extrai o datagrama encapsulado e seleciona o próximo roteador ao longo do caminho do destino, e assim sucessivamente até chegar ao seu destino final.

Ao contrário da versão atual, no IPv6 é permitido que o transmissor especifique uma rota de origem livre, através do uso do cabeçalho de extensão. O cabeçalho contém uma lista de endereços que especificam os roteadores intermediários através dos quais o

datagrama deve trafegar. Entre os campos do cabeçalho de roteamento os mais importantes são:

- O campo número de endereços, que especifica o número total de endereços da lista;
- O campo próximo endereço, que especifica o próximo endereço para o qual o datagrama deverá ser enviado (COMER 1998).

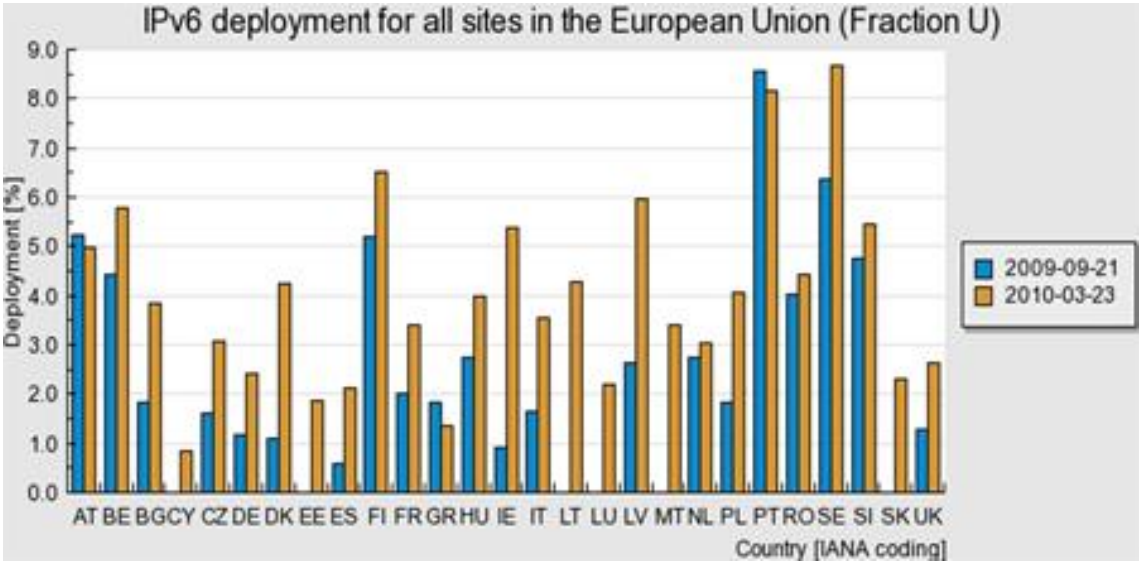
Ou seja, como descrito anteriormente o IPV6 foi projetado com o intuito de resolver o problema de falta de endereços do IPV4, além de cobrir outros problemas que foram surgindo com a larga escala do uso do IPV4, dentre elas, o desafio para os administradores dessa migração a forma segura da transição e da troca das informações fim a fim.

4. O desafio

Como mencionado anteriormente, o objetivo desse artigo é apresentar aos profissionais de TI uma análise sobre os riscos e desafios para a implementação desse novo protocolo principalmente no que se trata de segurança.

A implementação do IPV6 já está se tornando realidade. Como exemplo, a Portugal Telecom deu um passo em frente no sentido da introdução do IPv6 em todas as suas infraestruturas de rede, garantindo uma cobertura total da sua rede no segundo semestre de 2011 e anunciando o início de uma fase piloto dirigida ao segmento empresarial. Mário de Almeida, da Direção de Serviços Especializados ao Cliente, explica que "*o trabalho desenvolvido nos últimos tempos permitiu apresentar aqui hoje alguns resultados. Fizemos uma rede piloto para testarmos uma tecnologia IPv6 para o segmento empresarial. Queremos levar esta rede a clientes que queiram começar a experimentá-la*".

Figura 4: Implantação do IPV6 por país
Fonte:
http://www.telecom.pt/InternetResource/PTSite/PT/Canais/Media/DestaquesHP/Destaques_2010/ipv6estrategiapt.htm



Embora ainda seja pequena, a utilização do IPv6 tem aumentado gradativamente, porém precisa avançar ainda mais. A não implementação do IPV6 poderá acarretar problemas como:

- Dificuldade com o surgimento de novas redes;
- Diminuição do processo de inclusão digital o reduzindo o número de novos usuários;
- Dificuldade do surgimento de novas aplicações;
- Aumento da utilização de técnicas como a NAT;
- O custo de não implementar o IPv6 poderá ser maior que o custo de implementá-lo;
- Provedores Internet precisam inovar e oferecer novos serviços a seus clientes.

Ou seja, adiar por mais tempo a implantação do IPv6 pode trazer diversos prejuízos para o desenvolvimento de toda a Internet (SANTOS 2010).

Alguns itens se tornam cada vez mais desafiadores para os profissionais de TI, tais como:

- Quais técnicas de transição implementar?;
- Sistemas de autoconfiguração e descoberta de vizinhança;
- Modelos fim a fim e mobilidade IPV6;
- Ferramentas, melhores práticas, politicas, treinamentos, como gerenciar?;
- Implementação de segurança.

A transição para o novo protocolo demanda tempo, sendo que sistemas IPv6 terão que coexistir com sistemas rodando em estrutura IPv4, para que a transição ocorra gradualmente. As máquinas com infra-estrutura IPv6 deverão inter-relacionar-se com máquinas IPv4.

Sendo assim, mecanismos devem ser criados para que as regiões IPv4 interajam entre si através das regiões IPv6.

Para que a migração aconteça de forma suave e incremental foram desenvolvidos mecanismos que possibilitam tal tarefa, entre estes podem ser citados, pilha dupla, túnel IPv4/IPv6 e tradução IPv4/IPv6 (MARTINI 2003).

4.1. Pilha Dupla

A função da pilha dupla é prover um suporte a ambos os protocolos no mesmo dispositivo. A idéia básica é fazer com que um nó IPv6/IPv4, ao se comunicar com um nó IPv6, se comporte como um nó IPv6 e na comunicação com um nó IPv4, como um nó IPv4. Cada protocolo possuirá seus próprios mecanismos para adquirir seus endereços. Porém alguns aspectos também devem receber uma análise mais criteriosa como (JUNIOR 2005):

- Configuração dos servidores DNS;
- Configuração dos protocolos de roteamento;

- Configuração dos firewalls;
- Mudanças nos gerenciamentos de redes.

4.2. Túnel IPV4 e IPV6

As técnicas de tunelamento também são conhecidas como encapsulamento (JUNIOR 2005). A principal tarefa é prover o tráfego do IPV6 em túneis IPV4, ou seja, que permitam o transporte dos pacotes IPV6 através da infraestrutura IPV4 existente, sem a necessidade de mudanças nos mecanismos de roteamento. Algumas formas de encapsulamento são mais conhecidas como: protocolo 41, 6to4, ISATAP e Tunnel Brokers. Vale também comentar que existem os processos de tunelamento IPV6 em pacotes GRE (utilizando protocolo GRE) e também pacotes IPV6 encapsulados em pacotes UDP, através do protocolo TEREDO.

4.3. Tradução IPV4 e IPV6

Por meio das técnicas de tradução, é possível fazer um roteamento transparente entre nós de uma rede IPV6 com nós em uma rede IPV4 e vice-versa. Dentre essas técnicas de tradução, podem ocorrer:

- Tradução de cabeçalhos IPV4 em cabeçalhos IPV6 e vice-versa;
- Realização de conversões de endereços;
- Conversões de APIs de programação;
- Atuações na troca de tráfego TCP ou UDP.

Dentre os recursos existentes, são exemplos: SIIT (*Stateless IP/ICMP Translation Algorithm*), BIS (*Bump-in-the-Stack*), BIA (*Bump in the API*), TRT (*Transport Relay Translator*), ALG (*Application Layer Gateway*) e DNS-ALG.

4.4. A segurança

O tráfego ininterrupto de informações atualmente na internet expõe as informações a ataques e cópias indevidas. Para que se possa obter um nível mais elevado de segurança na comunicação, mecanismos lógicos para proteger os dados através de controle de acesso, detecção de intrusos, criptografia entre outros, deve ser implementado e aprimorado continuamente. Também não menos importante é a proteção ao acesso físico, permitindo, por exemplo, que poucas pessoas tenham acesso aos principais equipamentos como roteadores de borda, servidores, entre outros.

Dentro da classe de mecanismos lógicos, o IPV4 não oferece, por padrão, segurança dos dados em nível de rede. Os dados podem ser facilmente capturados, por *snniffers* (scanners de rede), que são programas destinados à captura de datagramas que estão trafegando na rede, permitindo a visualização dos dados. Além disso, os sistemas podem sofrer ataques, que são acessos indevidos ao sistema, em que o invasor poderá capturar, alterar ou destruir as informações (JUNIOR 2005). Alguns ataques mais comuns que ocorrem:

- Spoofing: personificação de endereço IP, o que permite que um host qualquer possa se passar por outro, modificando o endereço IP do host origem;

- DOS-DDOS: negação de serviço. Por causa da sobrecarga ocasionada pela repetição de alguma solicitação, o servidor ("alvo") é forçado a parar o serviço que disponibiliza.

Sendo assim, o grupo de segurança da IETF5 iniciou o projeto de um conjunto de padrões voltados à segurança sobre o IP, que foi chamado de *IP Security Protocol* (IPSec) com objetivo de prover segurança no tráfego de dados pela rede com o auxílio da criptografia, fornecendo proteção tanto ao pacote IP quanto às camadas superiores.

Para que sejam alcançados os objetivos do IPSec, é necessária à utilização de protocolos de tráfegos seguros, que são: *Authentication Header*(AH) e *Encapsulating Security Payload*(ESP) e de procedimentos e protocolos de gerência de chaves (IKE). Porém, por ter uma arquitetura aberta, o IPSec possibilita a inclusão de outros algoritmos de autenticação e criptografia (JUNIOR 2005).

O IPV6 provê uma segurança conhecida como segurança nativa provida pelo protocolo IPSec, na tentativa de definir uma solução global para o problema da falta de segurança na internet.

Vale ressaltar aos leitores que a proposta desse artigo é apresentar apenas uma análise técnica das defesas possíveis de implementação para a segurança da rede utilizando IPV6, ou seja, fica a recomendação de um estudo mais aprofundado sobre qualquer um dos aspectos aqui apresentados, se assim for o desejo do leitor.

O IPv6 oferece outras ferramentas tanto para defesa, quanto para o ataque que merecem destaque.

Para a defesa:

- O próprio IPsec;
- SEND;
- Crypto-generated Address;
- Unique Local Addresses;
- Privacy Addresses.

Para o ataque:

- Túnel automático;
- Neighbor Discovery e autoconfiguração;
- Modelo fim a fim;
- Novidade / Complexidade;
- Falta de políticas, treinamentos e ferramentas.

---

[5] IETF sigla para Internet Engineering Task Force é uma comunidade internacional (técnicos, agências, fabricantes, fornecedores, pesquisadores) preocupada com a evolução da arquitetura da internet e seu perfeito funcionamento. Tem como missão identificar e propor soluções a questões/problemas relacionados à utilização da Internet, além de propor padronização das tecnologias e protocolos envolvidos. As recomendações da IETF são usualmente publicadas em documentos denominados RFCs (Request for Comments), sendo que o próprio IETF é descrito pela RFC 3160 (IETF 2013).

De acordo ainda com SANTOS (2010), deve-se ainda observar outras medidas eficazes para tornar uma transação mais segura via IPV6, na internet:

- Ter preocupação com segurança e envolver a equipe de segurança desde o início;
- Obter equipamentos certificados;
- Educação / Treinamento;
- Fazer upgrade das ferramentas e processos de segurança;
- Desenvolver práticas de programação adequadas (e seguras) para IPv6;
- Procurar auditorias / equipes de teste que conheçam IPv6.

Algumas outras recomendações importantes para o administrador de redes internet é analisar que com a utilização de Pilha Dupla as aplicações ficam expostas aos ataques a ambos os protocolos, IPv6 e IPv4, o que pode ser resolvido configurando firewalls específicos para cada protocolo. As recomendações sugeridas (SANTOS 2010):

- As técnicas de Túneis e Tradução são as que causam maiores impacto do ponto de vista de segurança;
- Mecanismos de tunelamento são suscetíveis a ataques de DoS, falsificação de pacotes e de endereços de roteadores e relays utilizados por essas técnicas, como 6to4 e TEREDO;
- As técnicas de tradução implicam em problemas relacionados a incompatibilidade dessas técnicas com alguns mecanismos de segurança existentes. Similar ao que ocorre com o NAT no IPv4.

Para se proteger:

- Utilizar pilha dupla na migração, protegendo as duas pilhas com *firewall*;
- Dar preferência aos túneis estáticos, no lugar dos automáticos;
- Permitir a entrada de tráfego apenas de túneis autorizados.

Dentre todas as propostas apresentadas aqui nesse artigo, baseado em estudos realizados pelos autores citados, vale ressaltar a construção de uma eficiente política de segurança, poisu de nada adianta uma implementação IPV6 de forma ineficiente e desorganizada. Uma política de segurança é um instrumento importante para proteger a organização contra ameaças à segurança da informação e pertence ou está sob a responsabilidade de um administrador. A política de segurança não define procedimentos específicos de manipulação e proteção da informação. Por isso pode se tornar uma ferramenta eficaz na implementação ou transição do IPV6. Desta forma, a política pode definir as expectativas que podem ter quanto à segurança e quais são as atribuições em relação à segurança das informações e pacotes que trafegam pela rede mundial, estipulando, inclusive, as penalidades às quais estão sujeitos aqueles que a descumprem.

NIC BR (2003) apresenta um modelo de criação de política de segurança, ficando uma forte recomendação ao acesso dessas informações.

4. Considerações finais

Esse artigo teve a proposta apenas de divulgar algumas informações a respeito de novos conhecimentos sobre o protocolo IPV6 para os administradores que estejam interessados na migração dos serviços sobre sua administração, considerando, além de todas as complexidades apresentadas, o quesito segurança.

O projeto IPV6 apresentado aqui tem algumas vantagens sobre o IPV4, sendo que uma das mais importantes é o fato de apresentar segurança mandatária, instituída pela IETF com o intuito de reduzir a vulnerabilidade na troca de dados pela internet. Porém, muito ainda tem que ser estudado, pesquisado e desenvolvido, pois não existe uma base sólida comprovada que possa garantir que realmente o protocolo IPV6 é mais seguro que o IPV4, sendo assim, um fator muito importante é a criação das políticas de segurança claras.

Várias formas de implementação de segurança como, por exemplo, o IPSec, foi sugerido nesse trabalho, justamente com o intuito de estimular os administradores de internet aprofundarem os estudos e encontrar uma melhor técnica que adeque as suas necessidades.

Mesmo utilizando túneis, o fato do IPV6 apresentar uma extensão maior no seu endereço, já demonstra um grande passo em busca de maior eficiência, de acordo com os estudos realizados.

Também através do estudo realizado, pôde-se verificar que a migração para o IPV6 já está acontecendo por necessidade, visto que o protocolo IPV4 não foi projetado para suportar o atual momento que se encontra o mundo tecnológico. No Brasil, o NIC BR (2010) vem apresentando diversos estudos técnicos e teóricos do funcionamento do IPV6.

Espera-se que através das análises das informações apresentadas, os administradores de internet consigam obter informações para realizarem a transição ou a implementação de uma forma segura, seguindo as políticas de segurança interna das empresas e também legislações vigentes, aplicando orientações aos usuários e gerenciamento de sua rede interna de forma eficaz, possibilitando assim a divulgação cada vez maior do conhecimento desse novo protocolo.

5. Referências

BARBOSA, D. P. ; COAN, A. L. ; NOVAIS, T. M.; NISHIJIMA, M. Implicações de Externalidades Negativas da Internet sobre a Legislação Brasileira de Crimes no Ciberespaço: o Caso de Ataques por Negação de Serviço. Fundação Instituto de pesquisas econômicas, v. 1, p. 29, 2012.

COMER, D. E. Interligação em redes com TCP/IP. Rio de Janeiro , ed. Campus, 1998.

JUNIOR, L. G.; SOUZA, J. P. L.; NUNES, R. M.; BOGO, M. Análise da segurança em redes puramente IPV6. VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005.

Histórico da Internet. Disponível em: http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet. Acesso em: 18/08/2013.

MARTINI, F. Z.; BOGO, M. Análise e proposta de implementação de um ambiente de rede utilizando o protocolo IPV6. Anais do V Encontro de Estudantes de Informática do Tocantins. Palmas, TO. outubro, 2003. pp. 381-390.

NIC BR, S. O. Práticas de segurança para administradores de redes Internet. Disponível em: http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf, São Paulo, 2003.

SANTOS, R. R; MOREIRAS, A. M.; REIS, E. A.; ROCHA, A.S. Curso básico de IPV6. Núcleo de informação e coordenação do ponto BR, São Paulo, 2010.