

**UNIVERSIDADE PAULISTA - UNIP**

**GUILHERME RAVELI FURQUIM**

**ANÁLISE DE SEGURANÇA DE DADOS: IPV4 VS IPV6.**

**LIMEIRA  
2017**

**UNIVERSIDADE PAULISTA - UNIP**

**GUILHERME RAVELI FURQUIM**

**ANÁLISE DE SEGURANÇA DE DADOS: IPV4 VS IPV6.**

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor Me. Antonio Mateus Locci e Me. Sergio Eduardo Nunes.

**Limeira  
2017**

## **GUILHERME RAVELI FURQUIM**

### **ANÁLISE DE SEGURANÇA DE DADOS: IPV4 VS IPV6.**

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da Computação sob a orientação do professor Me. Antonio Mateus Locci e Me. Sergio Eduardo Nunes.

Aprovada em XX de XXXXX de 201X.

#### **BANCA EXAMINADORA**

---

Prof. Dr. Nome completo

---

Prof. Me. Nome completo

---

Prof. Esp. Nome completo

## DEDICATÓRIA

Dedico esse trabalho á Deus, por todas as vezes que me ajudou e me levantou quando eu caí. Agradeço meus professores pelo desenvolvimento acadêmico. Agradeço meus orientadores Antonio Mateus Locci e Sergio Eduardo Nunes por toda paciência, compreensão e orientação. Agradeço minha mãe e minha namorada por todo apoio e força desde o início da minha jornada acadêmica na universidade. Agradeço ao Renan Gonsalves Maia por toda ajuda, prontidão e dedicação junto ao desenvolvimento. Agradeço ao Thiago Martins pela orientação e ajuda quanto á teoria.

*"Para se ter sucesso, é necessário amar de verdade o que se faz. Caso contrário, levando em conta apenas o lado racional, você simplesmente desiste. É o que acontece com a maioria das pessoas."*

(Steve Jobs.)

## **RESUMO**

Desde o princípio da internet, o maior desafio era a conexão e comunicação entre os computadores, sem qualquer preocupação com segurança ou desempenho. Surgiu o protocolo IP versão quatro, denominado hoje como o IPV4 para que essa necessidade fosse atendida. Com o passar do tempo, segurança e desempenho se tornaram totalmente indispensáveis em praticamente toda comunicação pela internet e o IPV6 apresenta-se como a nova solução para tais problemas. Esse trabalho tem o intuito de usar o Wireshark para comparar as varreduras entre os protocolos IPV4 e IPV6.

Palavra-Chave: IPsec; IPV4; IPV6; Servidor; Wireshark.

## **ABSTRACT**

From the beginning of the internet, the biggest challenge was the connection and communication between computers, without any concern for security or performance. The IP protocol version four, known today as IPV4, appeared for this demand to be met. Over time, security and performance have become absolutely indispensable in virtually all Internet communication and IPV6 is the new solution to such problems. This assignment intends to use Wireshark to compare scans between the IPV4 and IPV6 protocols.

Key Words: IPsec; IPV4; IPV6; Server; Wireshark.

## LISTA DE FIGURAS

<a href="#">Figura 01 – Integração de três protocolos principais do IPsec</a> .....	13
Figura 02 – Roadmap para documentos IPsec .....	13
Figura 03 – Esgotamento do IPV4 em 30 de Novembro de 2010 .....	15
Figura 04 – Gráfico do esgotamento dos endereços IPV4, entre 2000-2011 .....	16
Figura 05 – Diferenças notáveis entre o IPV4 e IPV6 .....	18
Figura 06 – Painel principal do FileZilla Server no computador “Servidor” .....	20
Figura 07 – Tela de criação de usuário do FileZilla Server no computador “Servidor”. 20	
Figura 08 – Pastas compartilhadas com o usuário do FileZilla Server para o FileZilla Client no computador “Servidor” .....	21
Figura 09 – Painel principal do FileZilla Client no computador “Cliente” .....	22
Figura 10 – Mudança na tela do FileZilla Server após a conexão do usuário no servidor no computador “Servidor” .....	23
Figura 11 – Wireshark capturando packets da rede sem fio “Rede maliciosa” no computador “Wireshark” .....	24
Figura 12 – Comandos no Prompt de Comando com privilégios de administrador para inicializar o processo de transferência de arquivos FTP no computador “Cliente” .....	25
Figura 13 – Captura do arquivo “Ray.2004.mp4” em IPV4 no computador “Wireshark” .....	25
Figura 14 – Captura de IP origem e destino e notificação da transferência de arquivo FTP “Ray.2004.mp4” no computador “Servidor” .....	26
Figura 15 – Captura IPV6 com IPsec ativado no computador “Servidor” .....	26
Figura 16 – Dados da Captura IPV6 com IPsec ativado no computador “Servidor” ....	27
Figura 17 – Dados da Captura IPV6 com IPsec ativado no computador “Servidor” (Destino e Origem) .....	27
Figura 18 – Dados Detalhados da Captura IPV6 com IPsec ativado no computador “Servidor” .....	27

## SUMÁRIO

INTRODUÇÃO.....	10
1. Objetivo .....	11
1.1 Metodologia .....	11
2. IPSEC.....	12
2.1 Arquitetura IPsec .....	13
2.2 Cabeçalho ESP .....	14
3. IPV4 e suas limitações.....	15
4. IPV4 vs IPV6.....	16
4.1 Segurança .....	17
4.2 Qualidade de Serviços .....	17
4.3 Principais diferenças entre os protocolos IPV4 e IPV6.....	18
5. Desenvolvimento .....	19
CONCLUSÃO .....	28
REFERÊNCIAS BIBLIOGRÁFICAS.....	30

## INTRODUÇÃO

Quando se trata de internet, o assunto abrange várias áreas dentro de TI. Um dos maiores problemas que aparecem hoje na área de TI é de fato a segurança. Seja ela em redes, programação, stream de dados (jogos, filmes, músicas, imagens etc). A segurança sempre foi um fator muito pertinente a qualquer área, não somente em TI. Hoje temos vários recursos para combater e prevenir a insegurança (teclados virtuais para bancos, biometria por impressão digital para desbloqueio de celulares e acesso a contas em bancos, reconhecimento facial ou reconhecimento vocal para desbloqueio de dispositivos sonoros etc), mas não temos nada que definitivamente aniquila a insegurança em todas as áreas da computação.

Quando se trata de redes, temos o IPsec. O IPsec é um protocolo de segurança de IP, ou, do inglês, Internet Protocol Security. O IPsec é uma alternativa para combater a insegurança de rede. Ela é uma alternativa de camada de rede que possui o intuito de proteger o tráfego de dados na Internet. O protocolo de internet versão 6 (IPV6) possui o IPsec nativamente como parte de seu funcionamento, porém, para usá-lo, é necessário que a função seja habilitada no roteador. O IPV6 possui suporte nativo para IPsec, mas não é automático seu funcionamento. Atualmente, existem várias ferramentas e programas nos dias de hoje que permitem a captura total ou não de dados que trafegam pela Internet. No caso, isso é chamado de sniffer, do inglês. Um sniffer é como o nome diz, um "farejador". No caso, o sniffer fareja seus dados que passam pela rede. Na maioria dos casos, eles são utilizados por analistas e administradores de redes para identificarem dados ou pacotes duvidosos passando pela rede manuseada por eles ou mesmo por indivíduos tentando obter informações sensíveis, como senhas de acesso. E o IPV4 não tem nenhuma proteção contra isso, diferente do IPV6.

O IPsec nesse caso para o IPV4 se tornou uma opção inviável pela sua dificuldade de implementação. O IPsec é opcional no IPV4, mas exige um conhecimento muito grande em programação, pois é necessário reprogramar o IPV4 para que o protocolo de segurança seja colocado. Inclusive, foi justamente daí que surgiu a necessidade de uma nova tecnologia que eliminasse esses

problemas de segurança e comodidade, surgindo, então, o novo protocolo de internet, o IPV6 com o IPsec nativo. Como o IPsec implementa serviços de autenticação e criptografia na camada de rede, isso faz com que a segurança dependa o mínimo possível do usuário.

### **1.1 Objetivo**

O objetivo desse trabalho é provar que o IPV6 é de fato um protocolo mais seguro que o IPV4 e que a migração do IPV4 para o IPV6 é uma opção viável. Provarei isso de forma que será necessária conduzir pesquisas e testes com transferências de arquivos entre três máquinas. Um servidor registrador de packets de rede utilizando o Wireshark versão 2.4.2, um servidor FTP que terá uma conexão com o cliente, disponibilizando arquivos para o cliente realizar o download utilizando o FileZilla Server versão 0.9.60 beta e uma máquina para servir de cliente para transferir e baixar arquivos do servidor FTP utilizando o FileZilla Client versão 3.28.0.

O Wireshark vai interceptar e analisar os pacotes de ambos os protocolos enquanto a comunicação FTP de transferência de arquivos entre o servidor e o cliente esteja ocorrendo e vai registrar cada um deles em seu central de monitoramento. O intuito é comparar a quantidade de pacotes que foram colhidos com o IPV4 e o IPV6 e verificar sua legibilidade em termos de informações sensíveis, para testar a segurança do IPV4 que não possui o IPsec e o IPV6 que possui o suporte para o IPsec nativamente.

### **1.2 Metodologia**

Para que esse trabalho de conclusão de curso fosse possível, é necessário muitos testes com três máquinas e alguns softwares. A primeira etapa consiste em realizar os testes. Para isso, é necessário que os computadores sejam montados e devidamente preparados. O servidor registrador será feito em um notebook com Windows 7 Ultimate de 64 bits utilizando o software Wireshark versão 2.4.2, utilizando também uma placa de rede externa USB da marca TP-Link do modelo TL-WN722N de 150mbps operando em modo promíscuo para que fosse possível a captura de packets não destinados ao próprio computador. A máquina com servidor FTP também é outro notebook com Windows 10 Pro de

64 bits. O FTP será feito com um software chamado FileZilla Server versão 0.9.60 beta. O computador que estará baixando os arquivos do servidor fazendo com que as transferências de arquivos fossem possíveis é um notebook com Windows 8 Single Language de 64 bits com o FileZilla Client versão 3.28.0. Os arquivos que serão enviados serão arquivos de vídeo VLC (.mkv) e .mp4. O roteador que eu utilizei foi o D-Link DIR- 610 de 150mbps Single Band com capacidades e suporte para os protocolos IPV4 e IPV6.

Uma vez que os computadores e equipamentos de rede estiverem prontos, será possível conduzir os testes.

## **2. IPSEC**

O Internet Protocol Security – Protocolo de Segurança IP (IPsec) descrito na RFCs 2401/1998, 2402/1998 [IETF, 2017], entre outras, é uma alternativa de segurança a nível de camada de rede, criada para proteger o tráfego das informações na internet e bastante disseminada no mercado. O IPsec foi inicialmente projetado e criado para ser usado diretamente no IPV4 para que a segurança fosse implementada no protocolo com a intenção de fornecer essa mesma segurança para a transmissão de informações sensíveis e confidenciais pelas redes não protegidas. Por esse motivo, isso passou a ser um item obrigatório no IPV6 [RFC 2460, 2017].

Quando se trata de IPV6, como ele tem o suporte para IPsec nativamente, o ponto mais crítico e essencial quando se trata de segurança, é justamente a implementação do IPsec. O IPsec age na camada de rede fornecendo proteção e autenticação de pacotes IP entre dispositivos IPsec e garantindo confidencialidade, integridade e autenticidade de comunicação de dados em uma rede IP pública [WENSTROM, 2002]. Quando uma mensagem é transmitida utilizando uma rede pública como a Internet, a mensagem e seus dados trafegam por diversos equipamentos antes de chegar até o destino. Durante o trânsito até o destino, a mensagem está sujeita a ser interceptada e lida ou até mesmo alterada por uma terceira pessoa que não é para ter acesso a essa mensagem e seus dados. Não existe garantia que a mensagem recebida pelo destino seja a mesma enviada. [FALSARELLA, 2008]. Para que seja possível uma comunicação segura, é imprescindível a garantia de que a origem e o destino

dos pacotes sejam autênticos e verdadeiros, e também o sigilo e confidencialidade de suas informações internas.

Por exemplo, é totalmente necessário para alcançar esse objetivo, o sigilo, garantindo que ninguém lerá sua mensagem. Podemos contar também com a inteireza, ou integridade, que significa que sua mensagem não poderá ser alterada de nenhuma forma ou aspecto. Por último, contamos com a legitimidade, ou, a autenticidade, que garante que ninguém enviará mensagens falsas e enganosas. Algumas áreas que terão benefícios com a implementação do IPsec, são, por exemplo, a proteção de ataques tipo IP Spoofing, tráfego de e-mail e afins.

Figura 01 – Integração de três protocolos principais do IPsec.



Estrutura do Pacote IPsec

Fonte: FAQInformática, (2017)

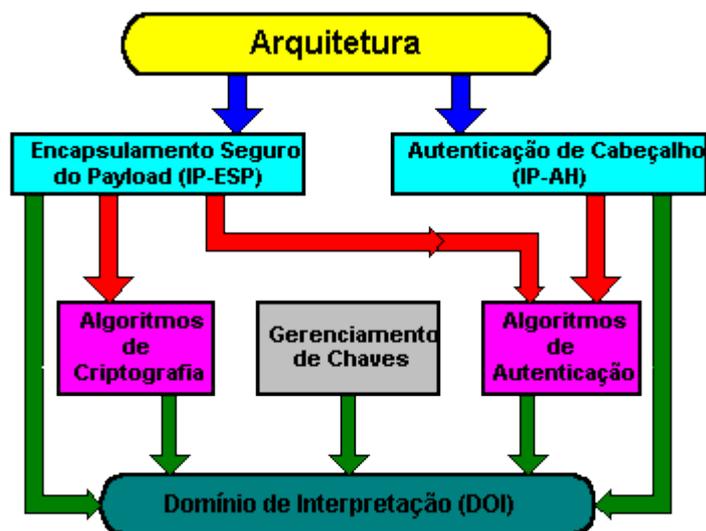
## 2.1 Arquitetura IPsec

Contudo, é necessário alguns protocolos dentro do IPsec para que isso seja possível. São três protocolos principais que são necessários para que isso ocorra: O primeiro é o Authentication Header (AH ou cabeçalho de autenticação). Com o cabeçalho de autenticação, é possível a segurança e veracidade de sua mensagem, afim de evitar qualquer reprodução que não seja legítima. Para garantir a autenticação da origem dos dados, o AH inclui uma chave compartilhada secreta no algoritmo que utiliza para a autenticação. Para garantir a proteção de repetição, o AH utiliza um campo de número de sequência dentro do cabeçalho do AH [IBM, 2014].

O próximo protocolo é o Encapsulating Security Payload (ESP ou Encapsulamento Seguro do Payload), que seria o protocolo que dará a criptografia para o arquivo durante a transferência FTP. Esse protocolo faz com

que os serviços de autenticação de pacotes sejam inclusos, ou seja, faz com que a integridade seja garantida através da criptografia, fazendo com que seja possível garantir que os dados serão vistos somente pelo destinatário correto e que não haverá nenhum tipo de alteração durante a transmissão do mesmo. Esses dois protocolos (AH e ESP) podem ser utilizados de forma independente ou em conjunto. Além do AH e o ESP, ainda existe o protocolo Internet Key Exchange (IKE). Esse protocolo é útil para realizar a gerência automática de chaves criptográficas, fazendo com que as mesmas sejam disponíveis em segurança. Isso é possível porque o IKE estabelece ligações AH ou ESP.

Figura 02 – Roadmap para documentos IPsec.



Fonte: Renata Cicilini Teixeira, (1999).

## 2.2 Cabeçalho ESP

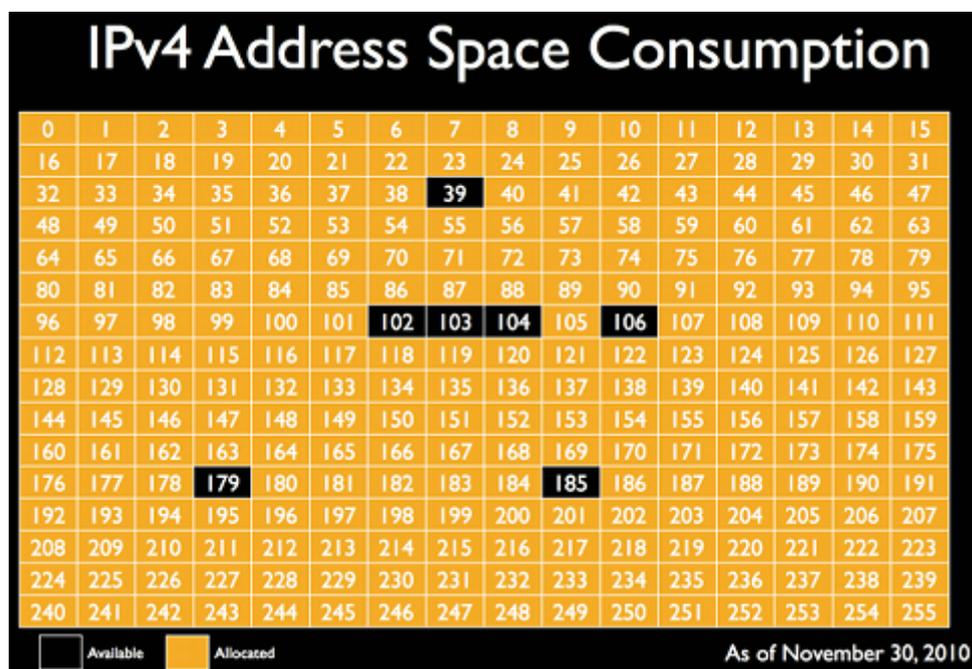
O cabeçalho ESP ou Encapsulating Security Payload como dito anteriormente, será o protocolo que dará a criptografia pelo IPsec para o arquivo selecionado para a transferência FTP. O cabeçalho ESP é um cabeçalho que traz a garantia de autenticação, integridade e confidencialidade nos packets de dados e também evita que esses mesmos packets sejam enviados novamente por alguma outra pessoa que não tenha a devida permissão para isso, comprometendo a autenticação, confidencialidade e integridade dos pacotes. O ESP faz essa criptografia de modo que seja impossível a legibilidade das

informações contidas dentro do arquivo caso ele venha a ser interceptado. Isso faz com que os dados em si sejam criptografados de forma que seja possível garantir que os dados desses packets trafegados pela Internet não sejam alterados. Além disso, o ESP utiliza o a criação e gerenciamento de chaves de segurança pelo protocolo Internet Key Protocol, ou IKE [BRAGA, 2011].

### 3. IPv4 e suas limitações

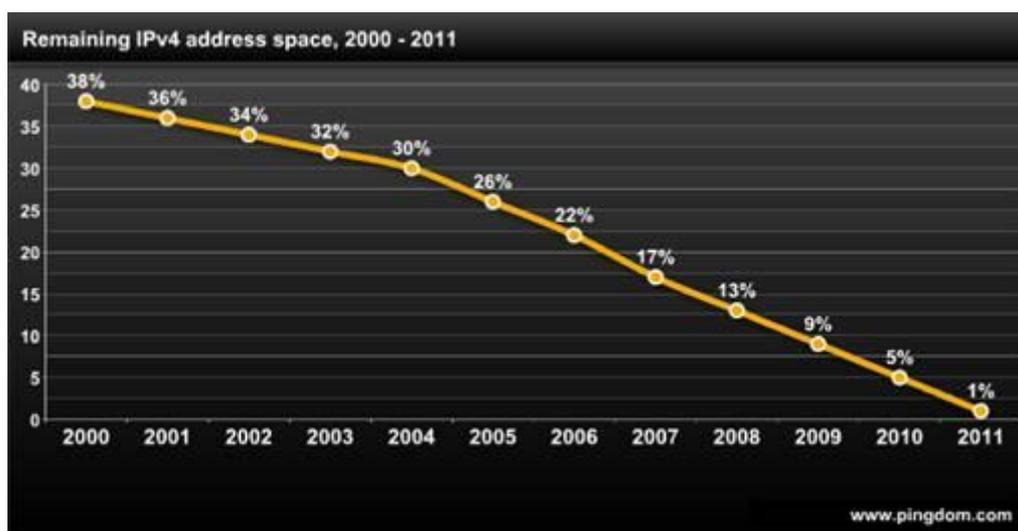
O IPv4 hoje tem muitas limitações, por esse motivo, foi substituído pelo IPv6. Vemos tais limitações como a escassez de endereços IPv4 atualmente. Durante quase 30 anos, o IPv4 tinha a necessidade de fornecer para todos os computadores nele conectado uma chave identificadora que fosse único pela internet toda. No caso, o IP (Protocolo de Internet). Fazendo assim, somente assim, era possível ter uma conectividade sem nenhum tipo de imprevisto ou falha. Mas logicamente isso não podia durar para sempre por conta dos números finitos num IP, logo, os IP's acabariam, tornando-se inútil os 32 bits utilizados para essa finalidade.

Figura 03 – Esgotamento do IPv4 em 30 de Novembro de 2010.



Fonte: Carlos Morimoto, (2011).

Figura 04 - Gráfico do esgotamento dos endereços IPv4, entre 2000–2011



Fonte: [www.pingdom.com](http://www.pingdom.com), (2013)

Outro problema muito sério que o IPv4 enfrenta é a ausência de qualidade de serviço. Segundo Canno (2013) a Qualidade de Serviço de uma rede é garantida pelos componentes da rede e equipamentos utilizados, estando baseada em um mecanismo com a intenção de garantir a entrega dos dados e que deve atuar na comunicação e interação dos equipamentos envolvidos. O IPv4 não trabalha nativamente com algum tipo de serviço que ofereça e garanta uma qualidade de transmissão. Na criação do IPv4, não era comum a preocupação com esse tipo de qualidade quando se trata de aplicações multimídia como temos hoje, por exemplo.

A convergência das redes de telecomunicações futuras para a camada de rede comum, o IPv6, favorecerá o amadurecimento de serviços hoje imprudentes, como streaming de vídeo em tempo real e fará aparecerem outros novos. Entre outras razões, é evidente que algum novo protocolo teria que implementar algumas funções que o protocolo passado falhou ou simplesmente não estiveram presentes pra início.

#### 4. IPv4 vs IPv6

Agora veremos e falaremos sobre alguns detalhes essenciais quanto a comparação do IPv4 ao IPv6. Resumindo, o IPv6 é diferente por conta de sua capacidade em endereços quase que ilimitados,

aumento da movimentação e fluxo de dados, melhor desempenho e superiores características de segurança [CANNO, 2013].

#### **4.1 Segurança**

Quando se trata de segurança, ficou evidente que por conta do IPsec, o protocolo IPV6 é mais seguro que o IPV4. Nos dias de hoje, temos mais de três décadas de uso de IPV4 no Brasil, sendo que também temos quase 19 anos de IPV6. Os objetivos primordiais quando se trata de segurança em IPV6 são iguais aos objetivos de segurança em qualquer servidor, ambiente ou infraestrutura de redes. Estes incluem: rigidez da base ou infraestrutura; comprovações legítimas, confiança e legitimação; o total oposto de rejeição e contabilização [CANNO, 2013].

Existem dicas recomendadas de segurança avançada para o uso do IPV6, como:

- Não utilizar endereços óbvios;
- Utilizar IPsec sempre que precisar de uma comunicação segura entre máquinas IPV6;
- No IPV4 bloquear as faixas não alocadas;

#### **4.2 Qualidade de Serviços**

Mais uma vez falaremos de qualidade de serviços. No lugar de quatro octetos representados em decimal, o protocolo IPV6 utiliza oito hexatetos representados em hexadecimal. A integração de Qualidade de Serviços no IPV4 é baseada nas portas TCP e UDP do pacote ou pacotes, fazendo com que seja possível fazer com que seu uso não consiga ser funcional em algumas situações. Com o uso de autoconfiguração, isso faz com que o IPV6 tenha a opção de atribuir endereços IP automaticamente a um host. Da mesma forma que o IPV4, o IPV6 é um protocolo responsável pelo endereçamento de hosts e roteamento de pacotes entre redes que são baseadas em TCP/IP. O IPV6 é um protocolo bem mais simples que o IPV4 [Renato Montes Canno, 2013]. Resumindo, o IPV6 fez com que fosse possível manter a maioria das características principais do IPV4, fazendo com que ele fosse um grande padrão mundial a ser seguido, com algumas pequenas alterações e acréscimos.

### 4.3 Principais diferenças entre os protocolos IPV4 e IPV6

Falamos das vantagens do protocolo IPV6 sobre o IPV4. Abaixo, tem uma imagem que comprova resumidamente as principais diferenças entre os dois protocolos:

Figura 05 – Diferenças notáveis entre o IPV4 e IPV6

IPV4	IPV6
Endereço de 32bits	Endereço de 128bits
Suporte opcional de IPSec	Suporte obrigatório de IPSec
Nenhuma referência a capacidade de QoS ( <i>Quality of Service</i> )	Introduz capacidades de QoS utilizando para isso o campo Flow Label
Processo de fragmentação realizada pelo router	A fragmentação deixa de ser realizada pelos routers e passa a ser processada pelos <i>host</i> emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo <i>extension header</i>
O <i>Address Resolution Protocol</i> (ARP), utiliza requisitos do tipo <i>Broadcast</i>	O ARP foi abandonado, sendo substituídos pelas mensagens <i>Neighbor Discovery</i>
<i>Internet Resolution Management Protocol</i> (IGMP) é utilizado para gerir relações locais de sub-redes	O IGMP foi substituído por mensagens <i>Multicast Listener Discovery</i>
Os Endereços de <i>Broadcast</i> são utilizados para enviar tráfego para todos os <i>host</i> de uma rede	Deixa de existir o endereço de <i>Broadcast</i> , para utilizar endereços <i>multicast</i>
O endereço tem de ser configurado manualmente	Adição de funcionalidades de autoconfiguração
Suporta pacotes de 576 bytes, passíveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

Fonte: <http://www.techsutram.com>, (2009)

Atualmente, os endereços IPV4 estão acabando. Como dito anteriormente, um endereço IPV4 é formado por 32 bits, ou 32 zeros e uns. Por conta do IPV4 ser composto por 32 bits, isso significa que o IPV4 permite 4.294.967.296 endereços diferentes. Hoje em dia, isso não parece um número muito grande, visto que muitas pessoas no mundo possuem acesso à internet e possuem mais de um dispositivo conectado na rede, entre eles, smartphones, tablets e

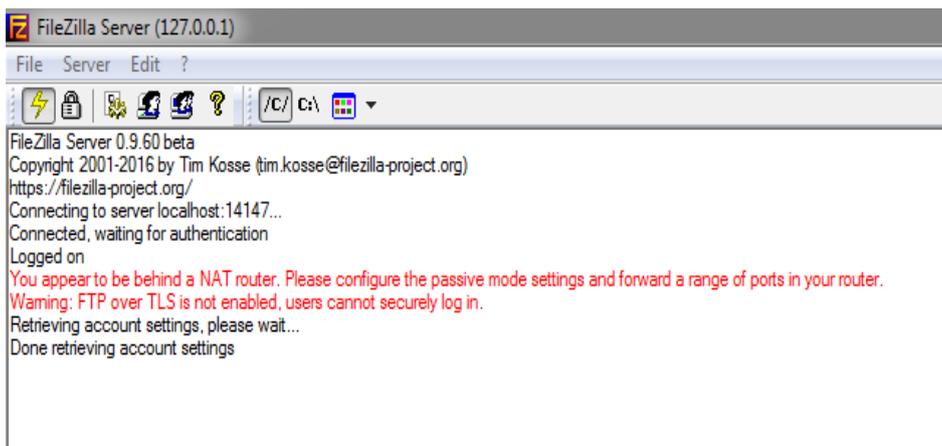
notebooks. Isso prova a escassez dos endereços IPV4. A quantidade de usuários acessando a internet não é a única razão pela qual os endereços IP estão ficando escassos. A quantidade de modems e servidores que utilizam endereços públicos o tempo todo, onde esses mesmos endereços não podem ser compartilhados, visto que eles são exclusivos aos dispositivos que neles estão conectados.

Segundo o Adriano Oliveira (2017) visto o IPV6 possui 128 bits, visto que o IPV4 possui somente 32, estima-se que até o ano de 2020 haverá mais de 50 bilhões de dispositivos online. É notável que o IPV6 ainda não foi totalmente implementado, atualmente. Porém, muitas empresas como Facebook, Google, Terra, UOL e Yahoo! já estão utilizando o IPV6. O Google oferece DNS público com IPV6 para que seja possível sua utilização. Mesmo que o IPV4 ainda seja a versão do Internet Protocol mais utilizada, o IPV6 além de ser mais seguro em diversos aspectos, vai permitir com seus 128 bits cada vez mais acessos à Internet.

## **5. Desenvolvimento**

O desenvolvimento do projeto consiste em transferir arquivos do computador de transferência, que será nomeado Transferência para o computador com o servidor FTP, que será nomeado de FTP enquanto o computador que terá o Wireshark ficará analisando a quantidade de pacotes em IPV4 e IPV6, que será nomeado "Wireshark". De imediato, é necessário configurar o servidor FTP. Para isso, estou utilizando o software FileZilla Server.

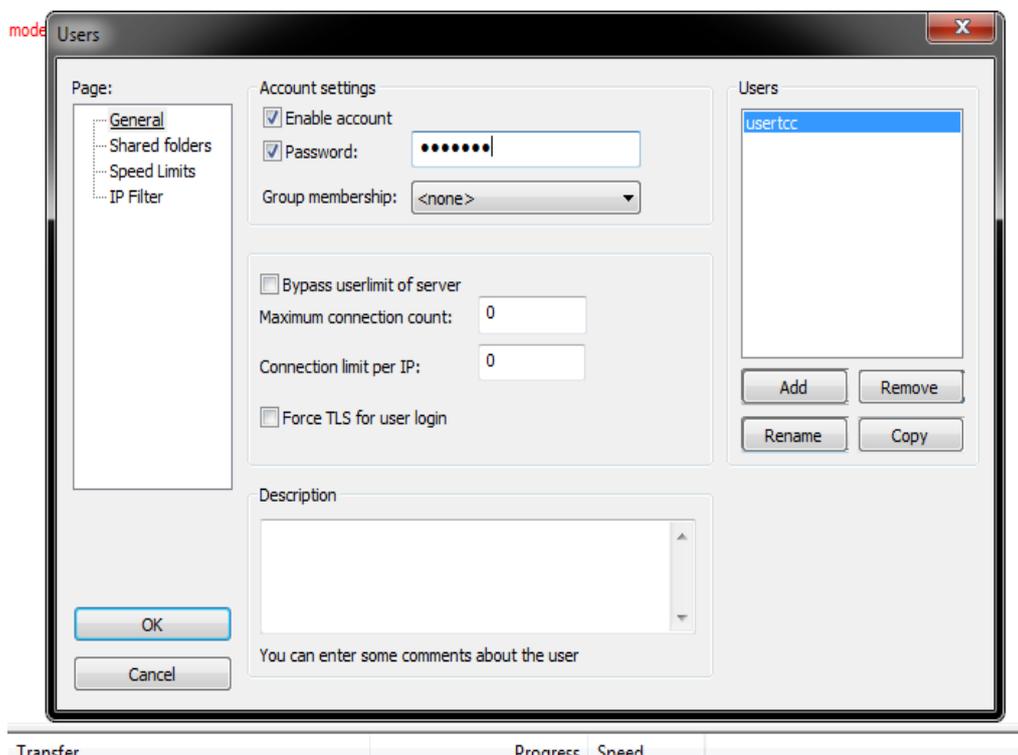
Figura 06 – Painel principal do FileZilla Server no computador “Servidor”



Fonte: O Autor, (2017)

De imediato, após configurar o servidor para localhost 14147, é essa a tela que temos. O próximo passo seria criar um usuário com senha para que o mesmo tenha as devidas permissões para acessar o servidor e ter acesso aos arquivos que estão armazenados o servidor.

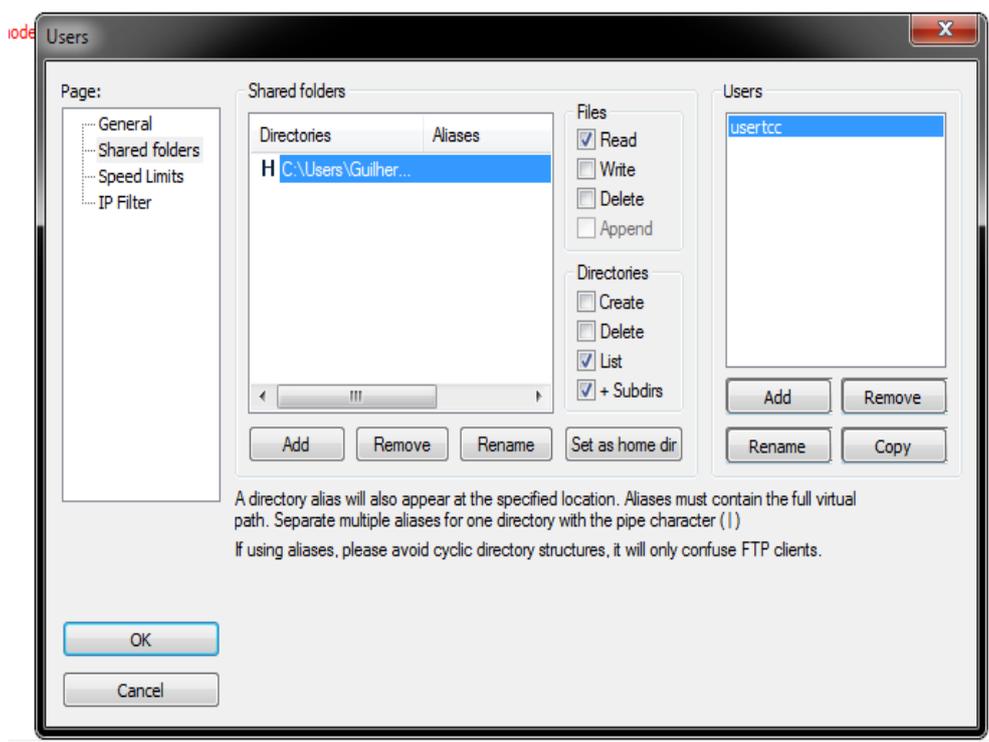
Figura 07 – Tela de criação de usuário do FileZilla Server no computador “Servidor”



Fonte: O Autor, (2017)

Após a criação, podemos verificar que temos todos os privilégios administrativos sobre esse novo usuário que foi criado. Feito isso, o próximo passo é colocar pastas de arquivos no servidor para que o cliente possa estar acessando.

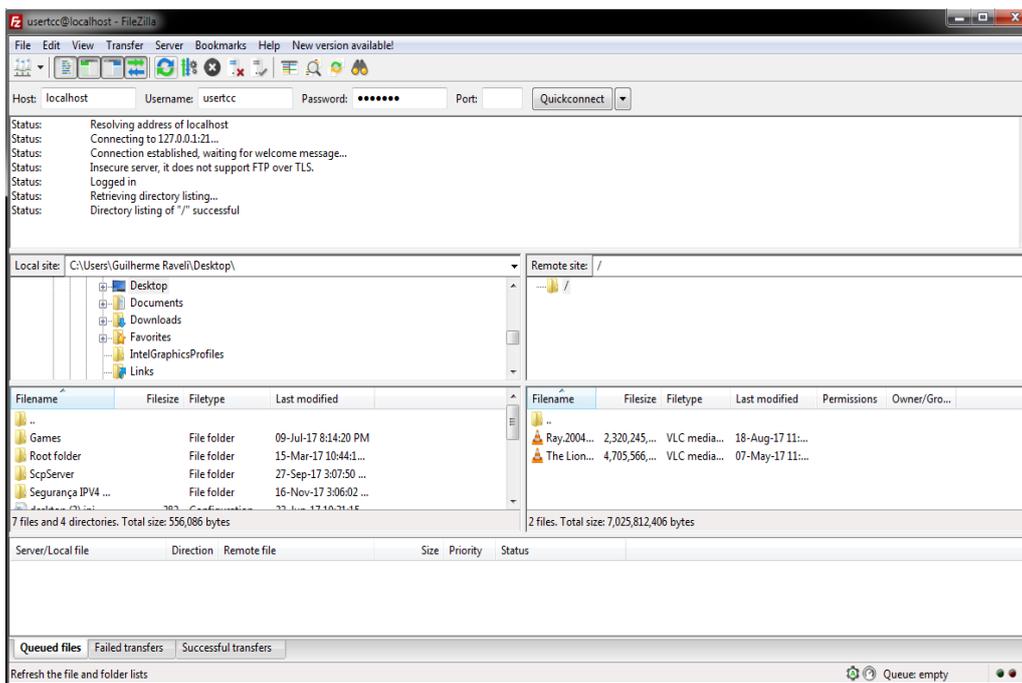
Figura 08 – Pastas compartilhadas com o usuário do FileZilla Server para o FileZilla Client no computador “Servidor”



Fonte: O Autor, (2017)

Nessa nova tela, podemos verificar o diretório da pasta que eu criei com alguns arquivos que o cliente tentará acessar. O diretório dessa pasta é “C:\Users\Guilherme Raveli\Desktop\Segurança IPV4 vs IPV6\Pasta FTP” e essa pasta possui dois arquivos, um com a extensão .mp4 e outro com a extensão .mkv. O arquivo .mp4 tem 2.16GB de tamanho e o arquivo .mkv tem 4.38GB de tamanho. Eu selecionei esses arquivos com um tamanho razoável para que seja bastante perceptível a contagem dos packets durante as varreduras. O próximo passo é colocar todas essas informações do servidor no FileZilla Client.

Figura 09 – Painel principal do FileZilla Client no computador “Cliente”



Fonte: O Autor, (2017)

Nessa tela do FileZilla Client, podemos verificar o acesso ao servidor com a pasta que demos permissão ao cliente, e também podemos verificar a movimentação do cliente no servidor no painel do FileZilla Server com a imagem abaixo:

Figura 10 - Mudança na tela do FileZilla Server após a conexão do usuário no servidor no computador "Servidor"

```

FileZilla Server (127.0.0.1)
File Server Edit ?
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> Connected on port 21, sending welcome message...
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 220-FileZilla Server 0.9.60 beta
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 220 Please visit https://filezilla-project.org/
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> AUTH TLS
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 502 Explicit TLS authentication not allowed
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> AUTH SSL
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 502 Explicit TLS authentication not allowed
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> USER usertcc
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> 331 Password required for usertcc
(000001)16-Nov-17 15:28:42 PM - (not logged in) (127.0.0.1)> PASS *****
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 230 Logged on
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> SYST
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 215 UNIX emulated by FileZilla
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> FEAT
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 211-Features:
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> MDTM
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> REST STREAM
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> SIZE
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> MLST type*;size*;modify*;
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> MLSD
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> UTF8
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> CLNT
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> MFMT
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> EPSV
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> EPRT
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 211 End
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> PWD
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 257 "/" is current directory.
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> TYPE I
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 200 Type set to I
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> PASV
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 227 Entering Passive Mode (127.0.0.1,209,98)
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> MLSD
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 150 Opening data channel for directory listing of "/"
(000001)16-Nov-17 15:28:42 PM - usertcc (127.0.0.1)> 226 Successfully transferred "/"
(000001)16-Nov-17 15:30:43 PM - usertcc (127.0.0.1)> 421 Connection timed out.
(000001)16-Nov-17 15:30:43 PM - usertcc (127.0.0.1)> disconnected.

```

Fonte: O Autor, (2017)

Agora que os dois computadores (FileZilla Server e FileZilla Client) estão interligados, é necessário colocar o terceiro computador para monitorar a rede, no caso, esse, o Wireshark. O Wireshark vai usar sua ferramenta nativa para capturar todo o tráfego de dados quando a transferência de arquivos começar. Abaixo, mostrarei o Wireshark com sua ferramenta de captura de packets funcionando:

Figura 11 – Wireshark capturando packets da rede sem fio “Rede maliciosa” no computador “Wireshark”

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	104.154.126.25	192.168.2.108	TCP	282	4070 → 50489 [PSH, ACK] Seq=1 Ack=1 Win=120 Len=228
2	0.001449	192.168.2.108	104.154.126.25	TCP	183	50489 → 4070 [PSH, ACK] Seq=1 Ack=229 Win=65184 Len=129
3	0.208986	104.154.126.25	192.168.2.108	TCP	759	4070 → 50489 [PSH, ACK] Seq=229 Ack=130 Win=120 Len=705
4	0.409491	192.168.2.108	104.154.126.25	TCP	54	50489 → 4070 [ACK] Seq=130 Ack=934 Win=65410 Len=0
5	2.628694	c8:22:02:03:10:b1	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.103
6	3.553953	104.154.126.25	192.168.2.108	TCP	68	4070 → 50489 [PSH, ACK] Seq=934 Ack=130 Win=120 Len=11
7	3.652693	c8:22:02:03:10:b1	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.103
8	3.753598	192.168.2.108	104.154.126.25	TCP	54	50489 → 4070 [ACK] Seq=130 Ack=945 Win=65407 Len=0
9	4.062242	c8:22:02:03:10:b1	Broadcast	ARP	60	Gratuitous ARP for 192.168.2.103 (Request)
10	4.419987	192.168.2.107	192.168.2.108	TCP	224	55125 → 49165 [PSH, ACK] Seq=1 Ack=1 Win=4096 Len=170
11	4.420175	192.168.2.108	192.168.2.107	TCP	352	49165 → 55125 [PSH, ACK] Seq=1 Ack=171 Win=255 Len=298
12	4.437883	192.168.2.107	192.168.2.108	TCP	56	55125 → 49165 [ACK] Seq=171 Ack=299 Win=4091 Len=0
13	4.574267	c8:22:02:03:10:b1	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.103
14	5.267799	192.168.2.1	239.255.255.250	SSDP	306	NOTIFY * HTTP/1.1
15	5.370020	192.168.2.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
16	5.474895	192.168.2.1	239.255.255.250	SSDP	378	NOTIFY * HTTP/1.1
17	5.578600	192.168.2.1	239.255.255.250	SSDP	378	NOTIFY * HTTP/1.1

▶ Frame 15: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0  
 ▶ Ethernet II, Src: Tp-LinkT\_df:79:a4 (c4:6e:1f:df:79:a4), Dst: ChiconyE\_60:02:d6 (64:5a:04:60:02:d6)  
 ▶ Internet Protocol Version 4, Src: 192.168.2.1, Dst: 239.255.255.250  
 ▶ User Datagram Protocol, Src Port: 56843, Dst Port: 1900  
 ▶ Simple Service Discovery Protocol

```

0000  64 5a 04 60 02 d6 c4 6e 1f df 79 a4 08 00 45 00  dZ.'...n ..y...E.
0010  01 2d 00 00 40 00 04 11 c3 1c c0 a8 02 01 ef ff  -.@... ..
0020  ff fa de 0b 07 6c 01 19 ad f4 4e 4f 54 49 46 59  ....1.. .NOTIFY
0030  20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53  * HTTP/1.1..HOS
0040  54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32  T: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43  50:1900. .CACHE-C
0060  4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d  ONTROL: max-age=
0070  31 30 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68  100..LOC ATION: h
0080  74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 32 2e  ttp://19 2.168.2.
0090  31 3a 31 39 30 30 2f 69 67 64 2e 78 6d 6c 0d 0a  1:1900/i gd.xml..
00a0  4e 54 3a 20 75 75 69 64 3a 30 36 30 62 37 33 35  NT: uuid :060b735
00b0  33 2d 66 63 61 36 2d 34 30 37 30 2d 38 35 66 34  3-fca6-4 070-85f4
00c0  2d 31 66 62 66 62 39 61 64 64 36 32 63 0d 0a 4e  -1fbfb9a dd62c..N
  
```

Fonte: O Autor, (2017)

Aqui podemos verificar uma varredura de pacotes da minha atual rede sem fio “Rede maliciosa” sem filtros de busca de pacotes. Agora irei iniciar a pesquisa dos pacotes da transferência da arquivos do protocolo IPV4. O servidor está no IP 192.168.2.108. Abaixo, mostrarei os comandos necessários para iniciar a transferência de arquivos:

Figura 12 – Comandos no Prompt de Comando com privilégios de administrador para inicializar o processo de transferência de arquivos FTP no computador “Cliente”

```

Administrator: C:\Windows\System32\cmd.exe - ftp 192.168.2.108
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ftp 192.168.2.108
Connected to 192.168.2.108.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
User (192.168.2.108:(none)): usertcc
331 Password required for usertcc
Password:
230 Logged on
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
-rw-r--r-- 1 ftp ftp      2320245693 Aug 18  2017 Ray.2004.mp4
-rw-r--r-- 1 ftp ftp      4705566713 May 08  2017 The Lion King.1994.mkv
226 Successfully transferred "/"
ftp: 136 bytes received in 0.00Seconds 136000.00Kbytes/sec.
ftp> get Ray.2004.mp4
200 Port command successful
150 Opening data channel for file download from server of "/Ray.2004.mp4"
  
```

Fonte: O Autor, (2017)

Figura 13 - Captura do arquivo "Ray.2004.mp4" em IPV4 no computador “Wireshark”

No.	Time	Source	Destination	Protocol	Length	Info
57	25.398086	192.168.0.105	192.168.0.108	FTP	197	Response: 220-FileZilla Server 0.9.60 beta
73	30.547277	192.168.0.108	192.168.0.105	FTP	68	Request: USER usuario
74	30.925346	192.168.0.105	192.168.0.108	FTP	89	Response: 331 Password required for usuario
111	36.105761	192.168.0.108	192.168.0.105	FTP	61	Request: PASS
121	37.069544	192.168.0.105	192.168.0.108	FTP	69	Response: 230 Logged on
127	39.655113	192.168.0.108	192.168.0.105	FTP	81	Request: PORT 192,168,0,108,196,77
128	40.141977	192.168.0.105	192.168.0.108	FTP	83	Response: 200 Port command successful
129	40.144685	192.168.0.108	192.168.0.105	FTP	60	Request: LIST
132	40.148106	192.168.0.105	192.168.0.108	FTP	109	Response: 150 Opening data channel for directory listing of "/"
137	40.150108	192.168.0.105	192.168.0.108	FTP	88	Response: 226 Successfully transferred "/"
169	66.110477	192.168.0.108	192.168.0.105	FTP	81	Request: PORT 192,168,0,108,196,78
170	66.764621	192.168.0.105	192.168.0.108	FTP	83	Response: 200 Port command successful
171	66.767906	192.168.0.108	192.168.0.105	FTP	73	Request: RETR Ray.2004.mp4
174	66.770708	192.168.0.105	192.168.0.108	FTP	129	Response: 150 Opening data channel for file download from server of "/Ray.2004.mp4"
1847	1404.053867	192.168.0.105	192.168.0.108	FTP	100	Response: 226 Successfully transferred "/Ray.2004.mp4"

Frame 1847890: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0  
 Ethernet II, Src: PaLladiu\_23:8a:95 (Sc:c9:d3:23:8a:95), Dst: ChiconyE\_60:02:d6 (64:5a:04:60:02:d6)  
 Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.108  
 Transmission Control Protocol, Src Port: 21, Dst Port: 50252, Seq: 416, Ack: 101, Len: 46  
 File Transfer Protocol (FTP)

```

0000  64 5a 04 60 02 d6 5c c9 d3 23 8a 95 08 00 45 00  dZ...E.
0010  00 56 5f fe 40 00 80 06 18 7e c0 a8 00 69 c0 a8  .V_...i..
0020  00 6c 00 15 c4 4c 6e d7 bf d9 fe 18 c5 12 50 18  .l..ln.....P.
0030  fa 8c 71 22 00 00 32 32 36 20 53 75 63 63 65 73  ..q..22 6 Succes
0040  73 66 75 6c 6c 79 20 74 72 61 6e 73 66 65 72 72  fully t transferr
0050  65 64 20 22 2f 52 61 79 2e 32 30 30 34 2e 6d 70  ed "/Ray .2004.mp
0060  34 22 0d 0a 4".
  
```

Fonte: O Autor, (2017)

Nesse teste, podemos verificar que após a aplicação do filtro “FTP” no Wireshark, foram descobertos e captados 15 packets em IPV4 totalmente sem criptografia. Isso faz com que seja fácil ver o que está sendo interceptado, junto com o IP de origem e destino. Do primeiro packet até o último, podemos verificar os estágios do envio FTP, de início ao fim. E também é fácil verificar a mesma informação no FileZilla Server com seu monitoramento abaixo:

Figura 14 – Captura de IP origem e destino e notificação da transferência de arquivo FTP “Ray.2004.mp4” no computador “Servidor”

```
(000002)16-Nov-17 15:47:43 PM - (not logged in) (192.168.2.108)> PASS ****
(000002)16-Nov-17 15:47:43 PM - usertcc (192.168.2.108)> 230 Logged on
(000002)16-Nov-17 15:47:58 PM - usertcc (192.168.2.108)> PORT 192,168,2,108,197,246
(000002)16-Nov-17 15:47:58 PM - usertcc (192.168.2.108)> 200 Port command successful
(000002)16-Nov-17 15:47:58 PM - usertcc (192.168.2.108)> LIST
(000002)16-Nov-17 15:47:58 PM - usertcc (192.168.2.108)> 150 Opening data channel for directory listing of "/"
(000002)16-Nov-17 15:47:58 PM - usertcc (192.168.2.108)> 226 Successfully transferred "/"
(000002)16-Nov-17 15:48:23 PM - usertcc (192.168.2.108)> PORT 192,168,2,108,198,15
(000002)16-Nov-17 15:48:23 PM - usertcc (192.168.2.108)> 200 Port command successful
(000002)16-Nov-17 15:48:23 PM - usertcc (192.168.2.108)> RETR Ray.2004.mp4
(000002)16-Nov-17 15:48:23 PM - usertcc (192.168.2.108)> 150 Opening data channel for file download from server of "/Ray.2004.mp4"
(000002)16-Nov-17 15:49:16 PM - usertcc (192.168.2.108)> 226 Successfully transferred "/Ray.2004.mp4"
(000002)16-Nov-17 15:51:16 PM - usertcc (192.168.2.108)> 421 Connection timed out.
(000002)16-Nov-17 15:51:16 PM - usertcc (192.168.2.108)> disconnected.
```

Fonte: O Autor, (2017)

Aqui no monitoramento do servidor, fica fácil ver toda a movimentação do que aconteceu com a conexão entre o cliente e o servidor. Aqui não demonstra que o Wireshark estava capturando as informações.

Figura 15 – Captura IPV6 com IPsec ativado no computador “Servidor”

The screenshot displays the Wireshark interface with a filter set to 'esp'. The packet list pane shows a series of ESP packets. The packet details pane for packet 49 shows the Ethernet II header, Internet Protocol Version 6 header, and Encapsulating Security Payload (ESP) header with SPI 0x00000100 and sequence 9.

No.	Time	Source	Destination	Protocol	Length	Info
23	12:28:52.746345	fe80::222:22ff:fe22:2222	ff02::5	ESP	122	ESP (SPI=0x00000100)
32	12:28:54.756345	fe80::211:11ff:fe11:1111	ff02::5	ESP	122	ESP (SPI=0x00000100)
35	12:28:54.816345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	130	ESP (SPI=0x00000100)
36	12:28:54.851345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	114	ESP (SPI=0x00000100)
37	12:28:54.856345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	130	ESP (SPI=0x00000100)
39	12:28:54.901345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	114	ESP (SPI=0x00000100)
40	12:28:54.936345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	138	ESP (SPI=0x00000100)
41	12:28:54.981345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	178	ESP (SPI=0x00000100)
42	12:28:54.991345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	114	ESP (SPI=0x00000100)
43	12:28:55.021345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	114	ESP (SPI=0x00000100)
44	12:28:55.026345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	138	ESP (SPI=0x00000100)
45	12:28:55.026345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	114	ESP (SPI=0x00000100)
46	12:28:55.031345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	114	ESP (SPI=0x00000100)
47	12:28:55.031345	fe80::222:22ff:fe22:2222	fe80::211:11ff:fe11:1111	ESP	234	ESP (SPI=0x00000100)
48	12:28:55.091345	fe80::211:11ff:fe11:1111	fe80::222:22ff:fe22:2222	ESP	130	ESP (SPI=0x00000100)
49	12:28:55.221345	fe80::211:11ff:fe11:1111	ff02::5	ESP	194	ESP (SPI=0x00000100)
51	12:28:55.411345	fe80::222:22ff:fe22:2222	ff02::5	ESP	146	ESP (SPI=0x00000100)
54	12:28:55.861345	fe80::222:22ff:fe22:2222	ff02::5	ESP	218	ESP (SPI=0x00000100)
58	12:28:57.551345	fe80::211:11ff:fe11:1111	ff02::5	ESP	242	ESP (SPI=0x00000100)
59	12:28:57.596345	fe80::222:22ff:fe22:2222	ff02::5	ESP	162	ESP (SPI=0x00000100)
62	12:29:01.156345	fe80::211:11ff:fe11:1111	ff02::5	ESP	162	ESP (SPI=0x00000100)
63	12:29:02.681345	fe80::222:22ff:fe22:2222	ff02::5	ESP	130	ESP (SPI=0x00000100)
64	12:29:03.251345	fe80::211:11ff:fe11:1111	ff02::5	ESP	146	ESP (SPI=0x00000100)
65	12:29:03.696345	fe80::222:22ff:fe22:2222	ff02::5	ESP	146	ESP (SPI=0x00000100)

Frame 49: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)

- Ethernet II, Src: Intel\_11:11:11 (00:11:11:11:11:11), Dst: IPv6mcast\_00:00:00:05 (33:33:00:00:00:05)
- Internet Protocol Version 6, Src: fe80::211:11ff:fe11:1111 (fe80::211:11ff:fe11:1111), Dst: ff02::5 (ff02::5)
  - 0110 .... = Version: 6
  - .... 1110 0000 .... = Traffic class: 0x000000e0
  - .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  - Payload length: 140
  - Next header: ESP (0x32)
  - Hop limit: 1
  - Source: fe80::211:11ff:fe11:1111 (fe80::211:11ff:fe11:1111)
  - [Source SA MAC: Intel\_11:11:11 (00:11:11:11:11:11)]
  - Destination: ff02::5 (ff02::5)
- Encapsulating Security Payload
  - ESP SPI: 0x00000100
  - ESP Sequence: 9

Fonte: O Autor, (2017)

Podemos perceber com o filtro ESP aplicado com o IPsec ativado na configuração IPV6, a sensibilidade das informações são fortemente aumentadas, fazendo com que não seja mais possível a leitura legível do que

está acontecendo, por conta da criptografia. Podemos notar também que nenhum packet FTP foi interceptado por conta do IPsec.

Figura 16 – Dados da Captura IPV6 com IPsec ativado no computador “Servidor”

```

Internet Protocol Version 6, Src: 3ffe::1, Dst: 3ffe::2
  0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 100
  Next Header: Encap Security Payload (50)
  Hop Limit: 64
  Source: 3ffe::1
  Destination: 3ffe::2
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]

```

Fonte: O Autor, (2017)

Aqui na Figura 16 podemos verificar os dados do ESP no IPV6 na captura de dados. Podemos ver nesses dados que não conseguimos detectar a origem e nem o destino da transferência de arquivo, e também na figura anterior, podemos verificar que também é impossível saber que tipo e nome do arquivo que está sendo transferido.

Figura 17 – Dados da Captura IPV6 com IPsec ativado no computador “Servidor”  
(Destino e Origem)

```

Ethernet II, Src: Dell_4a:d7:0a (00:11:43:4a:d7:0a), Dst: IPv6mcast_16 (33:33:00:00:00:16)
  ▸ Destination: IPv6mcast_16 (33:33:00:00:00:16)
  ▸ Source: Dell_4a:d7:0a (00:11:43:4a:d7:0a)
  Type: IPv6 (0x86dd)

```

Fonte: O Autor, (2017)

Na Figura 17 verificamos os computadores conectados na mesma rede como procedimento de esclarecimento, provando que sem medidas de segurança, é possível a detecção das máquinas onde a transferência está ocorrendo.

Figura 18 – Dados Detalhados da Captura IPV6 com IPsec ativado no computador  
“Servidor”

```

Destination: IPv6mcast_16 (33:33:00:00:00:16)
  Address: IPv6mcast_16 (33:33:00:00:00:16)
  .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
  .... ..1. .... = IG bit: Group address (multicast/broadcast)
Source: Dell_4a:d7:0a (00:11:43:4a:d7:0a)
  Address: Dell_4a:d7:0a (00:11:43:4a:d7:0a)
  .... ..0. .... = LG bit: Globally unique address (factory default)
  .... ..0. .... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)

```

Fonte: O Autor, (2017)

Aqui na Figura 18, podemos ver as informações mais detalhadas dentro do IPv6 sobre a transferência FTP, mas nenhuma informação comprometedoras do servidor ou do cliente é interceptado.

## CONCLUSÃO

O trabalho permitiu que as pesquisas realizadas me concedesse a informação de que o protocolo IPv6, como demonstrado nas pesquisas e nos testes, é bem mais seguro que o IPv4 por conta do IPsec nativo, pois graças ao IPsec nativo do IPv6, foi possível notar que a quantidade de packets capturados pelo Wireshark foi zerado, sem mais documentos, arquivos, dados sensíveis ou comandos durante toda a captura. Isso é devido ao IPsec com o ESP explicado anteriormente e sua função de criptografia de dados, inibindo a possibilidade de verificar o que está sendo baixado, o local de origem e o local de destino.

A utilização do IPsec em redes IPv6 protege muito bem os dados que nele são transmitidos. Uma outra vantagem disso também é a aniquilação de preparação e custos adicionais ao cliente para colocar uma segurança extra em sua rede e a responsabilidade de manutenção da mesma. Realizando esses testes com arquivos de vídeos, é um teste simples, mas serve para ilustrar que em outras condições, packets com o IPv4 podem estar sendo interceptados e traduzidos para revelar informações sensíveis como senhas de bancos, números de cartão de crédito, CPF e outros. Somente pela questão da segurança, é motivo o suficiente para concluir que a migração mundial do IPv4 para o IPv6 é a opção mais segura e viável.

Podemos afirmar isso por conta do suporte do IPsec nativo no IPv6, temos uma camada de segurança bem mais eficiente que o IPv4. A migração do IPv4 para o IPv6 como explicado anteriormente, é uma coisa inevitável. Os blocos restantes de IPv4 foram atualizados e otimizados para o controle de packets, assim gerando cada vez mais desempenho no uso da banda para o IPsec sobre o IPv6 [Almeida e Santa Inês, 2009]. O IPsec também inibe os três ataques mais comuns contra sua rede: ataques de replay, spoofing e tampering. Contudo, concluo que com base nos testes aqui apresentados, o IPv4 é facilmente substituível pelo IPv6 pela sua fragilidade, justamente por

seu não suporte do IPsec, uma ferramenta entre várias outras que são essenciais para uma navegação e experiência segura na internet, visto que hoje, tudo que fazemos em nossa vida é na internet. A migração é inevitável. A migração tem sido lenta por conta da dificuldade de migração e seu custo, mas estamos caminhando cada vez mais para a migração total de IPV4 para IPV6.

## REFERÊNCIAS BIBLIOGRÁFICAS

AUGUSTO, F. Entendendo o IPsec, 2011. Disponível em:<<https://fabiozibiani.wordpress.com/2011/01/09/entendendo-o-ipsec/>>.

Acessado em 29 de Setembro de 2017.

BRITO, S.H. B. IPv6 - O Novo Protocolo da Internet. São Paulo: Novatec Editora, 2013.

CANNO, R. Redes IP I: Comparativo entre IPv4 e IPv6, 2013. Disponível em:<[http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina\\_4.asp](http://www.teleco.com.br/tutoriais/tutorialredeip1/pagina_4.asp)>. Acessado em 27 de Setembro de 2017.

CANNO, R. Redes IPv6: Arquitetura Básica IPsec, 2013. Disponível em:<[http://www.teleco.com.br/tutoriais/tutorialipv6seg/pagina\\_5.asp](http://www.teleco.com.br/tutoriais/tutorialipv6seg/pagina_5.asp)>.

Acessado em 27 de Setembro de 2017.

DEVEL SISTEMAS – IPsec - Protocolo de redes IP. Disponível em: <<http://www.develsistemas.com.br/ipsec-protocolo-de-seguranca-para-redes-ip/>>. Acessado em 29 de Setembro de 2017.

FALSARELLA, D. Conceitos de IPSec, 2008. Disponível em: <<https://imasters.com.br/artigo/9325/redes-e-servidores/conceitos-de-ipsec/?trace=1519021197&source=single>>. Acessado em 30 de Setembro de 2017.

FAQ INFORMÁTICA - Protocolo IPsec, qual é a sua funcionalidade? 2017. Disponível em:<<https://faqinformatica.com/vpns-nivel-3-ip-security-protocol-ipsec/>>. Acessado em 30 de Setembro de 2017.

HIGA, P. O estoque de endereços IPv4 no Brasil acabou, 2014. Disponível em:<<https://tecnoblog.net/158099/ipv4-brasil-america-latina-esgotado/>>. Acessado em 19 de Novembro de 2017.

IBM - Cabeçalho de Autenticação (Authentication Header). Disponível em:<[https://www.ibm.com/support/knowledgecenter/pt/ssw\\_ibm\\_i\\_72/rzaja/rzaj\\_aahheader.htm](https://www.ibm.com/support/knowledgecenter/pt/ssw_ibm_i_72/rzaja/rzaj_aahheader.htm)>. Acessado em 30 de Setembro de 2017.

MORIMOTO, C. O esgotamento do IPV4, 2011. Disponível em:<<http://www.hardware.com.br/artigos/esgotamento-ipv4/>>. Acessado em 21 de Setembro de 2017.

TERRA - Entenda o protocolo IP e a diferença entre IPv4 e IPv6, 2011. Disponível em:< <https://www.terra.com.br/noticias/tecnologia/internet/entenda-o-protocolo-ip-e-a-diferenca-entre-ipv4-e-ipv6,3a98fe32cdbda310VgnCLD200000bbcceb0aRCRD.html>>. Acessado em 18 de Setembro de 2017.

OLHAR DIGITAL - Do IPv4 para o IPv6: Você sabe o que significa esta mudança? 2011. Disponível em:<[https://olhardigital.com.br/video/do\\_ipv4\\_para\\_o\\_ipv6\\_voce\\_sabe\\_o\\_que\\_significa\\_esta\\_mudanca/16840](https://olhardigital.com.br/video/do_ipv4_para_o_ipv6_voce_sabe_o_que_significa_esta_mudanca/16840)>. Acessado em 19 de Novembro de 2017.

OLIVEIRA, A. Os endereços IP estão acabando: a Internet já está migrando para IPv6, 2017. Disponível em:< <http://www.hardwaremagazine.com.br/2017/03/os-enderecos-ip-estao-acabando-internet.html>>. Acessado em 8 de Novembro de 2017.