ARTIGO

SEGURANÇA NO PROTOCOLO IPV6: DESAFIOS E SOLUÇÕES

Edgar Yukio Ishibashi
Paulo Sérgio Pádua de Lacerda
Silvio César Bogsan

RESUMO

O IPv6 (Internet Protocol version 6) foi desenvolvido para resolver as limitações do IPv4 em termos de esgotamento de endereços públicos válidos e oferecer uma gama de melhorias técnicas. No entanto, com a adoção crescente do IPv6, novos desafios de segurança também surgiram. Dessa forma, o objetivo geral desse artigo é explorar os aspectos de segurança relacionados ao IPv6, destacando as vulnerabilidades específicas, os riscos associados e as soluções propostas para mitigar essas ameaças. Desde a autoconfiguração até as considerações de firewall e os ataques de envenenamento de cache, examinaremos as principais preocupações de segurança nesse protocolo e como as organizações podem garantir uma implementação segura do IPv6.

Palavras-chave: IPv6; Segurança de Infraestrutura; Vulnerabilidade IP; Cibersegurança; Criptografia.

ABSTRACT

IPv6 (Internet Protocol version 6) was developed to address the limitations of IPv4 in terms of exhaustion of valid public addresses and offer a range of technical improvements. However, with the increasing adoption of IPv6, new security challenges have also emerged. This article explores IPv6-related security aspects, highlighting specific vulnerabilities, associated risks, and proposed solutions to mitigate these threats. From autoconfiguration to firewall considerations and cache poisoning attacks, we'll examine the top security concerns in this protocol and how organizations can ensure a secure IPv6 implementation.

Key words: IPv6, Infrastructure Security; IP vulnerability; Cybersecurity; Cryptography.

INTRODUÇÃO

Nos últimos anos, a rápida expansão da Internet e a proliferação de dispositivos conectados, principalmente as chamadas Internet das Coisas (IoT) redefiniram fundamentalmente a forma como interagimos com o mundo digital. Nesse cenário, o Protocolo de Internet versão 6 (IPv6) emergiu como uma solução essencial para enfrentar a crescente demanda por endereçamento IP, bem como para abordar as limitações inerentes do IPv4. No entanto, junto aos benefícios trazidos pela adoção do IPv6, surgiram também desafios significativos de segurança cibernética, à medida em que as redes se tornaram mais complexas e os cibercriminosos mais sofisticados.

Sendo assim, o objetivo geral deste artigo é explorar o cenário atual da segurança do protocolo IPv6, investigando os desafios únicos que surgem com sua implementação generalizada. Enquanto o IPv6 trouxe melhorias na segurança em relação ao seu antecessor, o IPv4 também introduziu novos vetores de ataque e vulnerabilidades que requerem uma análise aprofundada. A complexidade inerente aos cabeçalhos expandidos do IPv6, a autoconfiguração de endereços e os mecanismos de mobilidade acrescentam camadas adicionais de desafios de segurança. Diante do exposto, faz-se a seguinte pergunta: A implantação do protocolo IPv6 trará mais vulnerabilidades do que seu antecessor IPv4?

Ao longo deste artigo examinaremos as principais áreas de preocupação como a mitigação de ataques de negação de serviço (DDoS) em redes IPv6, as considerações de privacidade ao lidar com endereços globais persistentes e as estratégias para proteger a autoconfiguração de endereços, questões sobre o escaneamento da rede e o envenenamento de cache. Além disso, exploraremos as soluções e práticas recomendadas que estão sendo desenvolvidas para abordar esses desafios, incluindo firewalls de próxima geração, sistemas de detecção e prevenção de intrusões adaptados ao IPv6 e abordagens de educação e conscientização para os usuários finais. Para tanto foi feita uma pesquisa a respeito das tecnologias atuais que tentam mitigar as vulnerabilidades do protocolo IPv6.

À medida que avançamos em direção a um mundo em que a conectividade é onipresente, compreender as complexidades da segurança do IPv6 é fundamental para

ISSN 2965-5285

garantir a integridade, confidencialidade e disponibilidade das informações transmitidas por meio dessa infraestrutura vital.

HISTÓRICO

No início dos anos 1990, com o crescimento exponencial da Internet como plataforma de informação, comércio e entretenimento já era de conhecimento da comunidade científica que a versão 4 do protocolo IP (IPv4) não seria suficiente para suprir as demandas que estavam despontando. Técnicas como *Classless Interdomain Routing* (CIDR[1]) e *Network Address Translate* (NAT[2]) ou Tradução de Endereços de Rede foram formas paliativas de contornar o problema de escassez de endereçamento público, traziam uma falsa sensação de segurança por "ocultar" os endereços IP internos (Endereços Privados), mas não eram eficientes para aplicações que demandavam aplicações em tempo real como VoIP (Voz sobre IP).

Então, em dezembro de 1993, a IETF formalizou, por meio de uma *Request for Comments* (RFC 1550), pesquisas que desenvolvessem propostas para um novo protocolo, que melhorasse as questões de escalabilidade, segurança, suporte a qualidade de transmissão de voz, mobilidade e políticas de transição.

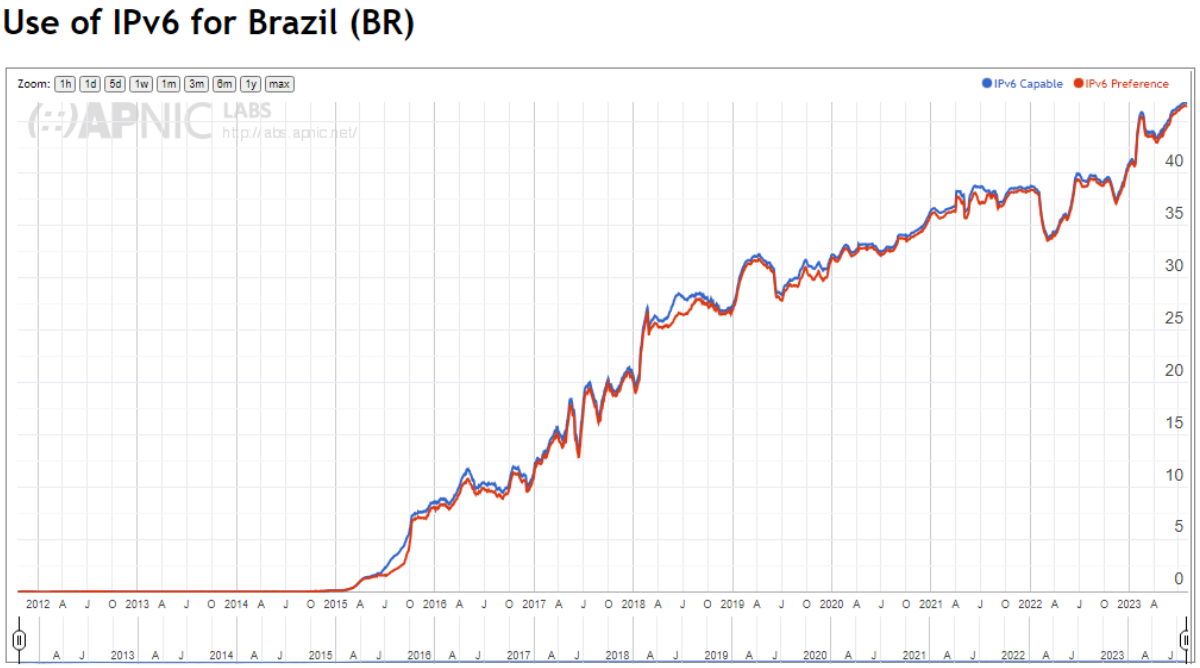
Finalmente em 1995 por meio da RFC 1752 foram apresentadas propostas que culminaram na versão 6 do protocolo IP o IPv6.

Atualmente a implantação do protocolo IPv6 no Brasil está em franco crescimento, em torno de 40% (Figura 1) o que denota a preocupação em segurança.

[1] Classless Inter-domain Routing (CIDR) definido pela RFC 4632 é uma forma de subdivisão dos endereços IP em blocos menores, visandoa uma melhor distribuição, de modo a evitar o desperdício de endereços IP.
[2] Network Address Translation (NAT) definido pela RFC 3022 é uma técnica paliativa que permite, a partir de um único endereço IP público válido, conectar vários dispositivos à Internet pela rede local

ISSN 2965-5285

Figura 1: Porcentagem de utilização de IPv6 no Brasil medida pelo APNIC

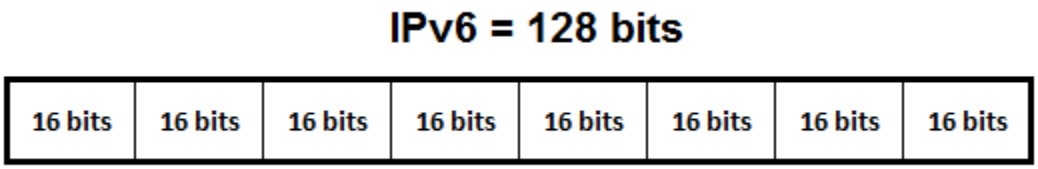


Fonte: ipv6.br, 2023.

AS DIFERENÇAS DO PROTOCOLO IPV6

O endereço IPv6 tem 8 campos de 16 bits, portanto é um endereço de 128 bits.

Figura 2: Representação do endereço IPv6



Fonte: elaborado pelos autores

Cada campo é representado por um número hexadecimal (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F) e separado por dois pontos ":"

2001:DB8:CACA:FACE:1111:2222:3333:4444/64

ISSN 2965-5285

Todos os zeros podem ser resumidos pela notação **::**

2001:DB8:CACA:FACE:0000:0000:0000:0000/64

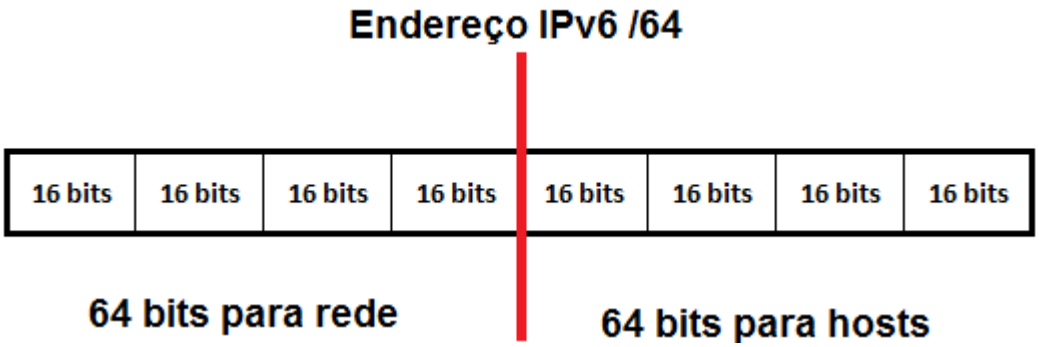
OU

2001:DB8:CACA:FACE::/64

A máscara de sub-rede é representada na forma blocos /64, /56 /48 etc,; os primeiros bits representam o endereço de Rede e os demais à direita representam os hosts, igual ao IPv4.

Isso significa que, para uma rede IPv6 /64 há 64 bits reservados para hosts o que dá 2^64 hosts nesta rede, ou 18.446.744.073.709.551.616.

Figura 3: Bits representando a rede e Bits representando os hosts.



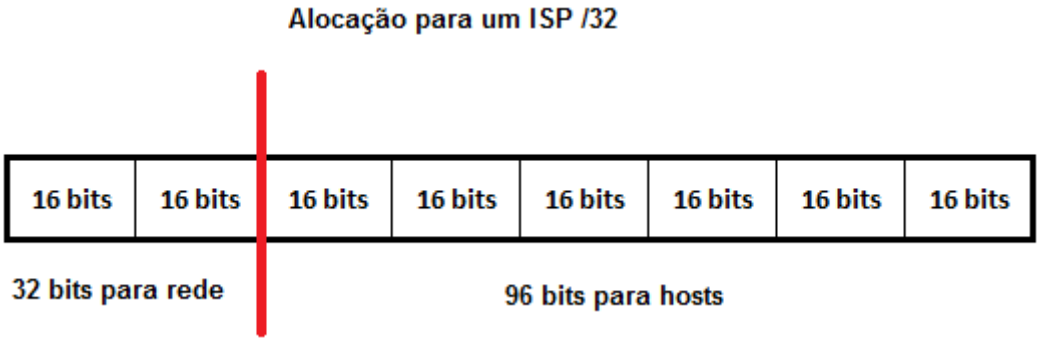
Fonte: elaborado pelos autores

Segundo a orientação do IETF, por meio da RFC 3177, é essa rede que o usuário final receberá em sua residência. Seria muito positivo receber 18 quintilhões de IPs válidos em ambiente doméstico, se comparados com 1 IP válido atualmente recebido.

ISSN 2965-5285

Para o provedor, a alocação mínima é um bloco /32.

Figura 4: Bits representando a rede recebida por um Provedor de Internet (ISP)

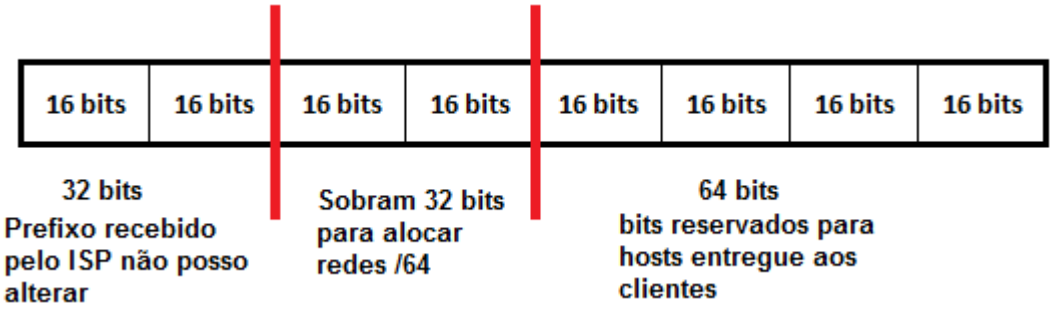


Fonte: elaborado pelos autores

Em princípio, o provedor teria 2^96 endereços IP para usar nesta rede, mas isso seria infinitamente inimaginável e não poderia alocar esses endereços IP para seus clientes, pois todos ficariam na mesma rede. Como a orientação da RFC 3177, recomenda-se entregar redes /64 para os usuários finais.

Significa que esse ISP *(Internet Solution Provider)* tem 32 bits no meio, para alocar redes /64. Em suma esse ISP tem 2^32 ou 4.294.967.296 redes de blocos /64.

Figura 5: Representação dos bits alocados para entrega de redes /64

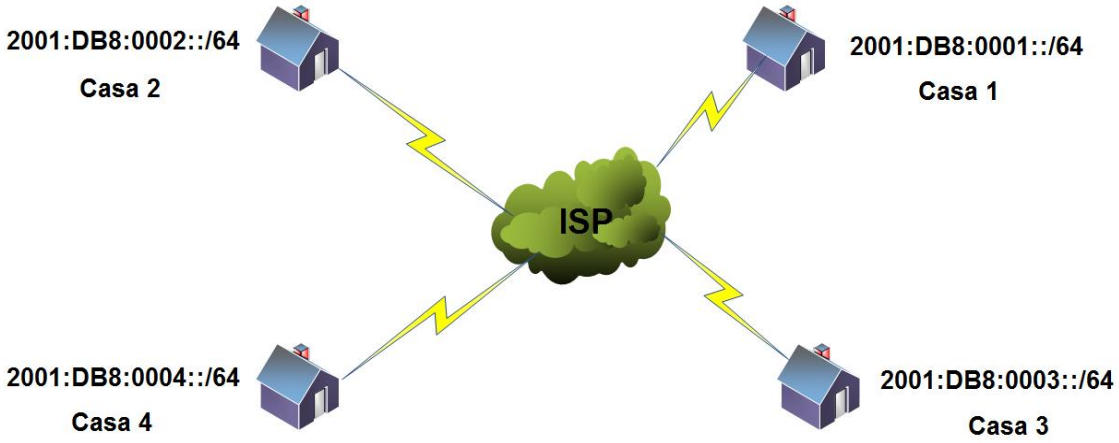


Fonte: elaborado pelos autores

Portanto a alocação de uma rede 2001:DB8::/32 em blocos /64 ficaria de acordo como representa a Figura 6.

ISSN 2965-5285

Figura 6: Exemplo de alocação de redes /64 para usuário final



2001:DB8:0000:0001:0000:0000:0000:0000 até 2001:DB8:0000:0001:FFFF:FFFF:FFFF:FFFF para casa 1

2001:DB8:0000:0002:0000:0000:0000:0000 até 2001:DB8:0000:0002:FFFF:FFFF:FFFF:FFFF para casa 2

2001:DB8:0000:0003:0000:0000:0000:0000 até 2001:DB8:0000:0003:FFFF:FFFF:FFFF:FFFF para casa 3

2001:DB8:0000:0004:0000:0000:0000:0000 até 2001:DB8:0000:0004:FFFF:FFFF:FFFF:FFFF para casa 4

É possível notar que a parte em vermelho representa a rede e em preto o intervalo de hosts em cada rede.

Outra grande diferença do protocolo IPv6 em relação ao anterior IPv4 é o formato do cabeçalho principal, passou de 20 a 60 bytes no IPv4 para 40 bytes no IPv6, além disso tornou-se mais flexível e eficiente com a inclusão de cabeçalhos de extensão.

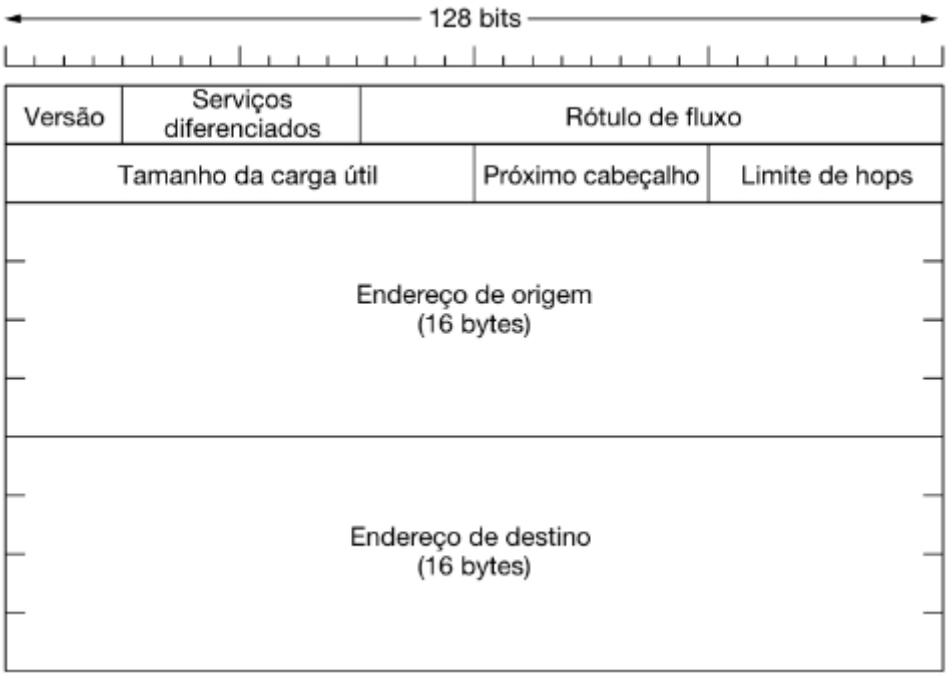
Segundo Tanembaum (2021):

> O campo Versão é sempre 6 para o IPv6 (e 4 para o IPv4). Durante o período de transição do IPv4, que já passou de uma década, os roteadores serão capazes de examinar esse campo para identificar o tipo de pacote que eles tem. A propósito, a realização desse teste desperdiça algumas instruções no caminho crítico, visto que o cabeçalho do enlace de dados normalmente indica o protocolo de rede para demultiplexação e portanto, alguns roteadores podem pular a verificação.

Portanto a otimização do cabeçalho IPv6 traz implementações que ajudarão o processo de roteamento e encaminhamento dos pacotes dentro da rede.

ISSN 2965-5285

Figura 7: Identificação dos campos principais do cabeçalho IPv6



Fonte: Tanenbaum, In: Redes de computadores, p. 298.

VULNERABILIDADES E DESAFIOS

Autoconfiguração e endereçamento dinâmico: Com a exponencial oferta de endereços IP, o serviço de entrega dinâmica de IP (DHCP) no IPv6 torna-se obsoleto e a autoconfiguração passa a ser uma técnica adotada, enquanto simplifica a atribuição de endereços, pode resultar em endereços imprevisíveis e dificultar o rastreamento. Isso pode ser explorado por invasores para evitar a detecção.

Envenenamento de cache: O ataque de envenenamento de cache IPv6 pode levar a redirecionamento de tráfego e manipulação de pacotes. O Protocolo Neighbor Discovery (NDP) usado no IPv6 é suscetível a esse tipo de ataque.

Ataques DoS amplificados: Assim como no IPv4, os ataques de negação de serviço (DoS) podem ser amplificados no IPv6 devido à falta de filtragem de pacotes e configurações incorretas de firewall.

ISSN 2965-5285

Escaneamento de rede: Com o espaço de endereçamento expandido do IPv6, o escaneamento de rede se torna mais desafiador. No entanto, ferramentas e técnicas específicas podem ser usadas para descobrir dispositivos vulneráveis.

SOLUÇÕES E MELHORES PRÁTICAS

Configuração segura: Implementar configurações seguras, como filtragem de pacotes e políticas de firewall adequadas, é essencial para mitigar riscos. Utilizar o NDP *(Neighbor Discovery Protocol) Secure*, que restringe a autoconfiguração não autorizada, é uma abordagem recomendada.

Monitoramento constante: Manter uma vigilância constante sobre a rede para detectar atividades suspeitas e anomalias é crucial. Em vários roteadores de firewalls de última geração existe à disposição ferramentas de monitoramento e detecção de intrusões chamados *Intrusion Detection System (IDS) e Intrusion Prevention System (IPS).* São tecnologias que monitoram o tráfego da rede comparando eventos e anomalias tomando medidas específicas de proteção, como negar o acesso ou registrar o evento.

Filtragem de Pacotes IPv6: Configurar regras de filtragem de pacotes em roteadores e firewalls para permitir apenas o tráfego IPv6 legítimo e bloquear pacotes malformados ou indesejados continua sendo uma prática essencial de segurança da rede.

Segmentação de rede: Dividir a rede em segmentos menores e aplicar políticas de controle de acesso ajuda a limitar o impacto de um eventual ataque.
Gerenciamento de Endereços: Adoção de práticas de gerenciamento de endereços IPv6, como gerar endereços usando algoritmos aleatórios ou temporários, para evitar rastreamento e melhorar a privacidade.

Proteção contra Ataques de Amplificação: Configurar filtros e limites de taxa para proteger contra ataques de amplificação que exploram recursos, como ICMPv6, para inundar redes com tráfego malicioso.

ISSN 2965-5285

Atualizações e Patches Regulares: Manter todos os dispositivos e sistemas atualizados com as últimas correções de segurança para evitar vulnerabilidades conhecidas.

Testes de Segurança e Avaliações de Vulnerabilidade: Realizar testes de penetração e avaliações regulares de vulnerabilidade para identificar falhas de segurança e tomar medidas corretivas proativas.

Controle de Acesso Baseado em Função (RBAC): Implementar *Role-Based Access Control* para restringir o acesso de usuários e dispositivos aos recursos de rede, reduzindo o risco de exposição a ameaças.

Assinatura e Criptografia de Tráfego: Utilizar protocolos de criptografia, como IPsec, para proteger a confidencialidade e autenticidade das comunicações IPv6.

Essas implementações abordam diversos aspectos de segurança, desde o controle de acesso, até a proteção contra ataques específicos; são fundamentais para garantir que a adoção do IPv6 ocorra de maneira segura e confiável.

CONCLUSÃO

O IPv6 trouxe inovações técnicas significativas para a Internet, mas também introduziu desafios de segurança distintos em comparação com o IPv4. A implementação segura do IPv6 exige uma compreensão aprofundada das vulnerabilidades específicas e das melhores práticas para mitigar riscos. Ao adotar abordagens de segurança proativas, como configurações adequadas, monitoramento constante e atualizações regulares, as organizações podem aproveitar os benefícios do IPv6 sem comprometer a integridade e a segurança de suas redes.

Por este motivo o objetivo geral desta pesquisa foi explorar o cenário atual da segurança do protocolo IPv6, investigando os desafios únicos que surgem com sua implementação generalizada

Os resultados mostraram que a segurança do protocolo IPv6 representa um campo de estudo e implementação de extrema importância à medida que o mundo se aprofunda na era da conectividade global e do aumento exponencial de dispositivos interconectados.

ISSN 2965-5285

A transição para o IPv6 trouxe consigo uma série de vantagens em termos de escalabilidade e endereçamento, mas também desafios significativos em relação à segurança cibernética. Neste artigo, exploramos os diversos aspectos de segurança que acompanham a adoção do IPv6.

Ficou evidente que, enquanto o IPv6 integra melhorias de segurança em comparação com o seu antecessor, ele também traz à tona vulnerabilidades específicas e vetores de ataque que necessitam de atenção cuidadosa. A complexidade dos cabeçalhos ampliados, juntamente com as características únicas do IPv6, como autoconfiguração de endereços e mobilidade, desafia os profissionais de segurança cibernética a se manterem atualizados e a adotarem abordagens inovadoras para proteger as redes.

À medida que o cenário de ameaças continua a evoluir, a colaboração entre a comunidade de segurança, fabricantes de equipamentos, provedores de serviços e usuários finais se torna essencial. É crucial desenvolver e implementar soluções adaptadas às nuances do IPv6, como sistemas de detecção e prevenção de intrusões aprimorados, estratégias robustas de gerenciamento de endereços e educação contínua sobre boas práticas de segurança.

A segurança cibernética nunca é um objetivo estático, mas sim um processo contínuo de avaliação, adaptação e aprimoramento. Ao reconhecer os desafios e as oportunidades apresentados pelo IPv6, podemos efetivamente mitigar riscos, proteger informações sensíveis e garantir a continuidade das operações em um mundo conectado. Compreender e abordar os aspectos de segurança do IPv6 não é apenas uma medida preventiva, mas um investimento na construção de um ambiente digital seguro e resiliente para as gerações futuras.

REFERÊNCIAS

Forouzan, Behrouz A.Protocolo TCP/IP [recurso eletrônico] / Behrouz A. Forouzan, Sophia Chung Fegan ; revisão técnica Flávio Soares Corrêada Silva, Roberto Hirata Jr ; tradução João EduardoNóbrega Tortello. -- São Paulo : McGraw-Hill, 2008

Tanenbaum, Andrew. Redes de Computadores [recurso eletrônico] / Andrew Tanenbaum, Nick Feamster, David Wetherall; 6º edição, Porto Alegre: Bookman, 2021.

Conceitos de IDS/IPS segundo a Juniper Networks acessado através da URL: https://www.juniper.net/br/pt/research-topics/what-is-ids-ips.html em 04/08/2023.

Filtragem de pacotes IPv6 em roteadores da Cisco acessado através da URL: https://www.cisco.com/c/pt_br/support/docs/ip/ip-version-6-ipv6/113489-ipv6-pfl-new-00.html em 04/08/2023.

Definição de Controle de Acesso Baseado em Função (RBAC) acessado através da URL: https://www.redhat.com/pt-br/topics/containers/what-kubernetes-role-based-access-control-rbac em 04/08/2023.

ipv6.br Conceitos sobre IPv6 do Núcleo de Informação e Coordenação do Ponto BR - NIC.br

ISSN 2965-5285