Segurança em tunelamento IPv6

Christovam Paynes Silva[1], **Luis A. D. Knob**[1], **Amilton Martins**[1], **Fahad Kalil**[1]

[1]Faculdade Meridional- IMED
Rua Senador Pinheiro, 304 – Passo Fundo – RS – Brazil

{christovam.paynes,luis.knob,amilton,fahad.kalil}@imed.edu.br

Abstract. *The transition from IPv4 to IPv6 is a reality , and it has become possible due to the development of various transition mechanisms , these techniques are termed as Tunneling , and Translation Dual Stack . As this transition is delayed , it is quite likely to take years to complete . The tunnels have become common for the deployment of IPv6 , however these techniques bring several vulnerabilities which can be used for any type of attack. Intruders can spoof packets by changing its source and injecting them directly into the ends of the tunnel , DOS techniques are possible or even packages that can evade firewalls encapsulated within other packages. Thus this study aims to demonstrate a security flaw in the 6over4 and that the use of IPv6 tunnel with IPSec provides a satisfactory solution to this attack.*

Resumo. *A transição do protocolo IPv4 para o IPv6 é uma realidade, e tem se tornado possível devido a elaboração de diversos mecanismos de transição, estes são denominados como técnicas de Tunelamento, Tradução e Pilha Dupla. Como esta transição está atrasada, é bem provável que demore anos para se completar. Os túneis se tornaram comuns para a implantação do IPv6, no entanto estas técnicas trazem diversas vulnerabilidades as quais podem ser utilizadas para algum tipo de ataque. Intrusos podem falsificar pacotes alterando sua origem e os injetando diretamente nas extremidades do túnel, técnicas de DOS são possíveis ou até mesmo pacotes que podem escapar dos firewalls encapsulados dentro de outros pacotes. Desta forma este trabalho tem como objetivo demonstrar uma falha no túnel 6over4 e que a utilização de um túnel IPv6 com IPSec traz uma solução satisfatória para este ataque.*

1. Introdução

A implantação do IPv6 faz parte da agenda das maiores empresas de comunicação e provedores de serviço do mundo, pelo eminente esgotamento dos endereços IPv4 existentes. O acesso à internet, principalmente pelos países em desenvolvimento, e a evolução constante dos meios de comunicação, contribuem substancialmente para o interesse atual tanto da academia como das empresas sobre esta questão.

Embora a necessidade para a alteração da versão do protocolo sustentador de toda a Internet seja fundamental, o alto custo de implementação de uma solução não compatível com a atual, torna necessário a introdução de diversas técnicas de transição, como o tunelamento, a pilha dupla e a tradução de endereços. Essas técnicas foram desenvolvidas para que ambos protocolos possam conviver até a migração final.

As técnicas de tunelamento, embora muito utilizadas, podem apresentar diversas falhas de segurança, por isso neste trabalho será realizado um estudo para demonstrar

uma falha na requisição de pacotes a um endereço dentro de um túnel 6over4, além de comprovar a eficácia do uso de IPSec para garantir a segurança destas conexões.

O trabalho está organizado da seguinte maneira: Na seção 2 os trabalhos relacionados são apresentados; na Seção 3 é feito uma revisão sobre a técnica de tunelamento utilizada; a Seção 4 apresenta os experimentos que foram realizados; finalmente, a Seção 5 apresenta a conclusão e trabalhos futuros.

2. Artigos Relacionados

Diversos trabalhos já foram realizados sobre segurança em tunelamento e em redes IPv6, dentre eles podemos citar, o trabalho *Securing Tunnel Endpoints for IPv6 Transition in Enterprise Networks* [Taib and Budiarto 2010] mostra que o uso de túneis são inseguros e permitem que intrusos falsifiquem o endereço de origem de um pacote e façam a injeção do mesmo na extremidade do túnel. O autor também utilizou de filtros separados para filtrar os pacotes IPv4 e IPv6, afim de evitar que nenhum pacotes fuja do filtro. Porém o uso do IPSec pode mitigar este problema, pois irá autenticar o pacote de entrada do túnel.

No trabalho *A Secure Packet Filtering Mechanism Tunneling* [Lee et al. 2007] devido a problemas de filtragem em pacotes encapsulados, os autores propõem um novo mecanismo de filtragem de pacotes. Como os pacotes encapsulados tem cabeçalhos IP duplos, alguns firewalls aplicam as regras apenas nos cabeçalhos exterior. Para resolver este problema foi implementada uma filtragem de pacotes baseada no Netfilter do Linux. Uma função específica investiga se o pacote está encapsulado ou não, caso seja positivo, a função envia o pacote para as tabelas do ip6tables e iptables para realizarem os filtros desta forma o pacote interior não escaparia do filtro.

O trabalho *Security Mechanisms for the IPv4 and IPv6 Transition* [Taib and Budiarto 2007], se concentra em destacar as principais vulnerabilidades em túneis e identifica os mecanismos de prevenção para os problemas identificados. Também tem por finalidade usar firewall para realizar a filtragem dos pacotes.

Em *Security in IPv6* [Yang et al. 2010], os autores remetem ao entendimento básico dos mecanismos de segurança comuns, tais como ataques e IPSec. São os tipos de ataques mais comuns inclusive no modo IPSec e realiza uma série de orientações de como proteger a camada IP.

O trabalho *Routing Loops Attacks Using IPv6 Tunnels* [Nakibly and Arov 2009], mostra uma nova categoria de ataque em túneis. Estes ataques aproveitam a inconsistência entre a sobreposição de roteamento IPv6 do túnel e do roteamento IPv6 nativo. Esses ataques formam loops de roteamento que em pouco tempo causa uma Negação de Serviço (DOS, do inglês *Deny of Service*) no túnel. Em um ataque apresentado em um túnel TEREDO, foi realizado um DOS usando apenas um pacote. Os ataques foram testados contra implementações ISATAP, 6to4 e TEREDO no Windows Vista e Server 2008 R2.

3. Túneis 6over4

A técnica 6over4 definida pela RFC2559, é composta por um túnel configurado manualmente que estabelece um canal entre dois nós IPv4, e tem a finalidade de enviar o tráfego IPv6 entre as extremidades. As técnicas de tunelamento fazem o encapsulamento de pacotes IPv6 em pacotes IPv4. Esse encapsulamento é conhecido como 6in4 ou IPv6-in-IPv4 de acordo com a RFC 4213.

No campo cabeçalho são inseridos os endereços de origem e destino para o IPv4 e o tipo 41, responsável por indicar que se trata de uma pacote IPv6 dentro de um pacote IPv4. Desta forma, o destinatário sabe que pacotes com o tipo 41 utilizam encapsulamento 6in4 e irá remover o cabeçalho IPv4 e tratar o IPv6. Esse encapsulamento permite o transporte do pacote até a outra ponta do túnel, entrando então na rede IPv6 do usuário.

Por possuir uma estrutura de encapsulamento não criptografado sobre a camada de rede é possível modificar o caminho de um pacote como se tivesse iniciado a partir de outro computador, através da técnica de IP spoofing, nos túneis IPv6. Uma forma de dificultar este ataque é utilizar criptografia no encapsulamento, não permitindo a modificação dos campos dentro do pacote. Por isso, a implementação IPsec é a resposta para essas falhas de segurança. O IPsec fornece integridade, confidencialidade, e proteção de origem entre extremidades do túnel 6over4.

Além disso, pode-se configurar Unicast Resvere Path Forwarding (Unicast RPF) nas interfaces seriais e dos túneis, para não permitir a formação de conexãos IPSec em outras interfaces. E também adicionar uma lista de acesso na interface externa, de forma a proibir conexões IPSec de outros dispositivos não autorizados. Através das associações de segurança, conseguimos diminuir problemas como injeção de pacotes IPv4 e falsificações de endereço.

4. Experimentos e análises

Nesta seção são descritos dois experimentos como estudos de caso. Ambos se concentram na implementação do túnel 6over4. O objetivo é mostrar a importância na implementação o protocolo IPSec no túnel, para garantir a segurança da conexão. Para a realização dos testes foi utilizada a distribuição Linux Fedora 18 com kernel 3.10.12-100,fc18.x86_x64 e instalada a ferramenta Common Open Research Emulator (CORE) na versão 4.6.1. O CORE permite construir todo o cenário e trabalhar com protocolos e aplicações autênticas em tempo real.

4.1. Estudo de caso 1

No primeiro estudo de caso é apresentado uma topologia, que demonstra a interligação da rede da Matriz com a da Filial. Observando, percebe-se que existem alguns roteadores no caminho e com segmentos de redes diferentes. Isso foi propositalmente inserido para poder demonstrar um cenário mais próximo da realidade, com diversos NATs, segmentos e conexões de redes diferentes, ao longo do caminho que o pacote percorre dentro do túnel 6over4.

Conforme mostra a Figura 1, temos a topologia que liga a Matriz e Filial. Essa ligação é realizada a partir do roteador com ip final 10:1 até o roteador com ip final 20:1, de forma a simular uma conexão de cliente-servidor. Foi então configurado o túnel 6over4 e sem o IPSec.

Após a configuração do cenário, foi realizado a falsificação do endereço IP para ser enviado da máquina atacante até a matriz. Para isto, foi utilizado a ferramenta thcping6 que faz parte da ToolKit do grupo THC [1].

[1] https://www.thc.org/

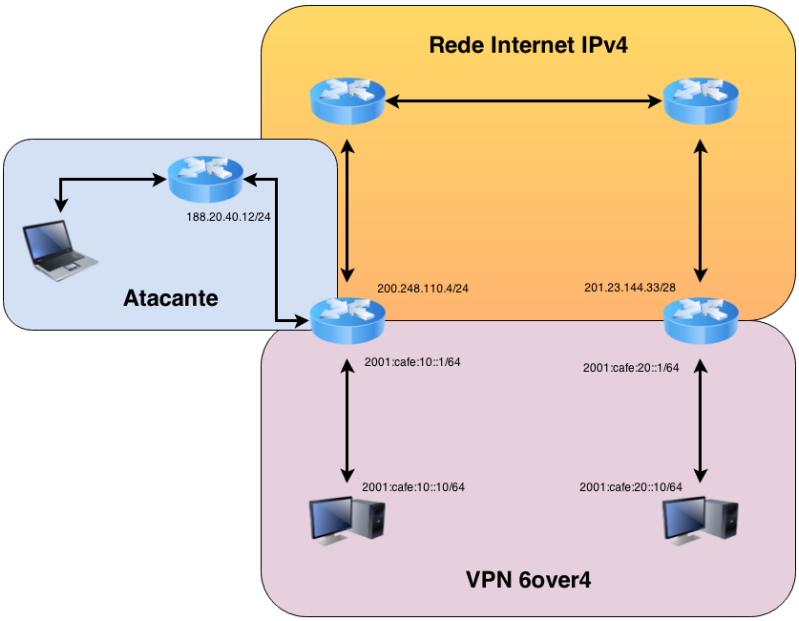

Figura 1. Topologia do Cenário

Na Figura 2, demonstra a utilização do thcping6 enviando um pacote ICMPv6 *echo request* para a Matriz, perceba que o envio está sendo realizado do host Atacante. A mensagem *No packet received, terminating*, avisa que não obteve uma resposta *echo reply* do host Matriz. Porém a intenção é essa mesma, conforme a sintaxe do comando quem vai receber está resposta, é o cliente com ip final 20:10.

Figura 2. Uso da aplicação thcping6

A Figura 3, mostra o *echo reply* sendo enviado do servidor para a cliente, embora o cliente não tenha realizado nenhuma solicitação. A máquina do Atacante conseguiu forjar o pacote e enviá-lo com sucesso. Pode-se observar a sequência numérica onde o número 1, mostra que existe um pacote IPv4 e o número 2 possui em seu campo Procotol o valor 41. Isso comprova que existe um pacote IPv6 encapsulado neste pacote IPv4. O número 3 mostra o pacote IPv6 com os IPs de origem e destino. Conforme o número 4, o campo Next Header informa que este pacote é um pacote ICMPv6.

4.2. Estudo de caso 2

No segundo estudo de caso, é proposto a implementação do IPSec entre os servidor e o cliente da VPN. A finalidade é fortalecer o túnel 6over4, com o intuito de eliminar as a falha apresentada anteriormente.

Esta solução tem a finalidade de criptografar todo o tráfego dentro do túnel. Assim, o pacote só será aceito na rede de destino se possuir um cabeçalho de autenticação IPSec. O cenário deste estudo de caso, é igual ao do estudo de caso 1.

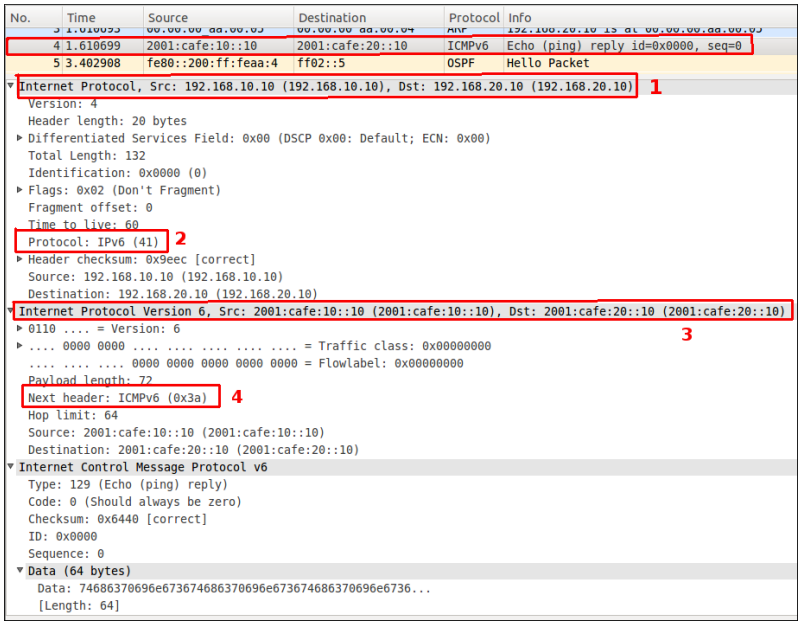

Figura 3. Captura da comunicação no roteador de borda

A Figura 4 mostra uma coleta dos dados com a ferramenta Wireshark no mesmo momento em que foi disparado um pacote ICMPv6 de echo-reply com o comando ping6 e interceptado o pacote no Roteador com ip final 10::1. Pode-se observar que do número 1 ao 3 temos praticamente as mesmas informações. Porém nesta captura temos uma diferença a partir do pacote IPv6 (número 3), o número 4 está mostrando que o pacote está criptografado, desta forma não sendo possível ver seu conteúdo ou qual o tipo de pacote que está encapsulado. Diferente do estudo de caso 1, onde mostrava no campo *Next Header* que o pacote era do tipo ICMPv6.

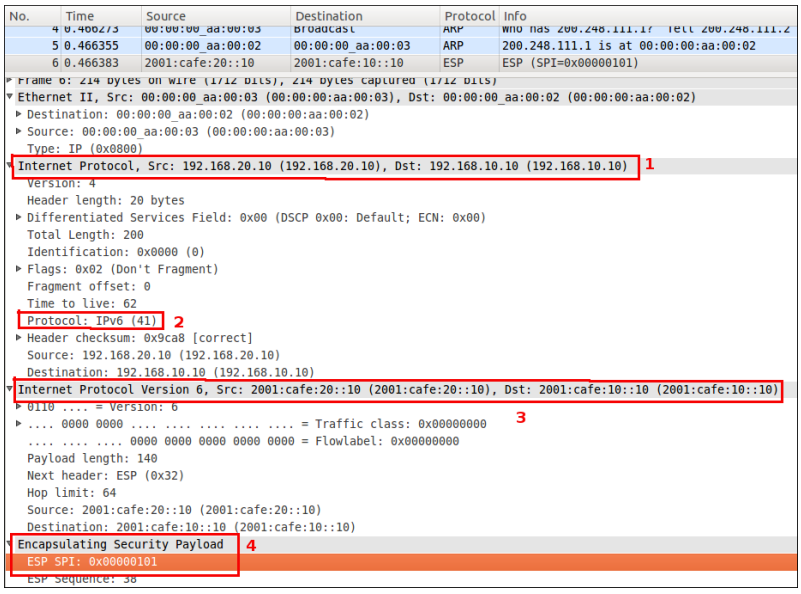

Figura 4. Captura com IPSec

5. Conclusão

Ambos experimentos mostraram a importância em ter boas práticas de implementação e muito cuidado com essa nova tecnologia. Sabendo que a mesma é de fato importante e que deverá ser implementada por completo nos próximos anos, a atenção deve ser redobrada.

O primeiro experimento mostrou uma falha preocupante, que pode servir para ataques mais profundos nos ambientes, possibilitando a captura de informações importantes através de outras ferramentas não apresentadas ou a negação de um serviço.

No segundo experimento, comprova que o IPSec é indispensável em uma implementação IPv6, principalmente quando utilizada em conjunto com técnicas de tunelamento. Quando colocado à prova, o comportamento do host ao receber um pacote que não estava autenticado e nem criptografado na entrada do túnel foi descartá-lo.

Entre os trabalhos futuros estão a realização de testes mais complexos, como o envio de informações dentro do túnel utilizando outros protocolos como o FTP. Além disso, outros tipos de túnel podem ser testados como o 6rd e o Teredo.

Referências

Lee, W.-J., Heo, S.-Y., Byun, T.-Y., Sohn, Y.-H., and Han, K.-J. (2007). A secure packet filtering mechanism for tunneling over internet. In Lee, Y.-H., Kim, H.-N., Kim, J., Park, Y., Yang, L., and Kim, S., editors, *Embedded Software and Systems*, volume 4523 of *Lecture Notes in Computer Science*, pages 641–652. Springer Berlin Heidelberg.

Nakibly, G. and Arov, M. (2009). Routing loop attacks using ipv6 tunnels. In *Proceedings of the 3rd USENIX Conference on Offensive Technologies*, WOOT'09, pages 7–7, Berkeley, CA, USA. USENIX Association.

Taib, A. and Budiarto, R. (2007). Security mechanisms for the ipv4 to ipv6 transition. In *Research and Development, 2007. SCOReD 2007. 5th Student Conference on*, pages 1–6.

Taib, A. and Budiarto, R. (2010). Securing tunnel endpoints for ipv6 transition in enterprise networks. In *Science and Social Research (CSSR), 2010 International Conference on*, pages 1114–1119.

Yang, D., Song, X., and Guo, Q. (2010). Security on ipv6. In *Advanced Computer Control (ICACC), 2010 2nd International Conference on*, volume 3, pages 323–326.