FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Paulo Henrique Menoni

CONFIGURANDO UM FIREWALL IPV6 EM REDES CORPORATIVAS

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Paulo Henrique Menoni

CONFIGURANDO UM FIREWALL IPV6 EM REDES CORPORATIVAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof.(o) Edson Gaseta

Área de concentração: Segurança em redes de computadores

Americana, SP.

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

M517c MENONI, Paulo Henrique

Configurando um firewall IPv6 em redes corporativas./ Paulo Henrique Menoni. – Americana: 2017.

60f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

Paulo Henrique Menoni

CONFIGURANDO UM FIREWALL IPV6 EM REDES CORPORATIVAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança em redes de computadores

Americana, 30 de Junho de 2017.

Banca Examinadora:

Edson Roberto Gaseta - (Presidente)
Especialização em Redes de Computadores
Faculdade de Tecnologia de Americana - FATEC

Acácia de Fátima Ventura - (Membro)
Doutorado em Educação
Faculdade de Tecnologia de Americana - FATEC

Benedito Aparecido Cruz - (Membro)
Mestrado em andamento em Multimeios
Faculdade de Tecnologia de Americana - FATEC

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por permitir que eu chegasse até aqui com determinação e perseverança, ao meu orientador Edson Roberto Gaseta pelo apoio prestado durante a construção deste trabalho, a Fatec Americana e os docentes pela dedicação dispensada e aos meus amigos que me ajudaram e apoiaram durante todo o curso.

DEDICATÓRIA

A minha esposa Vanessa e minha filha Julia, que são a razão de todo meu esforço e dedicação. Só se educa pelo exemplo.

RESUMO

O presente texto procura abordar todas as principais características do protocolo IPv6, bem como seus respectivos componentes. Através dele é possível verificar uma série de itens a serem configurados para manter uma rede IPv6 segura. O trabalho também abrange o conceito de firewall bem como sua utilização dentro do contexto IPv6, no intuito de garantir a segurança dentro de uma rede local e seu perímetro com a Internet. Com o esgotamento dos endereços IPv4, é de suma importância dominar as técnicas de firewall referentes ao protocolo IPv6 afim de mitigar as ameaças existentes recorrentes da comunicação fim-a-fim, onde todos os dispositivos de uma rede local estão passíveis de um ataque partindo de qualquer lugar na Internet. Através de um experimento irá ser demonstrados os riscos a uma rede sem qualquer proteção e os impactos que tal vulnerabilidade poderá acarretar.

Palavras Chave: IPv6; Firewall; IP6Tables.

ABSTRACT

The present text tries to address all the main characteristics of the IPv6 protocol, as well as its respective components. Through it you can check a series of items to configure to maintain a secure IPv6 network. The work also covers the concept of firewall as well as its use within the IPv6 context, in order to ensure security within a local network and its perimeter with the Internet. With the exhaustion of IPv4 addresses, it is extremely important to master firewall techniques related to the IPv6 protocol in order to mitigate the recurring threats of end-to-end communication, where all the devices in a local network are capable of attack starting from Anywhere on the Internet. An experiment will demonstrate the risks to a network without any protection and the impacts that such vulnerability may entail.

Keywords: *IPv6, Firewall; IP6Tables*

SUMÁRIO

Lista de Figuras:

Lista de Tabelas

1 INTRODUÇÃO

Com o crescimento do número de dispositivos conectados à Internet ocorreu o esgotamento dos endereços IPv4, o que fez com que houvesse uma grande mobilização para a rápida adoção do protocolo IPv6, que por natureza possui uma quantidade de endereços substancialmente maior que seu antecessor. O advento da Internet das coisas (IOT) tende a popularizar o IPv6 rapidamente e conseguinte a quantidade de dispositivos ligados a ela.

Contudo, a rápida adoção do IPv6 não se preocupou com a principal propriedade do protocolo, a comunicação fim-a-fim, o que poderia deixar um dispositivo vulnerável a ataques a partir de qualquer lugar do mundo. Para as organizações e empresas é fundamental que haja uma proteção entre o perímetro da rede local e a Internet afim de proteger as informações e os ativos de ataques maliciosos afim de explorar vulnerabilidades ou obter dados confidenciais. Para permitir o uso seguro da Internet alguns cuidados devem ser tomados onde é necessário que os serviços disponibilizados e as comunicações realizadas por este meio garantam princípios básicos de segurança, como:

- **Integridade**: proteger a informação contra alteração não autorizada.
- **Confidencialidade**: proteger a informação contra acesso não autorizado.
- **Disponibilidade**: garantir que um recurso esteja disponível sempre que necessário.

Este trabalho tem como finalidade explorar os aspectos técnicos e as características do protocolo IPv6, demonstrar técnicas de proteção utilizando firewall baseado no sistema operacional Linux, alicerçados nos princípios da segurança da informação e levando em conta as recomendações da RFC4890 e as boas práticas sugeridas pelos autores especialistas neste assunto. O desenvolvimento deste trabalho irá demonstrar as consequências em um ambiente de testes sem firewall IPv6 e as técnicas para a implantação do mesmo afim de mitigar tais ameaças.

2 REFERENCIAL TEORICO

Neste capítulo serão apresentadas as características, funcionamento e novos recursos do protocolo IPv6. Serão abordados as técnicas e os tipos de firewall que podem ser utilizados em uma rede corporativa.

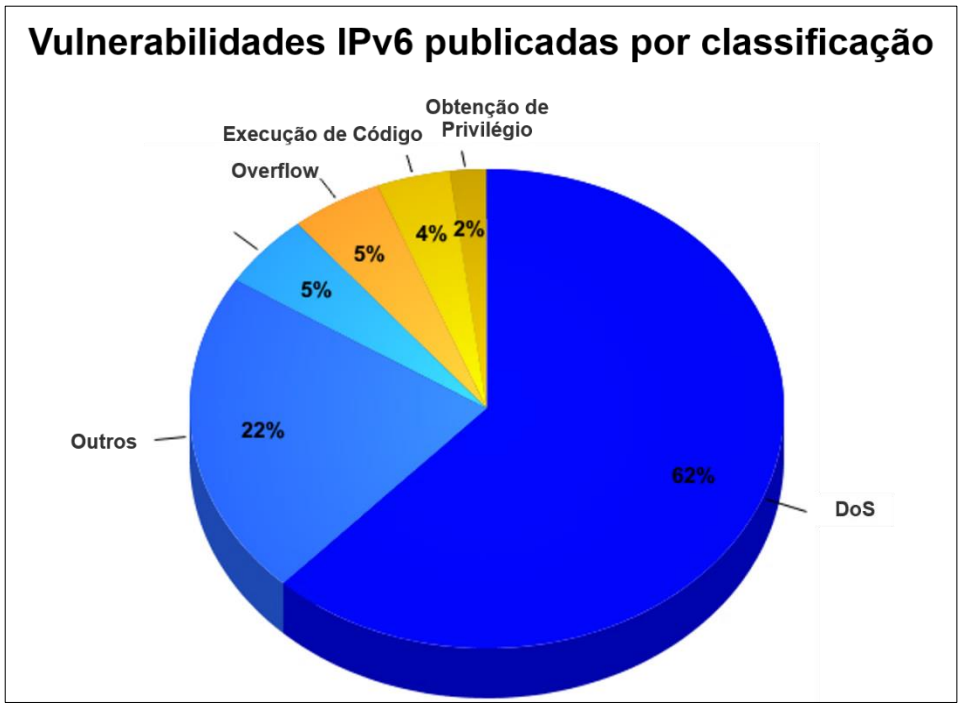
2.1 A Segurança da informação no protocolo IPv6

Segundo Minoli e Kounz (2009), o protocolo IPv6 permitirá a endereçabilidade fim-a-fim de centenas de bilhões de dispositivos nos próximos anos. A medida que a aumenta a quantidade de dispositivos conectados, tais como telefones celulares, sensores para uso agrícola, sensores meteorológicos, televisores, eletrodomésticos, sensores biométricos e biomédicos entre outros, existe uma necessidade intrínseca de cuidados com a segurança da informação e se torna imperativo a utilização de recursos de proteção para a preservação dos mesmos.

De acordo com Brito (2013), existe um folclore em torno do protocolo IPv6 que ele é mais seguro que seu antecessor IPv4. Por ser mais robusto e ter corrigido a maioria das falhas de desenvolvimento do IPv4 criou-se uma expectativa exagerada com relação ao IPv6, portanto é equivocado afirmar que o mesmo é mais seguro que seu antecessor pelo simples fato dele possuir suas respectivas falhas de segurança pertinentes ao desenvolvimento do protocolo. Por sua adoção ainda tímida perante ao IPv4, ainda é difícil dizer quais problemas de segurança o IPv6 traz consigo e fatalmente trará novas ameaças e tipos de ataques que não existem no seu antecessor IPv4. Na Figura 1 será mostrada uma lista de vulnerabilidades do protocolo IPv6 por classificação por tipo de ameaça.

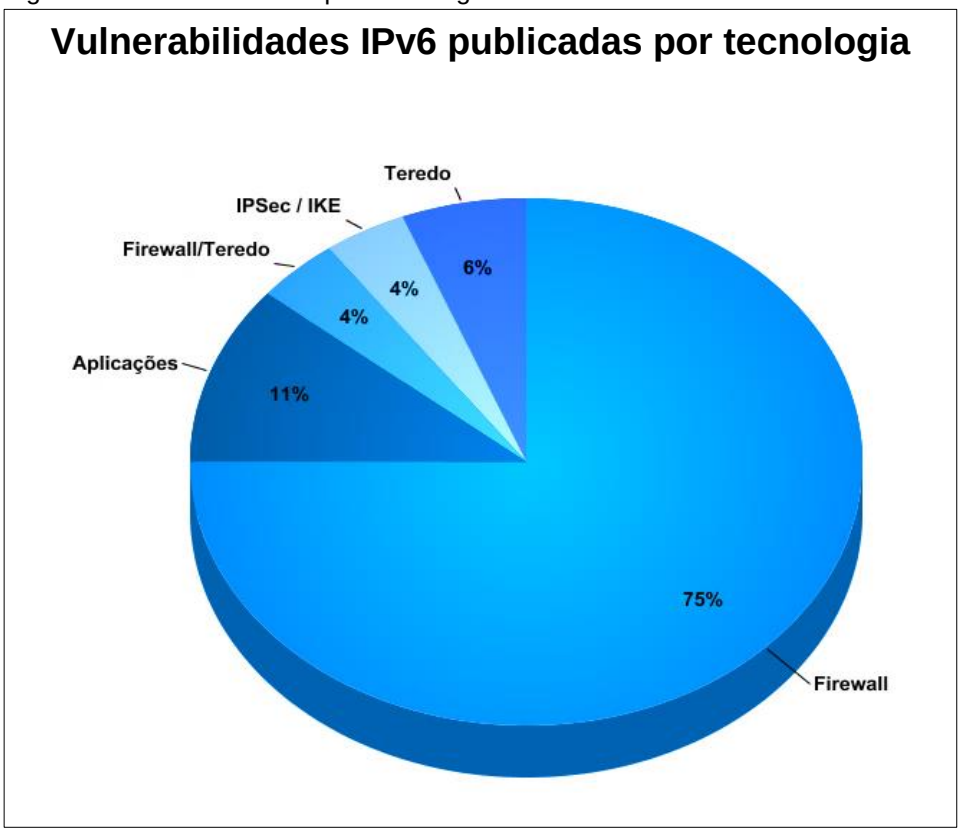
Segundo IPV6.BR(2012), é possível notar que o grande percentual de vulnerabilidades acontece na tecnologia de firewall onde o mesmo é incorretamente implementado pelo fabricante do software ou hardware ou mal implementado pelo próprio usuário ou administrador de redes que desconhece os riscos que esse tipo de falha pode trazer. Na Figura 2 será demonstrado os resultados desta pesquisa.

Figura 1 - Vulnerabilidade por classificação de Ameaças



Fonte: Comitê Gestor da Internet no Brasil (2012).

Figura 2 - Vulnerabilidade por tecnologia



Fonte: Comitê Gestor da Internet no Brasil (2012).

2.2 O Protocolo IPv6

No início da década de 1990, o IETF iniciou um projeto afim de desenvolver um protocolo que substituiria o IPv4 e que suportasse a alta demanda por endereçamentos públicos e oferecesse suporte a novos serviços multimídia, surgiu então o IPv6.

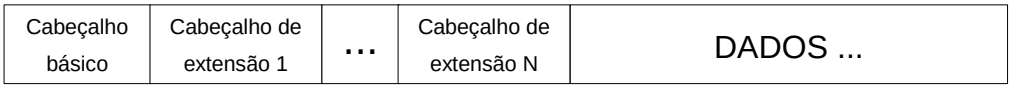
O protocolo IPv6 herdou muitas características do IPv4, o que no fundo, caracteriza o IPv6 sendo basicamente o IPv4 com algumas melhorias e pequenas modificações.

De acordo com Comer (2006), as mudanças inseridas pelo protocolo IPv6 são agrupadas em sete categorias que o autor explica a seguir:

- Endereços maiores: O tamanho do endereço é mudança mais visível. O protocolo IPv6 multiplica por quatro o tamanho de um endereço IPv4 de 32 bits, ou seja, o tamanho de endereço IPv6 é de 128bits.
- Hierarquia de endereço estendida: O IPv6 usa um espaço de endereço maior para criar níveis adicionais de hierarquia de endereçamento.
- Formato do cabeçalho flexível: O IPv6 possui um formato de datagrama totalmente novo, com cabeçalhos opcionais, o que torna o IPv6 totalmente incompatível com o IPv4.
- Opções avançadas: O IPv6 possui controle opcionais incluídos no datagrama os quais não eram disponíveis no IPv4.
- Provisão para a 0 de protocolo: Possui adaptabilidade a novas aplicações ou hardwares sem ter que especificar todos os detalhes.
- Suporte para autoconfiguração e numeração: O protocolo IPv6 permite que dispositivos atribuam endereços locais automaticamente.
- Suporte para alocação de recurso: O protocolo IPv6 possui um cabeçalho de diferenciação de serviços (DiffServ), este é idêntico ao do IPv4.

Formato geral de um datagrama IPv6: No protocolo IPv6 o formato do datagrama mudou completamente, onde um datagrama IPv6 tem um cabeçalho básico com tamanho fixo seguido por zero ou mais cabeçalhos de extensão e sem seguida vem os dados, como mostra a Figura 1:

Figura 3 - Formato do Datagrama IPv6

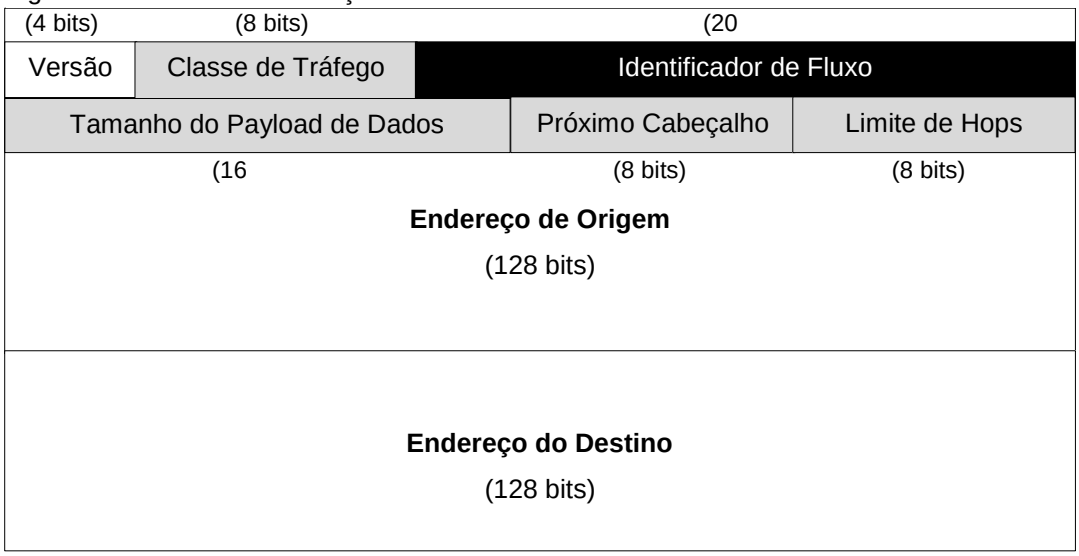


Fonte: adaptado de Comer (2006)

Formato básico do cabeçalho IPv6: Segundo Comer (2006), embora o endereço IPv6 seja maior em tamanho, seu cabeçalho tem menos informações que um cabeçalho de datagrama IPv4, por não possuir campos fixos, estes foram movidos para cabeçalhos de extensão, portanto são opcionais. No geral, as mudanças realizadas no cabeçalho do datagrama refletem as seguintes mudanças no protocolo:

- Alinhamento foi modificado de 32 bits par 64 bits.
- O campo de tamanho do cabeçalho foi eliminado, e o campo de tamanho do datagrama foi substituído pelo campo Tamanho do *Payload* (PAYLOD LENGTH).
- Os campos endereço de origem e destino foram aumentados para 16 octetos cada um.
- A informação de fragmentação foi movida para um cabeçalho de extensão, antes ficava fixo no cabeçalho.
- O campo Tempo de Vida (*Time to live*) foi substituído por um campo chamado Limite de Saltos (*Hop limit*).
- O campo Tipo de serviço (*Service type*) foi renomeado para Classe De Tráfego (*Traffic class*) e também foi estendido com o campo Rótulo de Fluxo (FLOW LABEL).
- O campo Protocolo (PROTOCOL) foi substituído por um campo que especifica o tipo do próximo cabeçalho.

Figura 4 - Formato do Cabeçalho IPv6



Fonte: adaptado de Comer (2006).

Conforme observado na Figura 2, o cabeçalho IPv6 divide-se nos seguintes campos:

- Versão (4 bits): Identifica a versão do protocolo usado, neste caso o valor do campo é 6.
- Classe de Tráfego (8 bits): Identifica os pacotes por classes de serviços ou prioridades.
- Identificador de fluxo (20 bits): Identifica os pacotes do mesmo fluxo de comunicações.
- Tamanho de Dados (16 bits): Indica o tamanho em bytes apenas dos dados enviados junto ao cabeçalho IPv6.
- Próximo cabeçalho (8 bits): Identifica o cabeçalho de extensão que segue o atual.
- Limite de encaminhamento (8 bits): Este campo é decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado.
- Endereço de origem (128 bits): Identifica o endereço de origem do pacote.
- Endereço de destino (128 bits): Identifica o endereço de destino do pacote.

Cabeçalhos de extensão: Segundo Tanenbaum (2011), o IPv6 introduziu o conceito de um cabeçalho de extensão (opcional). Esses cabeçalhos foram criados com a finalidade de oferecer informações extras, desde que elas sejam codificadas de maneira eficiente. Atualmente, há seis tipos de cabeçalhos de extensão definidos e todos eles são opcionais, mas se houver mais de um, eles terão de aparecer logo depois do cabeçalho fixo preferencial na ordem listada na Tabela 1.

Tabela 1 - Cabeçalhos de extensão

Cabeçalhos de extensão	Descrição
Hop-by-hop options	Informações diversas para os roteadores
Destination options	Informações adicionais para o destino
Routing	Lista parcial de roteadores a visitar
Fragmentation	Gerenciamento de fragmentos de datagramas
Authentication	Verificação da identidade do transmissor
Encrypted security payload	Informações sobre o conteúdo criptografado

Fonte: adaptado de Tanenbaum (2011).

2.2.1 A estrutura de endereçamento IPv6

De acordo com Brito (2013), o protocolo IPv6 tem como principal objetivo resolver o problema da falta de endereços disponíveis na Internet, provendo desta forma a inclusão de mais usuários e dispositivos conectados à rede global. Para se ter uma ideia da quantidade de endereços disponíveis em IPv6. A Tabela 2 compara a quantidade de endereços entre os dois protocolos.

Tabela 2 - Quantidade de endereços IPv4 e IPv6

Protocolo	Bits	Quantidade de endereços públicos
IPv4	32	4.294.967.296
IPv6	128	340.282.366.920.938.463.374.607.431.768.211.456

Fonte: adaptado de Brito (2013).

O que pode ser constatado é que o protocolo IPv6 tem uma quantidade de endereços que equivale a 79 trilhões de trilhões de vezes a quantidade de endereços IPv4.

2.2.2 Notação de endereçamento IPv6

Segundo Comer (2006), após resolvido o problema de esgotamento de endereços IP pelo protocolo IPv6, um novo problema surgiu, a manipulação por pessoas desses endereços e sua complexidade. Utilizar a notação binária ou decimal seria praticamente impossível para um formato de 128 bits, foi proposta a notação hexadecimal com dois pontos, sendo que a cada 16 bits é representado em hexadecimal separado por dois pontos. Existe uma vantagem visível por exigir menos dígitos e caracteres separadores que o decimal pontuado e também menos caracteres que o binário. Na Tabela 3 será comparada a complexidade entre os sistemas decimal e hexadecimal:

Tabela 3 - Notação IPv6 Hexadecimal e Decimal

Notação IPv6 Decimal	104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255
Notação IPv6 Hexa	68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF

Fonte: adaptado de Comer (2006)

Nota-se que a notação hexadecimal com dois pontos é mais simples em relação a decimal pontuada. Existem também duas técnicas de simplificação do endereçamento IPv6, a primeira é uma regra que permite omitir todos os zeros a esquerda de um quarteto. Portanto um número escrito "00b1" pode ser escrito como "b1"e ter o mesmo significado. Uma ressalva deve ser feita nesta regra, não é permitido a omissão de zeros a direita, por exemplo "1c00" não pode se comprimir em "1c".

A segunda regra permite a representação de uma sequência continua de zeros através do caractere "::", sendo que só é possível aplicá-la uma única vez em todo o endereço. Um endereço IPv6 possui oito quartetos, portanto, qualquer endereço com menos de oito quartetos que possua a notação "::" deverá ter a diferença preenchida com zeros até atingir o limite de oito quartetos (BRITO, 2013). Na Figura 5 é demonstrada a utilização das duas regras de simplificação.

Figura 5 - Técnica de Abreviação de endereços IPv6

Fonte: adaptado de Brito (2013).

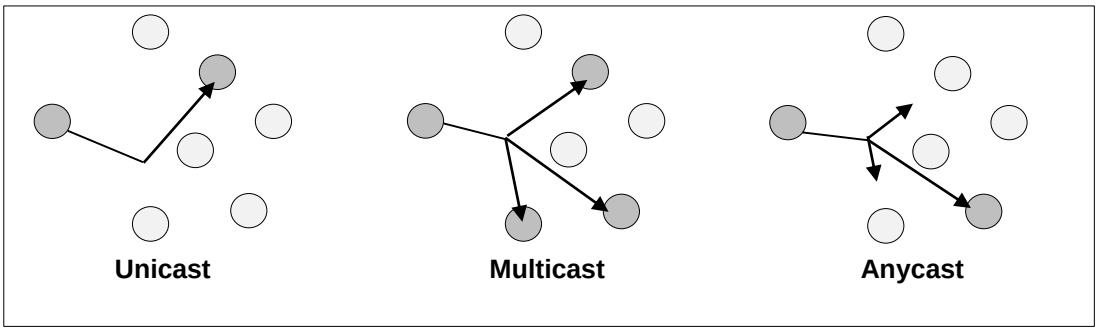
Segundo Brito (2013), o uso incorreto da segunda regra de abreviação pode causar ambiguidade, pois durante a reversão o sistema pode reescrever o endereço incorretamente. Por isso a segunda regra deve ser usada apenas uma vez.

2.2.3 Tipos de endereço

De acordo com Brito (2013) existem diferentes tipos de endereços IP, cada um de natureza especifica para uma rede de dados. No IPv6 existem três tipos de endereços:

- **Unicast:** desenvolvido para identificar um único host, portanto, um pacote enviado a um endereço *unicast* é entregue somente a um host. Também é conhecido como comunicação um-para-um.
- **Multicast:** serve para identificar um conjunto de hosts, portanto, quando um pacote é enviado a um endereço multicast é entregue a todos os hosts associados a esse endereço. Também é conhecido como comunicação um-para-muitos.
- **Anycast:** este tipo de endereço identifica um conjunto de hosts, porém, o pacote é entregue ao host mais próximo da origem. Isso é feito utilizado protocolos de roteamento com vetor de distância. Este tipo de endereço é conhecido como um-para-um-de-muitos

Figura 6- Tipos de endereço IPv6



Fonte: adaptado de Brito (2013).

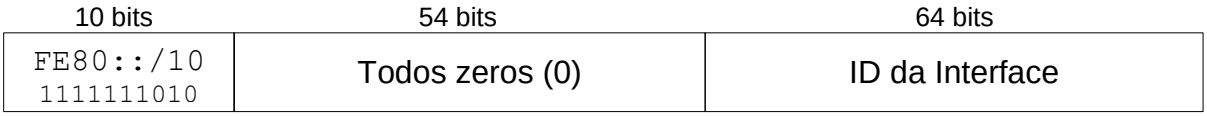
Vale ressaltar que diferentemente do protocolo IPv4, o protocolo IPv6 não possui o tipo de endereço broadcast. Essa função foi transferida para tipos específicos de endereços multicast, onde todos os hosts são ingressados automaticamente no grupo multicast-all-nodes identificado pelo endereço `FF02::1`. A comunicação multicast é obrigatória nas redes IPv6.

Endereços Unicast: Endereços unicast são utilizados para comunicação entre dois hosts, como computadores, servidores, telefones IP, celulares, etc. Estes endereços foram desenvolvidos para prover o modelo de comunicação fim-a-fim.

Link-Local: Os endereços IPv6 do tipo link-local são usados somente para enviar pacotes do enlace rede local, ou seja, são endereços que não são roteáveis para a Internet ou para qualquer outro roteador. Quando um host é conectado a uma rede local, seu algoritmo de endereçamento IPv6 irá lhe atribuir um endereço local automaticamente que será usado para comunicar-se com outros dispositivos IPv6 e serviços que estejam disponíveis na rede, tais como o Protocolo de Descoberta de Rede (NDP) ou um servidor DHCP, no caso DHCPv6. (ODOM, 2008).

Os primeiros 10 bits do endereço do tipo link-local englobam os seguintes intervalos: `FE80::/10, FE90::/10, FEA0::/10 e FEB0::/10`, os demais 54 bits são preenchidos com zeros e o sufixo de 64 bits identificador do host é gerado automaticamente a partir do MAC Address da interface de rede do dispositivo através do protocolo EUI-64. (ODOM, 2008).

Figura 7 - Formato de endereçamento Link-Local

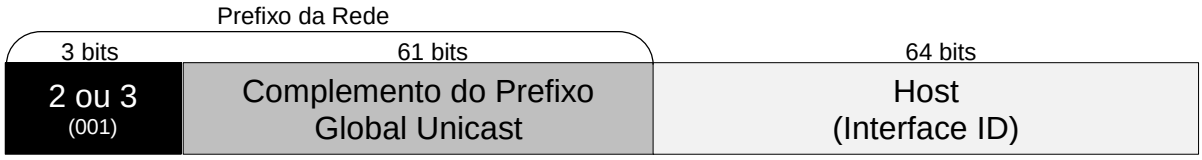


Fonte: adaptado de Odom(2008)

Unique-Local Address (ULA): Os endereços do unique-local disponibilizam um plano de endereçamento não roteável na internet, devendo ser utilizados somente em redes internas. Para este endereçamento foi definida a faixa "FC00::/7". Só deve ser usado caso haja a necessidade de interligar redes diferentes que não irão ter acesso à Internet, como redes de impressoras ou de gerência interna por exemplo (BRITO, 2013).

Global Unicast: Os endereços do tipo global unicast são públicos e roteáveis na Internet e são distribuídos pelas autoridades responsáveis pela governança da internet. A IANA, órgão que controla a distribuição desses endereços no mundo, disponibilizou 13% do total de endereços IPv6 disponíveis. Este percentual foi distribuído entre autoridades regionais (RIR) em prefixos /12 o que corresponde a uma quantia considerável de endereços. O prefixo 2000::/3 estão disponíveis na Internet (BRITO, 2013).

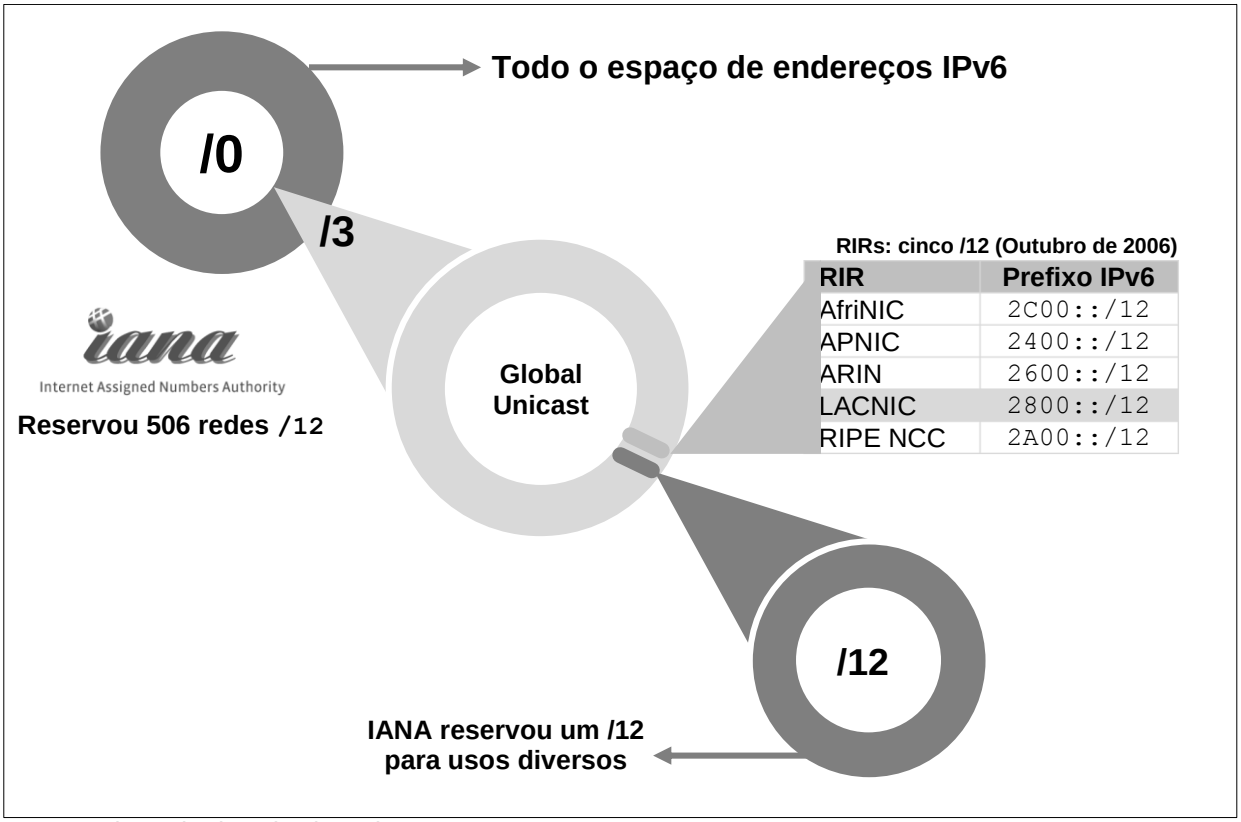
Figura 8 - Formato do Prefixo IPv6



Fonte: adaptado de Odom (2008)

O prefixo 2000::/3 compreende a faixa de endereços entre: 2000:0:0:0:0:0:0:0 até 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF o que é mais que suficiente para o crescimento da Internet nos próximos anos.

Figura 9 - Distribuição dos Prefixos IPv6 pelo IANA



Fonte: adaptado de Brito (2013)

A IANA disponibilizou uma a rede `2000::/3`, da qual é possível criar 512 prefixos `/12`. Considerando que a mesma distribui um prefixo `/12` para cada autoridade regional ou RIR (Regional Internet Registries) e mais um prefixo para usos diversos, a autoridade possui 506 prefixos /12 para futuro crescimento da Internet mundial utilizando somente uma fração do total de endereços disponíveis (BRITO, 2013). A autoridade regional da América Latina é conhecida como LACNIC recebeu o prefixo `2800::/12`, que foi subdividido em prefixos /16 para as autoridades nacionais de cada país. No caso do Brasil a autoridade é o NIC.BR, órgão ligado ao governo que controla a distribuição dos endereçamentos IPv6 entre as operadoras de telecomunicações. Estas por sua vez fazem a distribuição dos endereçamentos aos usuários finais e empresas seguindo recomendações da RFC4291, que orienta delegar prefixos /56 para usuários residenciais e prefixos /48 para empresas (NIC.BR,2017).

Endereços Multicast: Os endereços multicast são usados para comunicar-se com grupos de hosts, sendo obrigatório a sua utilização em redes IPv6. Os endereços multicast são iniciados em `FF00::/8`, ou seja, todos os endereços iniciados com `FF` sempre são multicast. Este tipo de endereçamento só deve ser utilizado na origem da comunicação pois ele representa um grupo com vários hosts. O grupo multicast-all-nodes possui todos os hosts de uma rede local e faz o papel de broadcast pois permite que um host se comunique com todos os outros que fazer parte deste grupo. O grupo multicast-all-nodes é representado pelo endereço `FF02::1`. Os grupos multicast padronizados pela RFC2375 são utilizados para os mais diversos contextos como por exemplo os protocolos de roteamento dinâmico, servidores de configuração dinâmica de endereçamento (DHCP) e servidores de sincronismo de horário (NTP).

Tabela 4 - Contextos dos Endereços Multicast IPv6

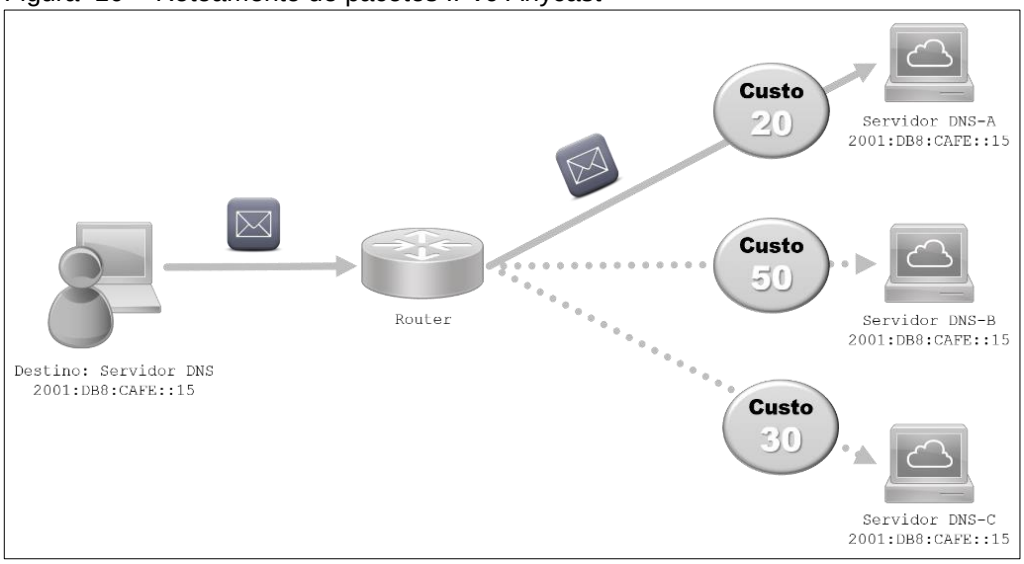
Endereço	Escopo	Descrição
`FF01::1`	Interface	Todas as interfaces
`FF02::1`	Enlace	Todos os hosts no link
`FF02::2`	Enlace	Todos os roteadores no link
`FF02::5`	Enlace	Protocolo OSPFv3 (roteadores)
`FF02::6`	Enlace	Protocolo OSPFv3 (roteadores)
`FF02::9`	Enlace	Protocolo RIPng
`FF02::A`	Enlace	Protocolo Cisco EIGRP
`FF02::1:FFXX:XXXX`	Enlace	Solicited-Node
`FF02::1:2`	Enlace	Todos os servidores DHCP e relay-agents
`FF02::1:3`	Site	Todos os servidores DHCP
`FF0X::101`	Variável	Todos os servidores NTP
*O Caractere “X” representa um valor variável.		

Fonte: adaptado de Brito (2013).

De acordo com IPV6.BR(2012), o funcionamento dos endereços multicast se assemelha aos do tipo broadcast, sendo diferenciado que enquanto o broadcast envia pacotes para todos os host da rede, o multicast envia somente a um grupo desejado. É importante que os roteadores ligados ao backbone de Internet não encaminhem pacotes do tipo multicast à rede mundial, ficando restrito ao enlace onde o mesmo está localizado.

Endereços Anycast: de acordo com Brito (2013), o modelo de endereçamento anycast usa o conceito de proximidade para encaminhar um pacote até um nó da rede permitindo utilizar o mesmo endereço “unicast” em múltiplos servidores ou roteadores, diminuindo assim a quantidade de saltos necessários para chegar até um determinado destino. O ganho de performance é sensível aplicando essa técnica em redes de grande porte. Uma aplicação muito comum é a criação de redes Anycast para servidores DNS afim de garantir rapidez nas transações de resolução de nomes. A Figura 10 ilustra esse modelo de aplicação.

Figura 10 - Roteamento de pacotes IPv6 Anycast



Fonte: adaptado de Brito (2013).

Endereços especiais: o protocolo IPv6 possui alguns endereçamentos especiais, o primeiro deles é o endereço de loopback representado pelo endereço `0000:0000:0000: 0000:0000:0000:0001/128` ou pela sua forma abreviada “`::1`”, este representa o próprio host. O endereço `2001:DB8::/32` foi reservado para fins didáticos, podendo ser utilizado em materiais acadêmicos, textos e documentações, evitando assim a exposição de endereços públicos desnecessariamente (RFC3849).

2.2.4 O protocolo ICMPv6

O protocolo ICMPv6 (Internet Message Control for IPv6) além de ser um software utilizado em diagnósticos de rede, ele é a base para o funcionamento de uma rede IPv6. O ICMPv6 é responsável pela comunicação entre os hosts de uma rede IPv6, portanto não deve ser bloqueado arbitrariamente como seu antecessor e sua utilização é obrigatória em redes IPv6. O ICMPv6 assumiu características de outros protocolos existente no seu antecessor afim de diminuir a multiplicidade de protocolos o que acaba dificultando a coerência e aumenta a quantidade de implementações nos diversos dispositivos existentes (IPV6.BR, 2012). Esses protocolos são:

- ARP (*Address Resolution Protocol*), mapeia endereços físicos em endereços lógicos;
- RARP (*Reverse Address Resolution Protocol*), faz o reverso do ARP, mapeia endereços lógicos em físicos;
- IGMP (*Internet Group Management Protocol*), responsável por gerenciar os membros de um determinado grupo multicast;

O ICMPv6 funciona inteiramente na camada 3 encapsulado dentro de pacotes IP e isso exige atenção pois um firewall pode bloquear funções básicas como a descoberta de vizinhança e autoconfiguração caso a implementação seja feita sem levar em conta essa característica (IPV6.BR,2012). É importante considerar que o ICMPv6 é utilizado pelos seguintes protocolos:

- MLD (*Multicast Listener Discovery*), que opera com o gerenciamento os grupos multicast;
- NDP (*Neighbor Discovery Protocol*), responsável por identificar e aprender características de rede da vizinhança;
- Path MTU (*Max Transfer Unity*), utilizado no processo de descoberta do menor caminho de comunicação entre dois nós;
- *Mobility Support*, gerencia os endereços de origem de host dinamicamente;

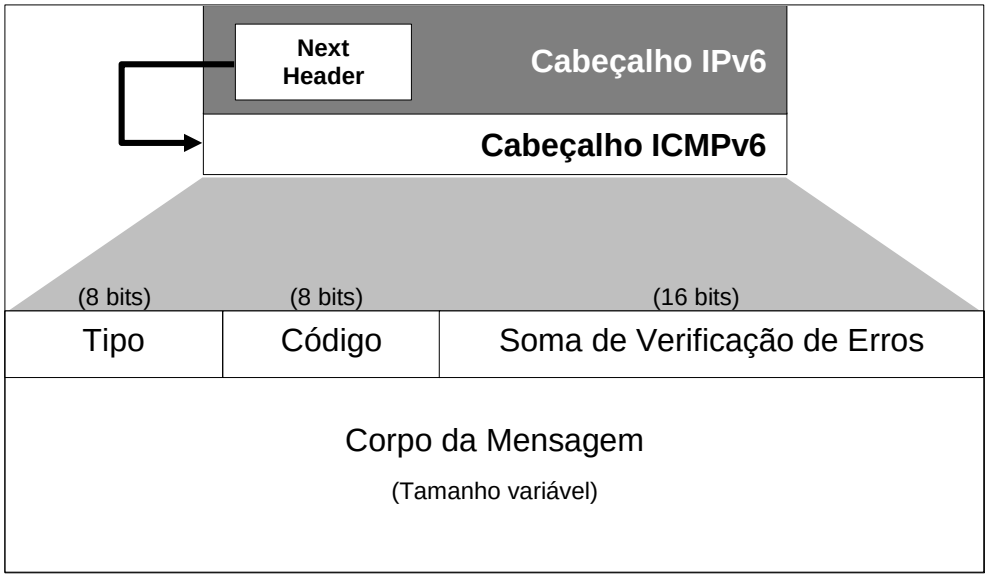
- Autoconfiguração Stateless, atribui automaticamente endereços IP globais sem uso do DHCP;

A integração do ICMPv6 ao protocolo IPv6 é através do código 58 no campo “Próximo cabeçalho” do cabeçalho básico do IPv6. Existem dois campos de tipo e código que representam o formato da mensagem, um deles é para verificação de erros e integridade das mensagens de controle e outro de tamanho variável que é a mensagem propriamente dita. Existem dois tipos de mensagens ICMPv6, as mensagens de erros e as mensagens de informação. As mensagens de erro são identificadas pelo bit à esquerda mais representativo igual a zero, enquanto as mensagens de informação são identificadas pelo bit 1 no mesmo campo (BRITO, 2013).

O ICMPv6 possui uma estrutura simples baseado em quatro campos:

- Type (8 bits): determina o tipo da mensagem e consequentemente o formato do corpo da mensagem.
- Code (8 bits): Informações adicionais sobre o motivo da mensagem
- Checksum (16 bits): Utilizado na detecção de erros no cabeçalho IPv6.
- Data (Tamanho variável): Informações relativas ao tipo da mensagem tais como erros ou diagnósticos.

Figura 11 - Formato do Cabeçalho ICMPv6



Fonte: adaptado de Brito (2013).

2.2.5 Classes das mensagens ICMPv6

De acordo com o IPV6.BR (2012), o amplo conjunto de informações transmitidas por meio dos pacotes ICMPv6 formam duas classes de mensagens, as de Erros as de Informação. As Tabelas 5 e 6 mostram as características de cada tipo de informação.

Tabela 5 - Mensagens de Erro ICMPv6

Type			Code		Extra
Valor	Nome	Descrição	Valor	Descrição	RFC
1	Destination Unreachable	Indica falha na entrega do pacote	0	Sem rota para o destino	RFC2643, RFC4443
			1	Comunicação com o destino proibida administrativamente	
			2	Além do escopo do endereço de origem	
			3	Endereço não acessível	
			4	Porta não acessível	
			5	Falha na política de ingresso/egresso	
			6	Destino rejeitado	
			7	Erro no cabeçalho de origem	
2	Packet Too Big	Indica que o pacote ultrapassou o limite do enlace	0	Pacote ultrapassou o MTU	RFC2463, RFC4443
3	Time Exceded	Indica que o limite de encaminhamento ou tempo de remontagem do pacote foi excedido	0	Limite de encaminhamento excedido no tráfego	RFC2643, RFC4443
			1	Tempo de remontagem de fragmento excedido	
4	Parameter Problem	Indica erro em algum capo do cabeçalho IPv6 ou que o tipo indicado no próximo cabeçalho não foi reconhecido	0	Campo errado do cabeçalho encontrado	RFC2643, RFC4443
			1	Encotrado um tipo do Next Header não reconhecido	
			2	Encontrado um IPv6 Option não reconhecido	
127	-	Reservado para expansão das mensagens de erro	-	--	RFC4443
255	-	Reservado para expansão das mensagens de erro	-	--	RFC4443

Fonte: Adaptado de IPV6.BR (2012)

Tabela 6 - Mensagens de Informação ICMPv6

Type			Code		Extra
Valor	Nome	Descrição	Valor	Descrição	RFC
128	Echo Request	Utilizadas no comando ping	0	-	RFC2463, RFC4443
129	Echo Reply		0	-	
130	Multicast Listerner Query	Utilizadas no gerenciamento de grupos multicast	0	-	RFC2710
131	Multicast Listerner Report		0	-	
132	Multicast Listerner Done		0	-	
133	Router Solicitation	Utilizadas com o protocolo de Descoberta de Vizinhança	0	-	RFC2461
134	Router Advertisement		0	-	
135	Neighbor Solicititation		0	-	
136	Neighbor Advertisement		0	-	
137	Redirect Message		00	-	
138	Router Renunbering	Utilizada no mecanismo de re-endereçamento de roteadores	0	Comando renumeração de roteadores	RFC2894
			1	Resultado da renumeração de roteadores	
			255	Reseta o número de sequencia	

Type			Code		Extra
139	ICMP Node Information Query	Utilizadas para descobrir informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de rede	0	Transmitir um campo que contém um endereço IPv6 que é o objetivo da query	RFC4620
			1	Transmitir um campo que contém um nome que é o objetivo da query	
			2	Transmitir um campo que contém um endereço IPv4 que é o objetivo da query	
140	ICMP Node Information Response		0	Uma resposta realizada corretamente	
			1	O dispositivo responsável por fornecer a resposta se recusou a responder	
			2	O Qtype da query é desconhecida pelo dispositivo que deve fornecer a resposta	
141	Inverse ND Solicitation Message	Utilizadas em uma extensão do protocolo de descoberta de vizinhança	0	-	RFC3122
142	Inverse ND Advertisement Message		0	-	
143	Version2 Multicast Listener Report	Utilizadas no gerenciamento de grupos multicast	-	-	RFC3810
144	HÁ Address Discovery Request Message	Utilizadas no mecanismo de mobilidade IPv6	0	-	RFC3775
145	HÁ Address Discovery Reply Message		0	-	
146	Mobile Prefix Solicitation		0	-	
147	Mobile Prefix Advertisement		0	-	
148	Certification Path Solicitation Message	Utilizadas pelo protocolo SEND	-	-	RFC3971
149	Certification Path Advertisement Message		-	-	
150	-	Utilizada experimentalmente com protocolos Seamoby	-	-	RFC4065
151	Multicast Router Advertisement	Utilizado pelo mecanismo multicast router Discovery	-	-	RFC4286
152	Multicast Router Solicitation		-	-	
153	Multicast Router Termination		-	-	
154	FMIPv6	Utilizada pelo protocolo de mobilidade FAST Handover	-	-	RFC5568

Fonte: adaptado de IPV6.BR (2012).

Segundo IPV6.BR (2012), além das mensagens descritas acima, existem alguns tipos que foram designados para uso experimental tais como os tipos 100, 101, 200 e 201 enquanto os tipos do 102 até o 126 não são utilizados.

2.2.6 O Protocolo NDP

De acordo com IPV6.BR (2012), o protocolo NDP (*Neighbor Discovery Protocol*) é parte essencial em redes baseadas no IPv6, pois foi desenvolvido com a finalidade de promover a interação entre os hosts vizinhos em uma rede onde os mesmos consigam verificar a presença uns dos outros, determinar endereços de seus vizinhos, encontrar roteadores e atualizar sua tabela de roteamento usadas na transmissão dos pacotes. O NDP conta com duas características essências para comunicação, a autoconfiguração de hosts e a transmissão de pacotes. O autor, explica que a autoconfiguração de hosts possui três funcionalidades:

- *Parameter Discovery* (Descoberta de parâmetros do enlace): é utilizado para descobrir informações sobre o enlace;
- *Address Autoconfiguration* (Autoconfiguração de endereços): executa a autoconfiguração stateless de endereços nos hosts;
- *Duplicate Address Detection* (Detecção de endereços duplicados) ou DAD: Verifica se o endereço desejado já está sendo usado por outro host;

O IPV6.BR (2012), explica que são seis as funcionalidades de transmissão:

- *Router Discovery* (Descoberta de roteadores): descobre se existem roteadores dentro do enlace;
- *Prefix Discovery* (Descoberta de prefixos): é utilizado para decidir para onde os pacotes serão transmitidos numa comunicação;
- *Address Resolution* (Resolução de endereços): descobre o endereço físico (MAC) de uma interface através de seu endereço lógico IPv6;
- *Neighbor Unreachability Detection* (Detecção de atividade no vizinho): descobre se um vizinho está alcançável dentro de uma rede;
- *Redirect* (Redirecionamento de rotas): é utilizada para que um roteador informe a melhor rota para envio de pacotes a um determinado destino;
- *Next-hop Determination* (Determinação de próximo salto): mapeamento de endereços IP para onde os pacotes devem ser enviados segundo seu endereço de destino;

De acordo com Brito (2013), o NDP não é um protocolo a parte dentro do IPv6, pois o mesmo funciona a partir do ICMPv6, portanto possui alguns tipos de mensagens reservadas para sua função. Além das mensagens de erros e as mensagens de informação (Tabela 7), o NDP possui os respectivos tipos de mensagens afim de descoberta de vizinhança:

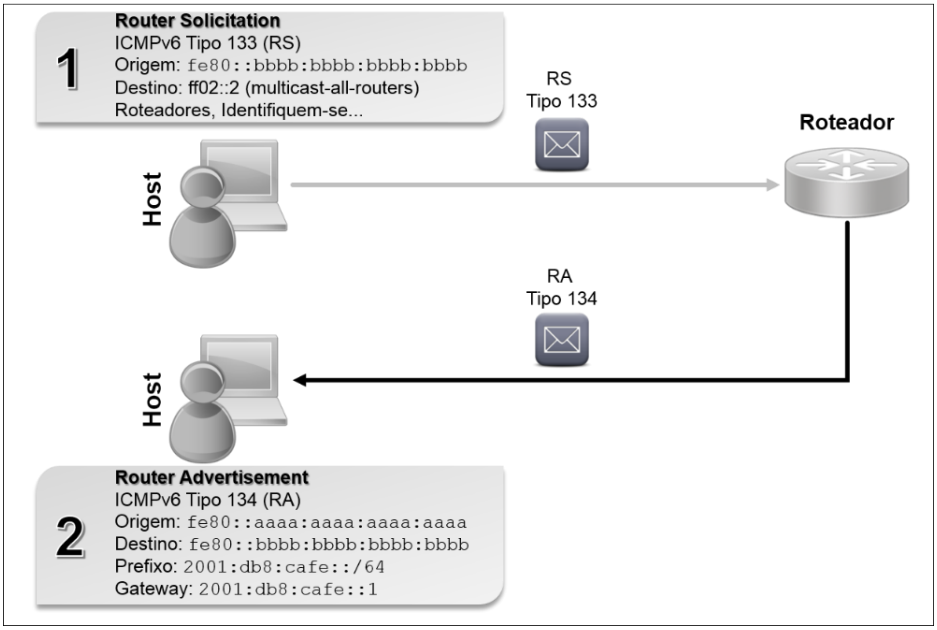
Tabela 7 - Tipos de mensagens NDP

Tipo	Mensagem	Descrição
133	RS – Router Solicitation	Enviada pelos hosts para encontrar roteadores
134	RA – Router Advertisement	Enviada periodicamente pelos roteadores
135	NS – Neighbor Solicitation	Enviado para obter informações de vizinhança
136	NA – Neighbor Advertisement	Enviada por um host como resposta à solicitação
137	Redirect	Enviado por roteadores para redirecionar rotas

Fonte: Adaptado de Brito (2013).

As mensagens do tipo Router Solicitation (RS), são utilizadas por hosts que desejam encontrar os roteadores dentro do enlace, afim de autoconfigurar seu endereço global. As mensagens do tipo Router Advertisement são enviadas pelos roteadores dentro do enlace afim de anuncia-los ou em respostas às mensagens de Router Solicitation. As mensagens do tipo Neighbor Solicitation (NS), é originada por um host da rede afim de obter informações sobre os hosts vizinhos que por sua vez responde com uma mensagem de Neighbor Advertisement informando o host originador que o mesmo se encontra no enlace. As mensagens de Neighbor Solicitation e Neighbor Advertisement são necessárias para três finalidades, resolução de endereços físicos, detecção de endereços duplicados e detecção de atividade no vizinho. Descoberta de roteadores e prefixos: Quando um host ingressa na rede local, ele precisa descobrir a existência de um ou mais roteadores no enlace, então ele envia um pacote ICMPv6 do tipo 133 (RS) com destino ao endereço multicast `ff02::2` (multicast-all-routers), de forma que os roteadores presentes no enlace respondem com uma mensagem do tipo router advertisement com uma mensagem ICMPv6 do tipo 134 (RA) com o destino o endereço unicast link-local do host solicitante. Nas mensagens do tipo 134(RA), o roteador informa os dados do prefixo da rede bem como a gateway da rede que deverá ser utilizado (BRITO, 2013).

Figura 12 – Descoberta de prefixos IPv6



Fonte: adaptado de BRITO (2013).

Resolução de endereços físicos: O endereço lógico conhecido como IP, serve para identificar os hosts de uma rede de maneira universal, porém dentro de um contexto de rede local a comunicação básica ocorre através dos endereços físicos, conhecidos como MAC Address. No protocolo IPv6 a responsabilidade de resolver endereços IP em endereços físicos é feito através do protocolo NDP por meio das mensagens ICMPv6 tipo 135 (NS) e ICMPv6 Tipo 136 (NA), onde cada host mantém uma tabela com as associações entre os endereços IPv6 e seu respectivo endereço MAC (BRITO, 2013).

2.3 Firewall no IPv6

De acordo com Brito (2013), o firewall IPv6 tem papel fundamental na segurança da rede devido a efetiva implantação da comunicação fim-a-fim como uma realidade, todas as redes globais são públicas o que torna o firewall elemento de atenção dentro de um contexto IPv6. Contudo é necessário levar em consideração alguns aspectos e particularidades referentes ao protocolo IPv6, como por exemplo, o papel desempenhado pelo protocolo ICMPv6, que possui diversas responsabilidades dentro da operação de uma rede IPv6, portanto, não pode ser bloqueado deliberadamente como acontecia no IPv4. Por outro lado, a liberação total de troca de mensagens ICMPv6 traz consequências sérias podendo dar origem a ataques de negação de serviços e outros tipos de riscos. A RFC4890 propõe uma série de boas práticas que devem ser adotadas na configuração de um firewall IPv6 principalmente direcionando quais mensagens ICMPv6 devem ser bloqueadas e quais devem ser permitidas. A Tabela 8 resume as recomendações da RFC4890:

Tabela 8 - Recomendações da RFC4890

Recomendado não descartar		
Mensagem (Tipo)	**Trânsito (Global)**	**Local**
Mensagens de Erro:	**Permite não local quando associado a conexões permitidas**	
Time Exceeded (3) – Código 1	✔	✔
Parameter Problem(4) – Código 0	✔	✔
Obrigatório não descartar		
Mensagem (Tipo)	**Trânsito (Global)**	**Local**
Manutenção da Comunicação:	**Permite não local quando associado a conexões permitidas**	
Destination Unreachable (1) – Todos os códigos	✔	✔
Packet Too Big (2)	✔	✔
Time Exceeded (3) – Somente Código 0	✔	✔
Parameter Problem (4) – Códigos 1 e 2	✔	✔
Verificação de Conectividade	**Permite ou Nega de acordo com a política de segurança da topologia**	
Echo Request (128)	✔	✔
Echo Response (129)	✔	✔
Configuração de endereços e seleção de roteadores	**Permitido somente em tráfego link-local**	
Router Solicitation (133)		✔
Router Advertisement (134)		✔
Neighbor Solicitation (135)		✔
Neighbor Advertisement (136)		✔
Inverse Neighbor Discovery Solicitation (141)		✔
Inverse Neighbor Discovery Advertisement (142)		✔

Obrigatório não descartar		
Mensagem (Tipo)	**Trânsito (Global)**	**Local**
Notificação de recebedores de multicast link-local:	**Permitido somente em tráfego link-local**	
Listener Query (130)		✔
Listener Report (131)		✔
Listener Done (132)		✔
Listener Report v2 (143)		✔
Notificação do Caminho de Certificação SEND	**Permitido somente em tráfego link-local**	
Certification Path Solicitation (148)		✔
Certification Path Advertisement (149)		✔
Multicast Router Discovery	**Permitido somente em tráfego link-local**	
Multicast Router Advertisement (151)		✔
Multicast Router Solicitation (152)		✔
Multicast Router Termination (153)		✔

Fonte: adaptado de IPV6.BR (2012)

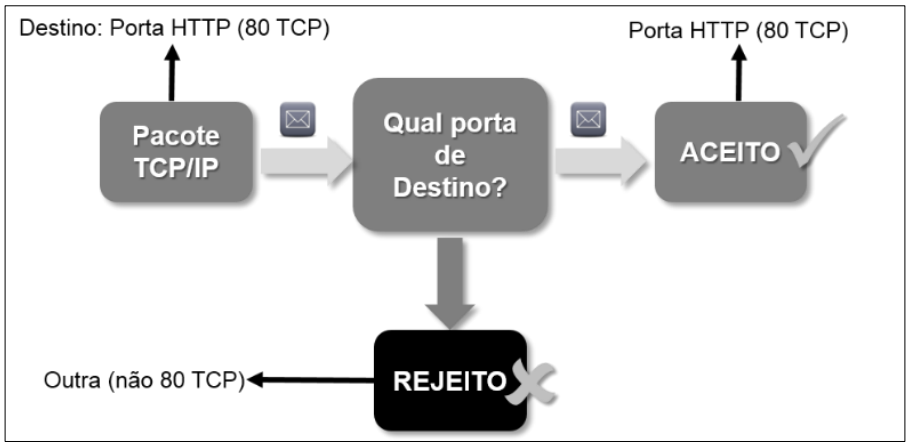
2.3.1 Tipos de Firewall

De acordo com Minoli e Kouns (2009), quando uma organização está procurando implementar segurança em uma rede, o tipo de firewall selecionado deve ser baseado em requisitos específicos. O tipo de ativos a serem protegidos determinará o tipo de firewall que deverá ser implementado. Houveram vários avanços nas tecnologias de firewall nos últimos anos, e embora possa haver algumas tecnologias especificas, a maioria dos firewalls agora podem ser agrupados nas seguintes categorias:

- Firewall Stateless;
- Firewall Stateful;
- Firewall de Aplicação;

Firewall Stateless: Os firewalls do tipo stateless funcionam examinando pacotes e se concentram em coletar informações de cabeçalho para tomar decisões de filtragem. Esse tipo de firewall opera avaliando endereços de origem e de destino e portas de serviço. Enquanto os firewalls de filtragem de pacotes não oferecem recursos sofisticados ou um alto nível de segurança, eles são baratos e são capazes de lidar com uma quantidade significativa de tráfego como por exemplo nos roteadores de borda de operadoras.

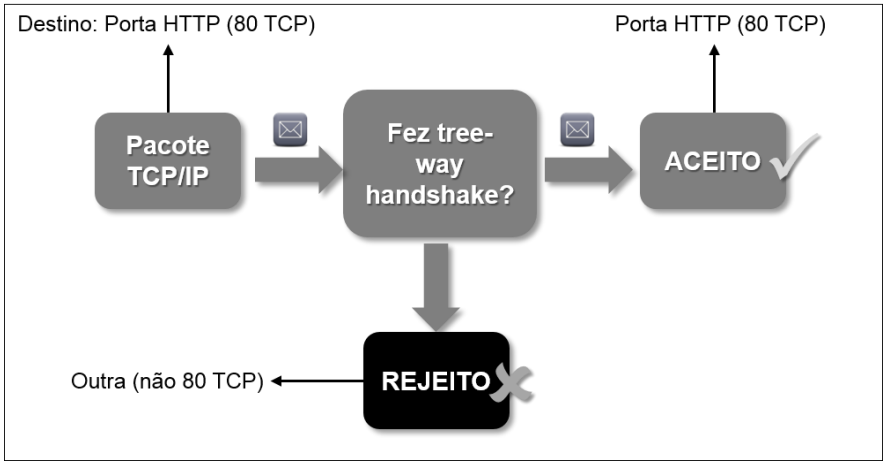
Figura 13 - Firewall Stateless



Fonte: próprio autor (2017).

Firewall Stateful: O firewall do tipo stateful (também conhecido como filtro dinâmico de pacotes), opera mantendo o controle das conexões, sendo capaz de distinguir o tráfego legítimo de um tráfego malicioso baseado no TCP Three-Way Handshake. Esta é uma melhoria de segurança importante e se torna na maioria dos casos uma vantagem sobre os firewalls do tipo stateless. O firewall stateful avalia muito mais do que informações de cabeçalho, ou seja, verifica o tráfego até a camada de aplicação do modelo OSI. No entanto, considerações de desempenho são importantes e devem ser avaliadas considerando que o estado de cada conexão é rastreado, o desempenho deste tipo de tecnologia de firewall pode ser um problema e dimensionar adequadamente a arquitetura e seus requisitos é de suma importância.

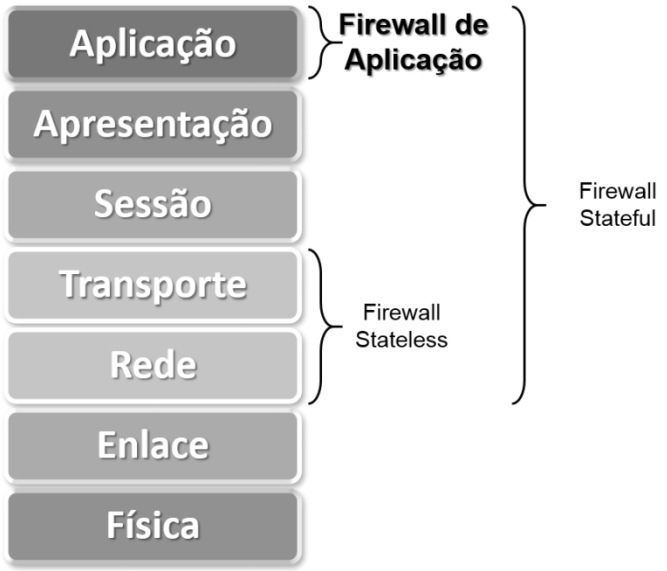
Figura 14 - Firewall Stateful



Fonte: próprio autor

Firewall de Aplicação: O firewall de aplicação ou proxy é considerado por muitos como a tecnologia de firewall mais complexa, porém, a mais segura. A diferença fundamental desta tecnologia em comparação com a filtragem de pacotes é que não há comunicação direta entre um cliente e servidor. O proxy atua efetivamente como um intermediário entre dois pontos de extremidade que precisam se comunicar e só permite conexões passando pelo firewall de aplicação.

Figura 15 - Tipo



Fonte: adaptado de Minoli e Kounz (2009).

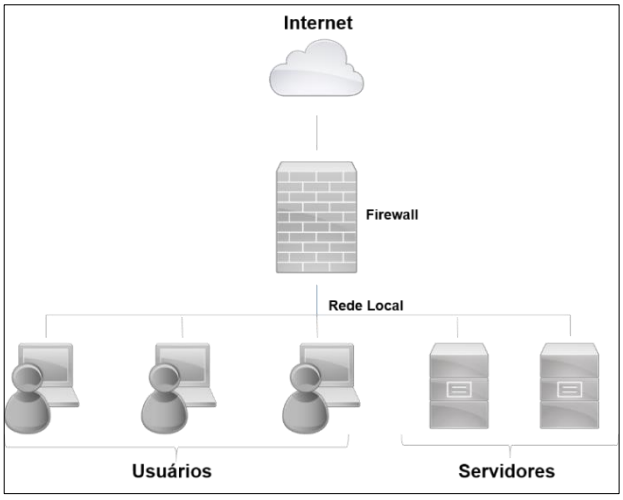
Zona Desmilitarizada (DMZ): Em um mundo onde a comunicação instantânea é fundamental, as organizações precisam ser capazes de se conectar com qualquer um e todos. Para que isso aconteça, é preciso permitir que os aplicativos e serviços se comuniquem conforme o necessário. Isso normalmente requer a implementação de uma DMZ para fornecer serviço público ao mesmo tempo proteger os ativos de uma organização. Uma DMZ é baseada no uso militar do termo que define uma zona de demarcação ou buffer entre duas redes que não são de confiança. Uma capacidade chave de um firewall é ser capaz de criar uma DMZ e então controlar o acesso dentro e fora da rede protegendo os serviços públicos que são oferecidos.

2.3.2 Arquitetura de firewall

De acordo com Minoli e Kouns (2009), tão importante quanto escolher o tipo apropriado de firewall a ser implementado, é saber onde colocar um firewall dentro da rede da organização. Antes de ter uma sólida estratégia de como instalar firewalls definindo zonas de arquitetura de segurança, a maioria das organizações procurou implantar firewalls em pontos-chave do perímetro, especificamente entre as fronteiras de rede não confiáveis da Internet e da sua rede. À medida que a indústria de segurança amadureceu, aumentou a necessidade de segurança de ativos críticos, portanto, uma segmentação adicional foi estendida às redes corporativas internas. Mesmo que a maior parte da rede interna é considerada confiável, em muitos casos há uma necessidade de políticas de segurança adicionais a serem aplicadas e uma defesa de rede em camadas deve ser implementada. Embora existam muitas variações, as duas arquiteturas de firewall básicas que são mais comumente usadas de acordo com o autor são as seguintes:

- *Dual homed firewall*: Esta configuração, também conhecida como host bastião, é a mais comum por ser simples e segura. O firewall atua como a linha divisória entre duas redes, como a rede local confiável de uma organização e a Internet não confiável. O firewall está posicionado para interceptar todo o tráfego que entra e sai e é normalmente configurado para permitir muito pouco tráfego ou nenhum para a rede confiável.

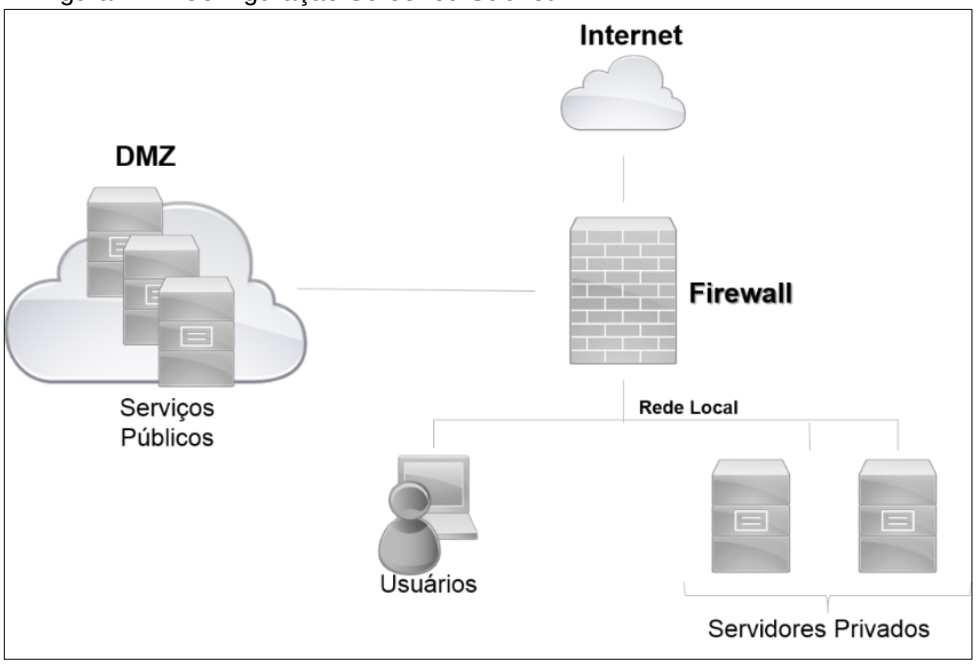
Figura 16 - Dual Homed Firewall



Fonte: adaptado de Hagen (2006).

- *Screened subnet*: Esta configuração cria um segmento de rede isolado, chamado DMZ, que pode ser controlado e monitorado separadamente da rede local. Uma sub-rede selecionada pode ser criada usando várias interfaces (pelo menos três) em um único firewall ou também pode ser implementada usando vários firewalls para criar o ambiente. Para a proteção de ativos críticos, o uso de vários firewalls é recomendado e, em alguns casos, pode proporcionar benefícios ao uso de vários fornecedores de firewall.

Figura 17 - Configuração Screened Subnet



Fonte: Adaptado de Hagen (2006).

Os profissionais de segurança devem implementar a defesa em profundidade e usar o princípio do privilégio mínimo para o controle de acesso na determinação da arquitetura de segurança de uma organização. Os firewalls devem ser implantados entre cada uma das zonas de segurança definidas para a organização enquanto fornece aos administradores de segurança a granularidade e flexibilidade para implementar os controles necessários com base na criticidade dos ativos (HAGEN, 2006).

2.3.3 Tipos de ataques conhecidos no protocolo IPv6

Segundo Brito (2013), a maioria dos ataques que ocorrem no IPv6 explora vulnerabilidades no protocolo NDP, protocolo de descoberta de vizinhança, que possui grande importância na operacionalização de redes IPv6. Portanto a maioria dos ataques acontecem com o intuito de paralisar uma rede IPv6 interrompendo o funcionamento correto do protocolo NDP. A seguir o autor lista os tipos de ataques mais comuns envolvendo o protocolo de descoberta de vizinhança.

- **Envenenamento da tabela de vizinhança:** Este tipo de ataque explora o protocolo NDP fazendo os hosts da rede inserir várias entradas falsas na sua tabela de vizinhança fazendo com que o host tenha o desempenho prejudicado em decorrência do número de entradas na tabela de vizinhança ou no pior dos casos estourar o limite entradas na tabela o que pode deixar o host inoperante na rede.
- **Falsificação de roteadores e prefixos:** Essa vulnerabilidade permite que um host desconhecido envie mensagens de ICMPv6 RA do tipo 134 falsas para se passar pelo roteador afim de interceptar o tráfego das comunicações. Este tipo de ataque também é utilizado afim inviabilizar o processo de roteamento entre as sub-redes e comprometer o funcionamento da rede como um todo.
- **Network Scanning (Varredura de endereços):** Essa técnica consiste em varrer uma rede em busca de dispositivos que possuam portas abertas com o intuito de encontrar falhas a serem exploradas. No caso do IPv6 esse mecanismo de varredura tornou-se complicado devido a quantidade de endereços possíveis dentro de um contexto IPv6. Um exemplo é uma subrede com prefixo de 64 bits que possui 18.446.744.073.709.551.616 endereços disponíveis, o que de certa forma inviabiliza este tipo de técnica. Porém podem ser utilizadas técnicas de scanning para endereços simples de ser configurados como por exemplo o endereço `2001:db8:cafe:dad0::4`, pois é passível de rastreabilidade por parte do atacante.

2.3.4 Mecanismos para defesa em redes IPv6

De acordo com Hagen (2006), não existe um guia de segurança e firewall completo para IPv6, porém, existem algumas técnicas de segurança IPv6 e filtros de firewall que devem ser considerados:

- Implementação de filtro de entrada no firewall de perímetro para endereços usados internamente.
- Filtrar serviços desnecessários no firewall de perímetro.
- Implantação de firewalls baseados em host para uma defesa em profundidade.
- Os sistemas críticos devem ter IPv6 estático, não obvio.
- Considere o uso de entradas vizinhas estáticas para sistemas críticos
- Certifique-se de que os nós finais não encaminhem pacotes com cabeçalhos de *Routing Extension*.
- Os firewalls de rede nunca devem encaminhar pacotes do tipo multicast.
- Os firewalls devem suportar a filtragem com base nos endereços de origem e destino, cabeçalhos de extensão e informações de protocolo de camada superior.
- Bloquear a utilização de técnicas de tunelamento afim de evitar ataques do tipo “backdoor” dentro da rede local.

Estas técnicas evitam grande parte dos ataques que são de conhecimento público já disseminado na comunidade técnica e que com certa certeza podem mitiga-los. A medida que o protocolo IPv6 é adotado, novos ataques irão surgir e consequentemente novos mecanismos de defesas serão desenvolvidos. Portanto é importante que o uso do IPv6 aumente em grande escala afim de aumentar a maturidade do protocolo e consequentemente a segurança embarcada no mesmo (BRITO, 2013).

3 DESENVOLVIMENTO

O objetivo deste capitulo é demonstrar através de um ambiente de testes as possíveis vulnerabilidades que podem ser encontradas em uma rede IPv6 sem os requisitos de firewall estudados no capítulo anterior. Após a detecção das falhas serão repetidos os mesmos testes utilizando os conceitos adquiridos e as boas práticas descrita nesse trabalho afim de criar defesas no perímetro da Internet.

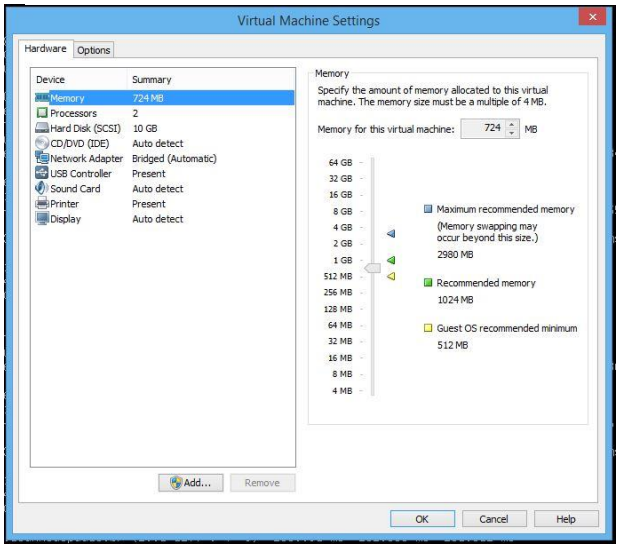
3.1 O ambiente de testes

Este ambiente de testes foi desenvolvido utilizando a tecnologia de virtualização de sistemas operacionais chamada VMware® na sua versão Workstation 12.5.5 build-5234757, instalado sobre um sistema hospedeiro Microsoft Windows 8.1 Professional 64 bits. No ambiente de testes foi utilizado para o host Atacante um link do tipo *Tunnel Broker* que é uma alternativa para conseguir se conectar à Internet via IPv6, quando o mesmo ainda não está disponível em sua rede ou em seu provedor de Internet. Esta técnica permite que hosts IPv4 isolados em uma rede acessem redes IPv6, neste caso simulando um ataque externo partindo de qualquer lugar da Internet. O sistema de *Tunnel Broker* utilizado foi o da empresa *Hurricane Eletric* (https://www.tunnelbroker.net/). Para os demais hosts, foi utilizado um link de dados da empresa Desktop Sigmanet (http://www.desktop.com.br/) com suporte nativo a IPv6, simulando um cliente corporativo implementando o novo protocolo em sua rede local.

O ambiente de testes é composto pelos seguintes elementos:

- **Host atacante:** Máquina virtual equipada com o sistema operacional Debian x64 versão 8.5. Esta máquina está fora da rede local simulando um possível invasor desferindo ataques de negação de serviços variados afim de descobrir a topologia da rede interna e quais serviços estão sendo executados em cada host encontrado. Na sua preparação foram instalados os softwares NMAP e Hydra com o intuito de testar as vulnerabilidades dentro da rede IPv6 do cliente em questão.

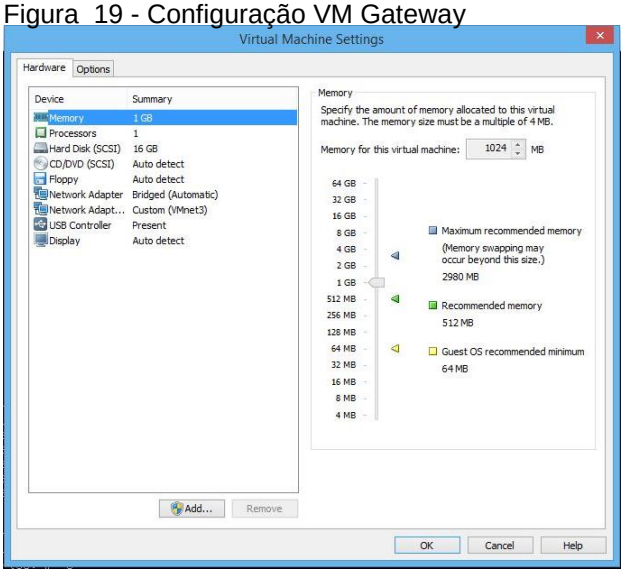
Figura 18 - Configuração VM Atacante



Fonte: próprio autor

- **Host Gateway:** Está máquina está equipada com sistema operacional Debian x64 fazendo a função de roteador de perímetro entre a rede local e a Internet. No Cenário-1 ele fará apenas papel de roteador IPv6 e no Cenário-2 será implementado um firewall IPv6 com o intuito de proteger a rede local de ataques partindo da Internet.

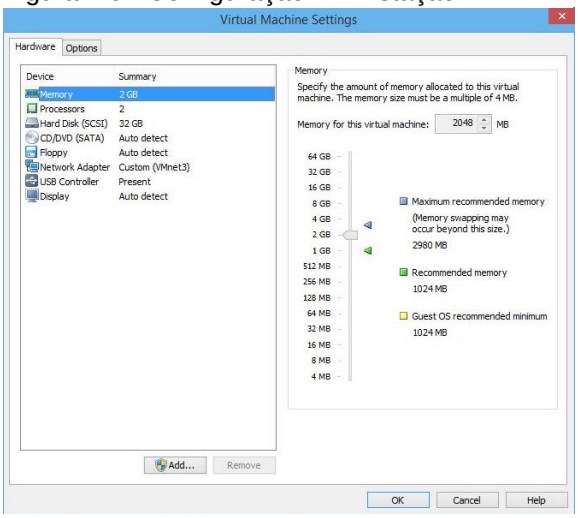
Figura 19 - Configuração VM Gateway



Fonte: próprio autor

- **Host Estação-1:** Esta máquina virtual está equipada com o sistema operacional Microsoft Windows 7 Professional simulando uma estação de trabalho dentro de um ambiente corporativo com as funcionalidades de firewall nativas do sistema desativadas.

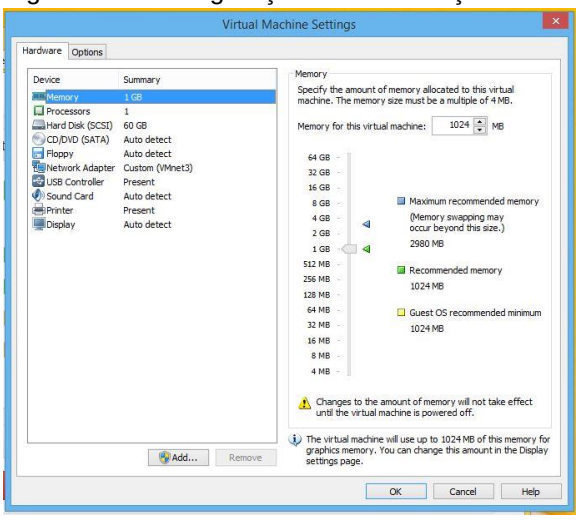
Figura 20 - Configuração VM Estação-1



Fonte: próprio autor

- **Host Estação-2:** A respectiva máquina virtual será equipada com o sistema Microsoft Windows 8.1 simulando uma estação de trabalho dentro de um ambiente corporativo com as funcionalidades de firewall nativas do sistema ativadas.

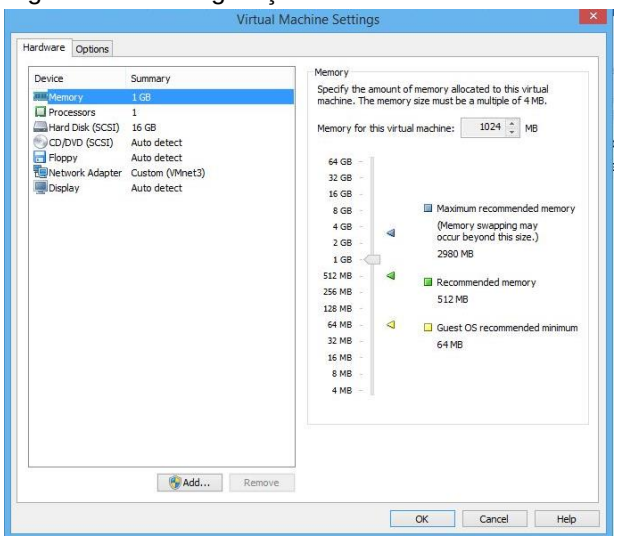
Figura 21 - Configuração da VM Estação-2



Fonte: próprio autor

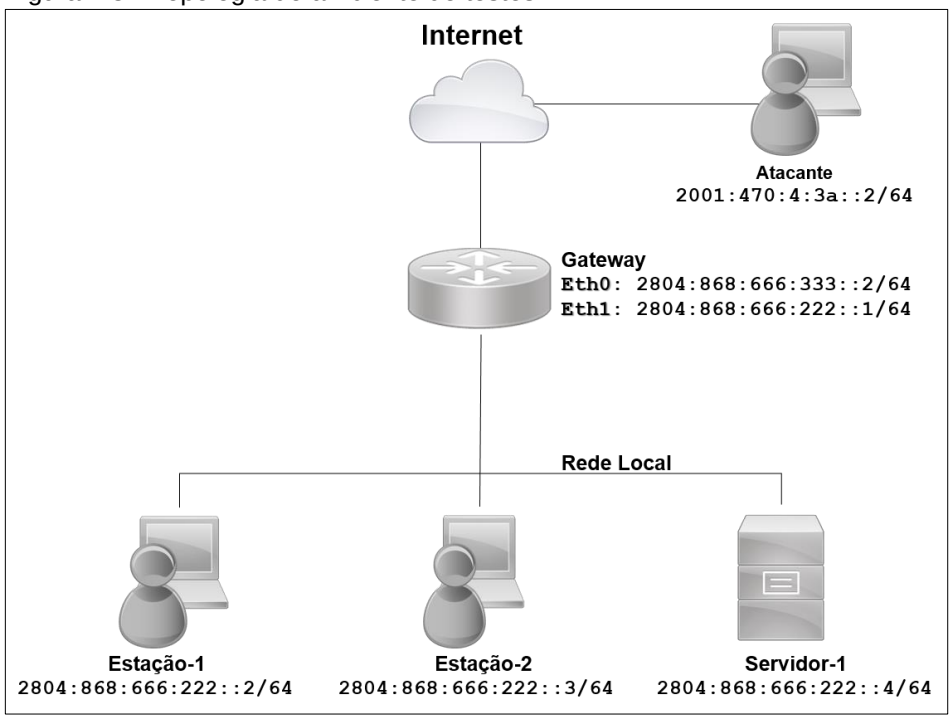
- **Host Servidor-1:** Máquina virtual com o sistema operacional Debian x86_64 versão 8.5 simulando um servidor WEB Apache com banco de dados Mysql para acesso a partir da Internet. Este host possui um serviço de *Secure Shell* (SSH) instalado e aberto para acesso remoto.

Figura 22 - Configuração da VM Servidor-1



Fonte: próprio autor

Figura 23 - Topologia do ambiente de testes



Fonte: próprio autor

3.1.1 Preparação do ambiente de testes

Configurações executadas no host Atacante:

Figura 24 – Edição do arquivo `/etc/rc.local`

```
ifconfig sit0 up
ifconfig sit0 inet6 tunnel ::209.51.161.58
ifconfig sit1 up
ifconfig sit1 inet6 add 2001:470:4:3a::2/64
route -A inet6 add ::/0 dev sit1

echo "nameserver 2001:4860:4860::8888" > /etc/resolv.conf
```

Fonte: Próprio autor

Instalação dos softwares NMAP e Hydra:

```
#apt-get install nmap hydra
```

Teste de conectividade com a Internet com IPv6:

Figura 25 - Testes de conectividade IPv6

```
root@attack-tcc:~# traceroute6 www.ipv6.br
traceroute to www.ipv6.br (2001:12ff:0:4::9), 30 hops max, 80 byte packets
 1  phmenoni-1.tunnel.tserv12.mia1.ipv6.he.net (2001:470:4:3a::1)  131.894 ms  134.587 ms  136.682 m
s
 2  10ge13-20.core1.mia1.he.net (2001:470:0:8c::1)  139.256 ms  139.391 ms  139.305 ms
 3  2001:478:124::1122 (2001:478:124::1122)  246.334 ms *  246.362 ms
 4  ae3-0.core-a.spo-piaf.algartelecom.com.br (2001:1291:0:be::a)  261.602 ms  261.509 ms  261.418 m
s
 5  et-3-0-0-0.edge-d.spo-piaf.algartelecom.com.br (2001:1291:0:d4::b)  248.541 ms  248.550 ms  252.
418 ms
 6  2001:1291:1602:24::b (2001:1291:1602:24::b)  252.314 ms  269.017 ms  251.761 ms
 7  xe-4-2-1-0.core1.nu.registro.br (2001:12ff:1::180)  251.858 ms  251.917 ms  254.949 ms
 8  xe-0-0-0.ar3.jd.registro.br (2001:12ff:2:1::250)  254.863 ms xe-0-0-0.ar3.nu.registro.br (2001:1
2ff:2:1::249)  251.479 ms  251.760 ms
 9  www.icannsãopaulo.br (2001:12ff:0:4::9)  253.091 ms  252.666 ms  251.612 ms
```

Fonte: próprio autor

Configurações executadas no host Gateway:

Figura 26 – Edição do arquivo `/etc/network/interfaces`

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet6 static
      address 2804:868:666:333::2
      netmask 64
      gateway 2804:868:666:333::1

allow-hotplug eth1
iface eth1 inet6 static
      address 2804:868:666:222::1
      netmask 64
```

Fonte: próprio autor

Ativando o repasse (*forwarding*) de pacotes IPv6 e configuração do DNS:

Figura 27 - Configurações de repasse de pacotes e DNS

```
#sysctl -w net.ipv6.conf.all.forwarding=1
#echo "nameserver 2001:4860:4860::8888" > /etc/resolv.conf
```

Fonte: próprio autor

Teste de conectividade com a Internet com IPv6:

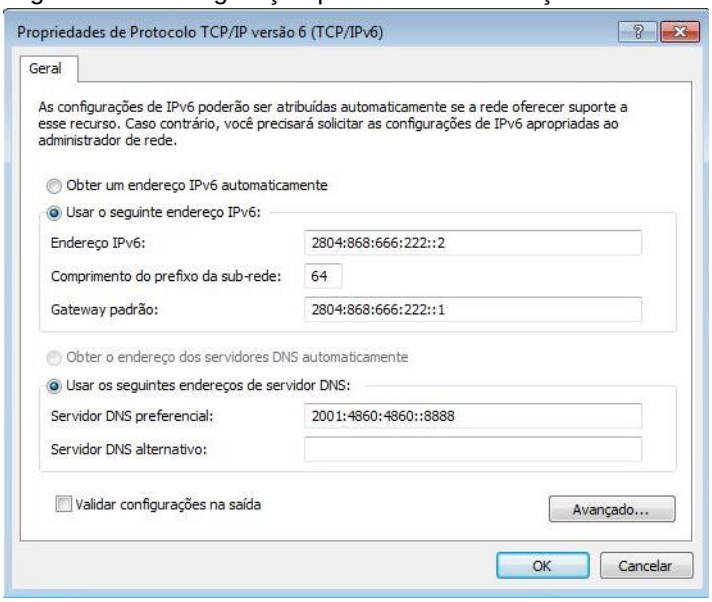
Figura 28 - Teste de conectividade IPv6

```
traceroute to www.ipv6.br (2001:12ff:0:4::9), 30 hops max, 80 byte packets
 1  2804:868:666:333::1 (2804:868:666:333::1)  27.265 ms * *
 2  2804:868:3::1 (2804:868:3::1)  26.652 ms  27.089 ms  26.878 ms
 3  2804:4c0:ffff:ff3e::1 (2804:4c0:ffff:ff3e::1)  29.359 ms  29.390 ms  29.398 ms
 4  2804:4c0:ffff:fc36::2 (2804:4c0:ffff:fc36::2)  29.185 ms  28.967 ms  28.926 ms
 5  xe-5-1-0-0.core1.jd.registro.br (2001:12ff:1::157)  29.184 ms  28.572 ms  28.879 ms
 6  xe-0-0-0.ar3.jd.registro.br (2001:12ff:2:1::250)  28.790 ms  9.414 ms  9.612 ms
 7  igfbrazil2007.br (2001:12ff:0:4::9)  9.130 ms  10.124 ms  10.134 ms
```

Fonte: próprio autor

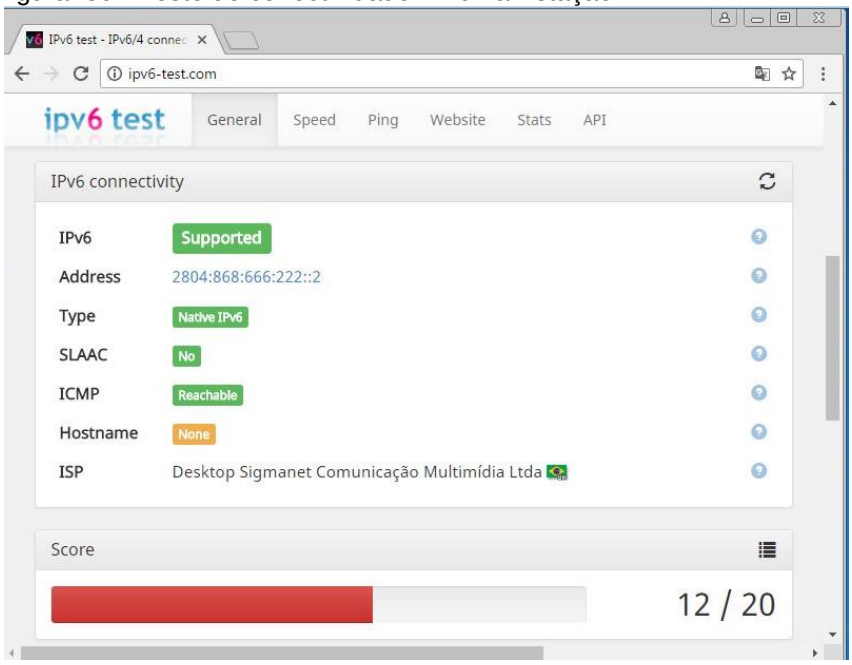
Configurações executadas no host Estação-1:

Figura 29 - Configuração placa de rede Estação-1



Fonte: próprio autor

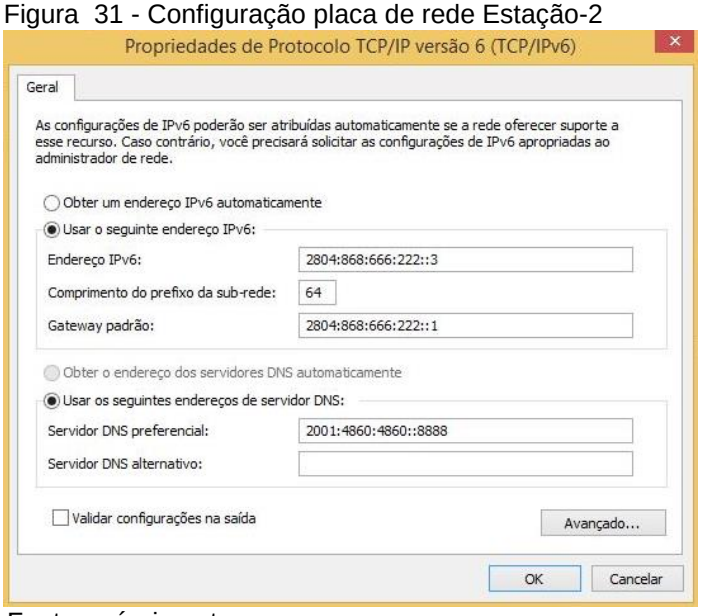
Figura 30 - Teste de conectividade IPv6 na Estação-1



Fonte: próprio autor

Configurações executadas no host Estação-2:

Figura 31 - Configuração placa de rede Estação-2



Fonte: próprio autor

Figura 32 - Teste de conectividade IPv6 na Estação-2

Fonte: próprio autor

Configurações executadas no host Servidor-1:

Figura 33 - Edição do arquivo `/etc/network/interfaces`

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet6 static
      address 2804:868:666:222::4
      netmask 64
      gateway 2804:868:666:222::1
```

Fonte: próprio autor

Instalação do serviço OpenSSH Server:

Figura 34 - Instalação dos pacotes de serviços

```
#apt-get install openssh-server
```

Fonte: próprio autor

3.1.2 Execução dos testes de ataque:

Os ataques foram realizados a partir do Host Atacante utilizando os respectivos mecanismos:

- *Port Scanning*: Varredura de portas disponíveis que podem ser utilizadas em um ataque de força bruta ou negação de serviço.
- *Brutal Force:* Trata-se de uma técnica de quebra de senhas pela força bruta utilizando um método de adivinhação de senhas baseado em um dicionário ou um banco de dados mais complexo.

Ataque de varredura de portas (Port Scanning):

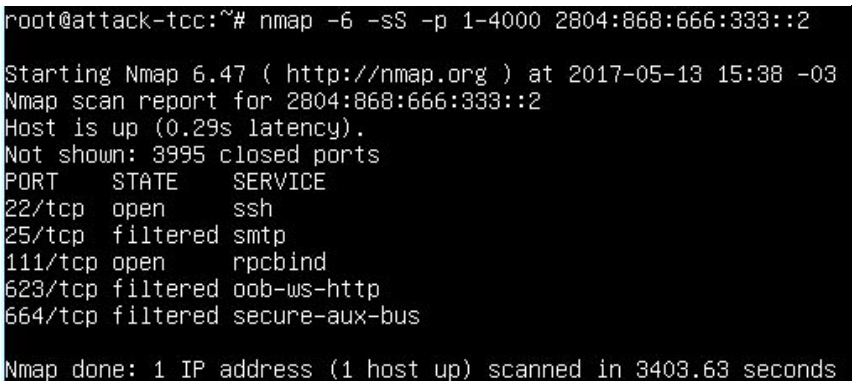
Neste ataque foi utilizado o *Nmap* ("*Network Mapper*"), uma ferramenta de código aberto para exploração de redes e auditoria de segurança. A função neste teste é demonstrar que a inexistência de um firewall IPv6 fornece ao atacante acesso a todas as portas dos hosts dentro desta determinada rede. Enquanto no protocolo IPv4, os hosts ficavam protegidos de certa forma pelo NAT, isto não acontece com o IPv6 pela sua característica fim-a-fim consequentemente a exposição de todos os hosts à Internet é inevitável.

Ataque de força bruta (Brutal Force):

O software *Hydra* é conhecido como um dos melhores para esta finalidade e pode ajudar a detectar usuários que usam senhas frágeis. Um host que tenha sofrido uma exposição pode ser explorado sem grandes dificuldades com o intuito de aproveitar-se de outras máquinas. Utilizar logins padrões como admin, administrador, root, verificar dicionários disponibilizados na internet, listas de palavras comuns que tem uma grande probabilidade de servirem como senha, como nomes de times de futebol, substituições óbvias de algumas letras como a troca de "a" por "@" ou "o" por "0", sequencias numéricas e de letras, informações pessoais coletadas principalmente em redes sociais como nome, sobrenome, data de nascimento.

Ataque de varredura de portas no host **Gateway:**

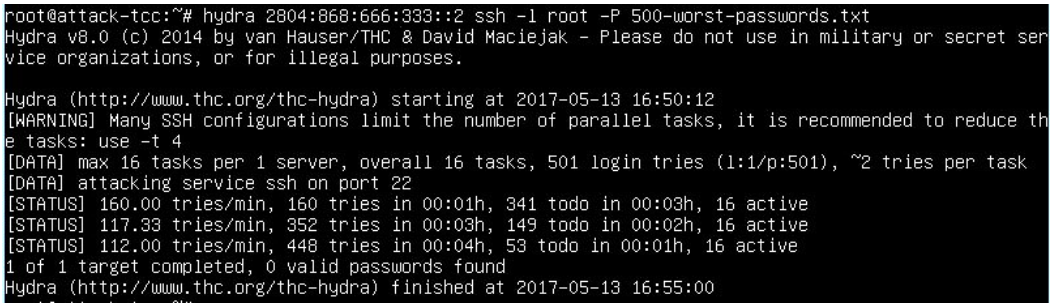
Figura 35 - Varredura de portas Host Gateway



Fonte: próprio autor

Ataque de força bruta no host **Gateway:**

Figura 36 - Ataque de força bruta host Gateway



Fonte: próprio autor

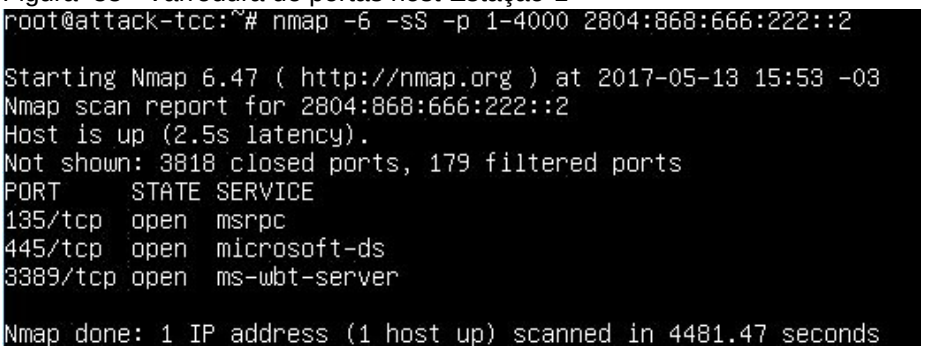
Auditoria das tentativas de invasão no host **Gateway:**

Figura 37 - Log de tentativas de ataque

Fonte: próprio autor

Ataque de varredura de portas no host **Estação-1:**

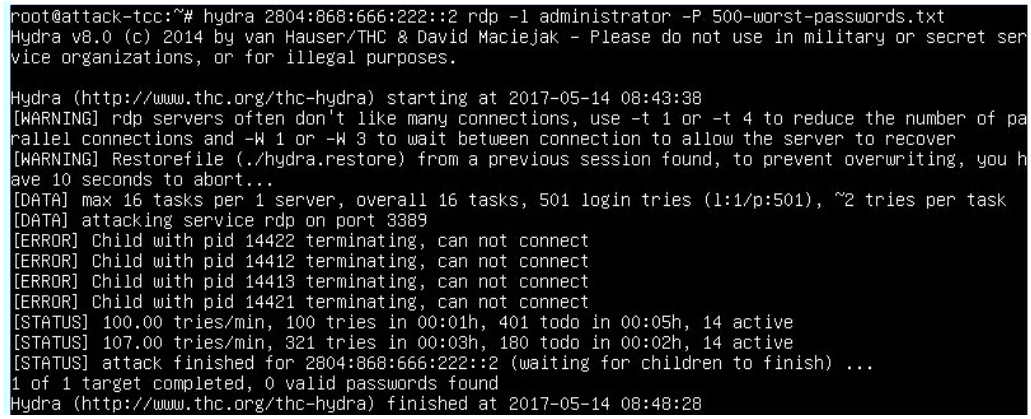
Figura 38 - Varredura de portas host Estação-1



Fonte: próprio autor

Ataque de força bruta no host **Estação-1:**

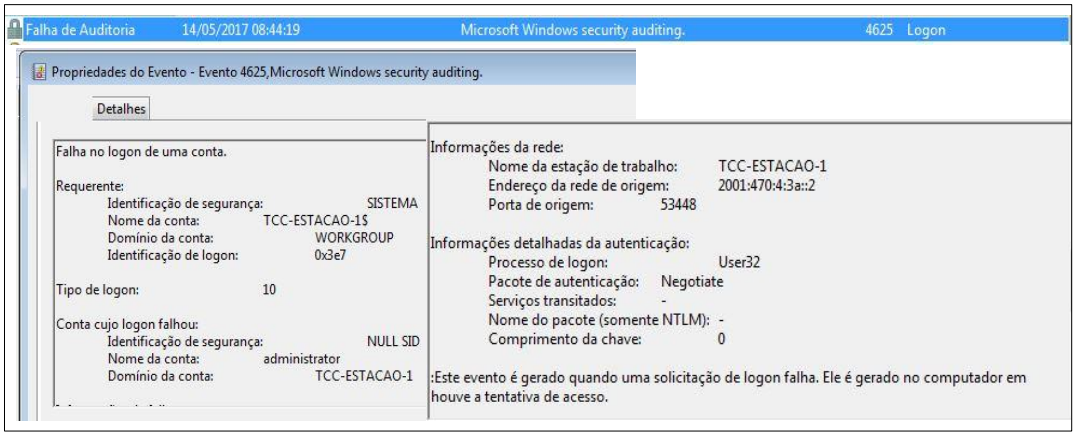
Figura 39 - Ataque de força bruta no host Estação-1



Fonte: próprio autor

Auditoria das tentativas de invasão ao host **Estação-1:**

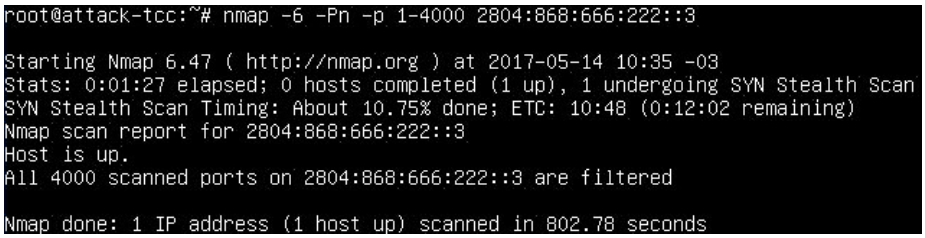
Figura 40 - Log da tentativa de ataque no host Estação-1



Fonte: próprio autor

Ataque de varredura de portas no host **Estação-2:**

Figura 41 - Varredura de portas host Estação-2



Fonte: próprio autor

Auditoria do firewall das tentativas de invasão ao host **Estação-2:**

Figura 42 - Log do Firewall do host Estação-2

Fonte: próprio autor

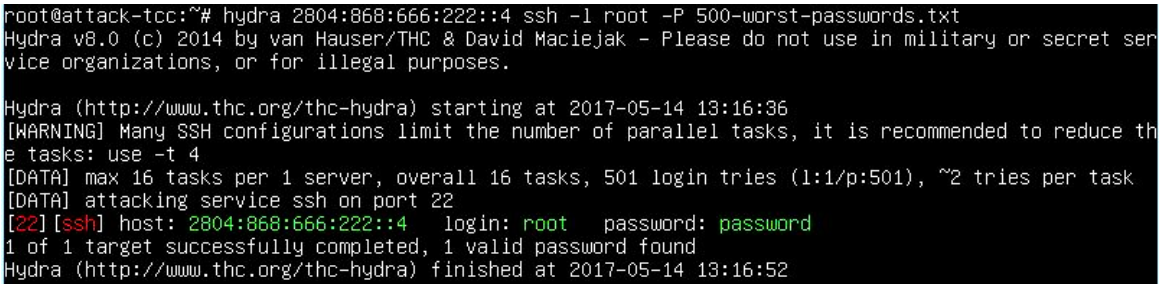
Ataque de varredura de portas no host **Servidor-1**:

Figura 43 - Varredura de portas host Servidor-1

Fonte: próprio autor

Ataque de força bruta no host **Servidor-1:**

Figura 44 - Ataque de força bruta no host Servidor-1



Fonte: próprio autor

Auditoria do firewall das tentativas de invasão ao host **Servidor-1:**

Figura 45 - Log do Firewall do host Servidor-1

Fonte: próprio autor

3.1.3 Repetição dos testes de ataque com firewall IPv6 ativado no Gateway:

Neste cenário serão executados novamente os testes de ataque, porém o host Gateway terá um firewall IPv6 stateful ativo seguindo as recomendações da RFC4890 e do privilégio mínimo discutidos nos capítulos anteriores. Será utilizado o software *ip6tables* (https://www.netfilter.org/) nativamente presente nos sistemas operacionais Linux. Esse script de firewall será armazenado no arquivo `/etc/rc.local` garantindo o início automático do mesmo.

Configuração do Firewall IPv6 no host Gateway:

Tabela 9 - Script de Firewall IPv6 com IP6TABLES

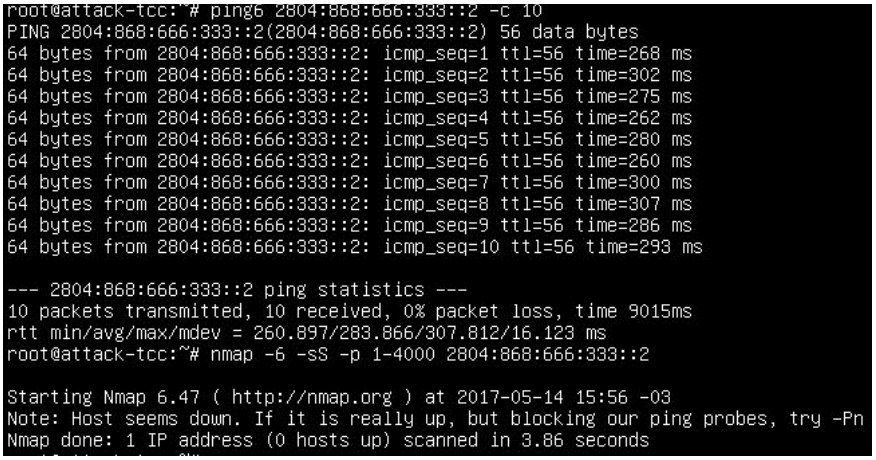
```
#!/bin/sh


IP6TABLES=ip6tables
MODPROBE=modprobe
```

```
# Interfaces de Redes
LAN=eth1
WAN=eth0

echo "Carregando Firewall IPv6 TCC Fatec Americana"

# Carregando os módulos necessários
$MODPROBE ip6_tables
$MODPROBE ip6table_filter



# Ativando o repasse de pacotes IPv6 entre as Interfaces
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

# Politica padrão de Entrada como DROP
$IP6TABLES -P INPUT DROP

# Ativando o Firewall de Entrada como Stateful
$IP6TABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Regras de Firewall para Liberar Entrada (INPUT)
$IP6TABLES -A INPUT -i lo -j ACCEPT
$IP6TABLES -A INPUT -i $LAN -j ACCEPT
$IP6TABLES -A INPUT -i $WAN -p icmpv6 -j ACCEPT

# Politica padrão de Encaminhamento como DROP
$IP6TABLES -P FORWARD DROP

# Ativando o Firewall de Encaminhamento como Statefull
$IP6TABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Regras de Firewall para Liberar Encaminhamento (INPUT)
$IP6TABLES -A FORWARD -i $LAN -o $WAN -j ACCEPT
$IP6TABLES -A FORWARD -i $WAN -o $LAN -p icmpv6 -j ACCEPT
```

Fonte: próprio autor

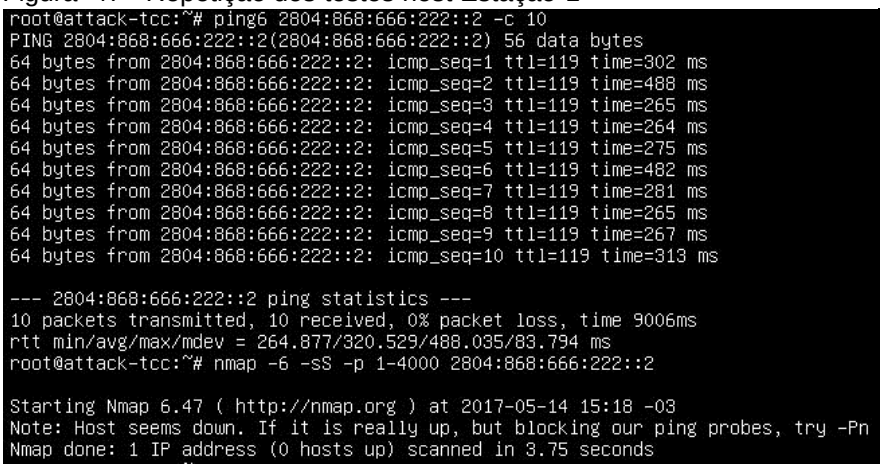
Repetição dos testes de conectividade e ataque de varredura de portas:

Figura 46 - Repetição dos testes host Gateway



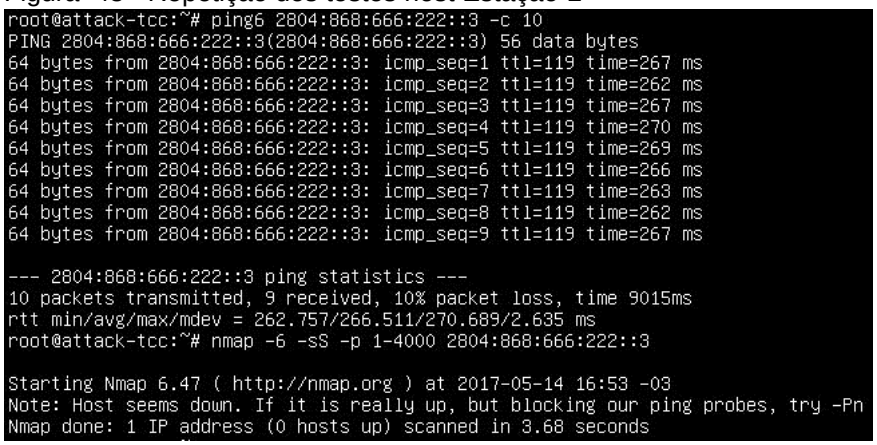
Fonte: próprio autor

Figura 47 - Repetição dos testes host Estação-1



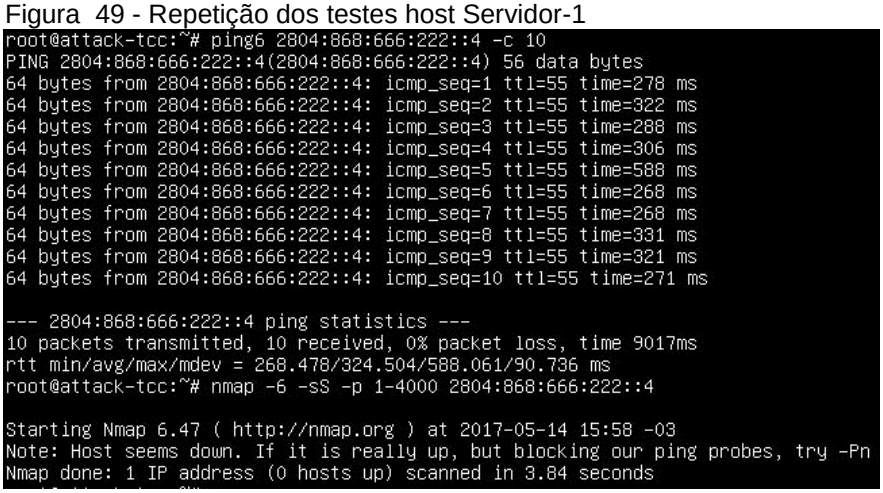
Fonte: próprio autor

Figura 48 - Repetição dos testes host Estação-2



Fonte: próprio autor

Figura 49 - Repetição dos testes host Servidor-1



Fonte: próprio autor

3.1.4 Discussão dos resultados dos testes

Durante os testes foram simuladas algumas situações onde determinado host estaria vulnerável e um ataque de força bruta poderia em alguma ocasião quebrar a senha de algum serviço remoto. Os ataques de varredura forneceram os subsídios para o ataque de força bruta nas respectivas portas conforme a Tabela 10:

Tabela 10 - Relação de portas abertas nos hosts

Host	Endereço IPv6	Portas abertas	Protocolo
Gateway	2804:868:666:333::2	22	TCP
Estação-1	2804:868:666:222::2	135, 445, 3389	TCP
Estação-2	2804:868:666:222::3	-	TCP
Servidor-1	2804:868:666:222::4	22	TCP

Fonte: próprio autor

O host Gateway possui a porta 22 (SSH) aberta para todos se conectarem e conforme o teste de força bruta demonstrou, várias tentativas de quebrar a senha do usuário “root” do serviço SSH ocorreram, porém sem sucesso. Isso não significa que o host esteja seguro, ou seja, é somente uma questão de tempo para algum indivíduo conseguir obter a senha e acessar remotamente o servidor.

O host Estação-1 possui 3 portas abertas, 135 e 445 (Windows Share) e a porta 3389 (Remote Desktop). O ataque de brutal force tentou descobrir a senha do

usuário “administrador” do serviço Re, porém não obteve sucesso. Não será considerado seguro pois novos ataques de força bruta irão ocorrer e consequentemente o vazamento das credenciais dará acesso ao atacante remotamente. Outro agravante é que as portas de *Windows Share* estão abertas e isto pode gerar uma falha na integridade do sistema, dando ao atacante acesso ao sistema de arquivos do host em caso de falha de segurança do sistema Operacional.

O host Estação-2, possui um firewall ativo nativamente em seu sistema operacional, o que garantiu um grau de proteção suficiente contra os ataques de varredura e força bruta, pois não expos nenhum serviço ao atacante. Porém, o mesmo está vulnerável a ataque de negação de serviço (DDoS) o que pode indiretamente criar uma falha de segurança no sistema operacional.

O host Servidor-1 foi alvo do ataque de varredura que expôs o serviço SSH ao atacante. Durante o teste de força bruta, o serviço estava usando uma senha fraca “*password*” conforme a Figura 47:

Figura 50 - Exposição da senha ao ataque de força bruta

Fonte próprio autor

Esta falha comprometeu a segurança do sistema operacional, garantido acesso irrestrito ao atacante. Um incidente com esse host poderia ter exposto outros dispositivos em situação parecida na rede local, o que iria amplificar o problema causando o comprometimento total dos hosts da mesma.

Após o termino dos testes foi adicionado ao host Gateway um script de *firewall stateful* afim de garantir a segurança aos hosts que estão conectados abaixo dele. Foram realizados novamente os testes e desta vez nenhum host ficou exposto aos ataques de varredura e consequentemente aos ataques de força bruta. O script utilizado utilizou o conceito de privilégio mínimo, seguindo a recomendação da RFC4890, e os dispositivos que ficaram expostos no primeiro teste, acabaram protegidos pelo firewall implantado entre o perímetro da rede local e Internet.

4 CONSIDERAÇÕES FINAIS

O IPv6 foi projetado para ser utilizado em redes públicas, ou seja, a Internet. Se a segurança do IPv6 estiver comprometida, ela pode expor o dispositivo ou a rede local a ataques originados através da Internet como demonstrado nas sessões de testes do capítulo anterior. No ambiente corporativo, é imprescindível isolar o tráfego dos dispositivos e usuários que operam nativamente em IPv6 da Internet. Conforme observado nos testes, um host comprometido pode causar danos irreparáveis a uma empresa ou organização, afetando diretamente os pilares básicos da segurança da informação:

Integridade: Um indivíduo que obtém acesso a um dispositivo IPv6 pode alterar as informações contidas no mesmo, para se beneficiar ou prejudicar terceiros e isto pode gerar danos financeiros e morais a corporação. A também a opção de fazer com que o host comprometido passe a responder como roteador da rede, sequestrando todo tráfego que atravessa por ele, esse tipo de ataque é nativo do IPv6 e consequentemente será interceptado pelo atacante. Este ataque só pode ser executado através de um host dentro da rede local e é conhecido como falsificação de roteadores e prefixo, onde um dispositivo se passa como roteador da rede.

Confidencialidade: Um dispositivo que foi explorado com certeza absoluta não possui mais dados confidenciais, pois o indivíduo que obteve acesso ao mesmo pode acessar todos os dados, inclusive senhas e arquivos criptografados.

Disponibilidade: O atacante com acesso a uma rede local IPv6 pode desferir um ataque de negação de serviço dentro da mesma, fazendo com que a rede local inteira deixe de responder. Ele pode usar o ataque de envenenamento de tabela de vizinhança, fazendo com que todos os hosts deixei deixem de responder a solicitações IPv6 e consequentemente parem de operar na rede local.

A utilização de um firewall entre o perímetro da rede local e a Internet é o mecanismo mais simples e confiável para evitar que ataques partindo da Internet acabem comprometendo os sistemas computacionais e gerando prejuízos de grande monta às empresas e organizações sendo imprescindível a utilização do mesmo em redes IPv6.

REFERÊNCIAS BIBLIOGRÁFICAS

BRITO, Samuel H. B. **IPv6 O novo protocolo da Internet.** São Paulo: Novatec, 2013.

COMER, Douglas. **Interligação de redes com TCP/IP.** 5 ed. Rio de Janeiro: Elsevier, 2006.

DAVIES, E. *et al.* **Recommendations for filtering ICMPv6 messages in firewalls RFC4890**. Disponível em: <https://www.ietf.org/rfc/rfc4890.txt> - Acessado em: 08 jan. 2017.

EQUIPE IPV6.BR. **Apostila de IPv6.** Disponível em: <ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf> - Acessado em: 05 jan. 2017.

EQUIPE IPV6.BR. **Laboratório de IPv6.** São Paulo: Novatec, 2015.

HAGEN, Silvia. **IPv6 essentials.** 2.ed. Sebastopol: O'Reilly Media, 2006.

HINDEN, R. *et al.* **IPv6 multicast address assignments RFC2375.** Disponível em <https://tools.ietf.org/html/rfc2375> - Acessado em: 12 fev 2017.

HUSTON, G. *et al*. **IPv6 Address prefix reserved for documentation RFC3849.** Disponível em <https://tools.ietf.org/html/rfc3849> - Acessado em 08 de janeiro de 2017.

MINOLI, D.; KOUNS, J. **Security in an IPv6 environment.** Boca Raton: Auerbach Publications, 2009.

ODOM, Wendell. **CCNA ICND2 Oficial de certificação do exame.** 2. ed. Rio de Janeiro: Altabooks, 2008.

RASH, Michael. **Linux firewalls**. San Francisco: No Starch Press, 2007.

TANEBAUM, Andrew S. **Redes de computadores.** 4 ed. Rio de Janeiro: Campus (Elsevier), 2003.