Methodology for the security analysis of IPv4-as-a-Service IPv6 transition technologies

Ameen Al-Azzawi and Gábor Lencse

Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Műegyetem rkp. 3, Budapest, 1111, Hungary
Email: alazzawi@hit.bme.hu, lencse@hit.bme.hu

As the depletion of IPv4 addresses accelerates, the urgency of transitioning to IPv6 has intensified. To address this imperative, numerous IPv6 transition technologies have emerged to facilitate this migration process. While existing methodologies offer insights into the security implications of these technologies, this paper presents a novel approach to security analysis that surpasses conventional methods. By leveraging the STRIDE threat modeling technique, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, we conduct a comprehensive security analysis of prominent IPv6 transition technologies, including Combination of Stateful and Stateless Translation (464XLAT), Dual-Stack Lite (DS-Lite), Lightweight 4over6 (Lw4o6), and Mapping of Address and Port using Translation (MAP-T) / Mapping of Address and Port with Encapsulation (MAP-E). Our methodology not only evaluates the categorization of transition technologies but also considers the location and the statefulness of the attacked router, whether it's a Customer Edge (CE) router or a Provider Edge (PE) device. Additionally, we introduce an abstraction method to derive potential vulnerabilities at a more general level from those discovered at a more specific level. Through synthesizing previous research endeavors and rigorously examining these technologies for vulnerabilities, our approach offers valuable insights into the security landscape of IPv4-as-a-Service (IPv4aaS) IPv6 transition technologies. By addressing the limitations of existing methodologies and providing a more holistic framework for security analysis, this paper contributes to the ongoing discourse on IPv6 transition strategies. It enhances the resilience of network infrastructures against evolving security threats.

Keywords: STRIDE; IPv6 transition; MAP-T; DS-Lite; IPv4aaS; Translation; MAP-E; Lw4o6; Spoofing; 464XLAT

Received 23 July 2024; revised 04 February 2025

1. INTRODUCTION

IPv6 was introduced in 1998 to address the growing shortage of IPv4 addresses [33]. As the digital ecosystem expanded, the limitations of IPv4 address became increasingly apparent, making the transition to IPv6 address essential. However, this transition introduces new security challenges, particularly with IPv4aaS technologies that enable IPv4 connectivity over IPv6 networks. Our paper addresses these challenges by proposing a novel methodology for analyzing the security of five prominent IPv4aaS technologies. As the digital ecosystem continues to expand at an unprecedented pace, the limitations imposed by the dwindling IPv4 address space have become increasingly apparent. This scarcity not only hampers the growth of networked devices but also

complicates the management of existing infrastructures.

In response to these challenges, a transition to the IPv6 protocol was a necessity. As a result, several IPv6 transition technologies have emerged, each offering unique approaches to facilitate the migration from IPv4 to IPv6. These technologies aim to bridge the compatibility gap between the two protocols, enabling seamless communication between IPv6-only clients and legacy IPv4 servers.

However, while these transition mechanisms have been in place for over a decade and continue to demonstrate significant potential in facilitating the ongoing transition to IPv6, they are not without their own set of security concerns. The inherent complexities of transitioning between protocols introduce potential vulnerabilities that malicious actors may exploit. Some commonly used IPv6 transition mechanisms include Dual-Stack, Tunneling, and Translation techniques. Tunneling technique is mainly based on encapsulation, which is a fundamental technique in networking, where a data packet (e.g., an IPv4 packet) is enclosed within another packet (e.g., an IPv6 packet) to enable transmission across networks that use different protocols. In the context of IPv6 address transition technologies, encapsulation plays a critical role in transporting IPv4 address traffic over IPv6 networks, ensuring compatibility during the transition phase.

Dual-Stack allows both IPv4 and IPv6 protocols to coexist on the same network infrastructure, providing a seamless transition path for organizations. It involves configuring networking devices, hosts, and applications to support both IPv4 and IPv6 simultaneously [31].

From the more than three dozen IPv6 transition technologies listed in [24], the "IPv6 Operations" working group of the Internet Engineering Task Force (IETF) focuses on the five most prominent IPv4aaS IPv6 transition technologies that we listed in the abstract. IPv4aaS refers to various technologies and services that allow IPv4 connectivity to be delivered over IPv6 networks, facilitating the transition by enabling continued access to IPv4 resources. RFC 8585 [32] lists 464XLAT [30], DS-Lite [12], Lw4o6 [11], MAP-T [28], and MAP-E [35] to be supported by IPv6 customer edge routers. Their advantages and drawbacks are analyzed in RFC 9313 [26]. At the current stage of transitioning the Internet from IPv4 to IPv6, several Internet Service Providers (ISPs) decided that they do not want to maintain dual-stack networks, rather they want to use only IPv6 in the access and core networks. However, they still need to provide IPv4 Internet access to their customers. To that end, they used one of the previously mentioned five IPv4aaS technologies. For this reason, we also focused on the security analysis of the five most prominent IPv4aaS IPv6 transition technologies.

The central problem addressed in this paper is the inadequacy of existing security analysis methodologies for IPv4aaS IPv6 transition technologies. While the existing methodologies offer some insights into the security implications of these technologies, they often fall short of providing a comprehensive and practical framework for evaluating security risks.

In this context, [23] presents a comprehensive approach to address the challenges posed by the IPv6 transition. The methodology outlined in [23] operates at multiple levels, encompassing the overarching transition categories such as single or double translation (applying two routers: the first one translates IPv4 into IPv6, and the second one translates IPv6 into IPv4 or vice versa), the individual IPv6 transition technologies, and their practical implementations. This structured approach forms the foundation upon which our subsequent analysis is built.

This paper presents a novel approach that leverages the STRIDE threat modeling technique in conjunction with the methodology proposed in [23] to conduct a comprehensive security analysis of five prominent IPv4aaS technologies. Our proposed alternative methodology is inspired by our prior experience in the security analysis of IPv6 transition technologies as detailed in [2], [3], [4], and [5]. This revised approach, elucidated in detail in the subsequent sections, offers notable advantages over existing methodologies and serves as a guiding framework for the remainder of this paper. Additionally, we introduce a formal method for abstraction in Subsection 5.1 to derive potential vulnerabilities at a more general level from those discovered at a more specific level. We recognize that many IPv6 transition technologies have been proposed over time; however, the landscape has shifted. Earlier methods like 6to4, Teredo, and 6rd have become largely obsolete or see limited adoption today due to security issues and reduced usage. Our focus is on IPv4aaS technologies, such as DS-Lite, MAP-T, MAP-E, and 464XLAT, which are better suited to handle IPv4 address exhaustion and support IPv6 address adoption. These are expected to be widely used in the coming years, ensuring that our methodology addresses the most relevant security concerns in real-world scenarios.

The contributions of this paper are threefold. First, we provide a comprehensive security analysis of five prominent IPv4aaS technologies, identifying common vulnerabilities and their implications. Second, we propose a practical framework for evaluating

the security of IPv6 transition technologies, offering actionable insights for network administrators and security professionals. Finally, we demonstrate the effectiveness of our approach through a detailed attack-and-mitigation scenario, highlighting its relevance in practical scenarios.

The remainder of the paper is structured as follows: in Section 2, we explain the operations of the five IPv4aaS technologies. Section 3 provides an overview of the related work conducted in similar domains. Section 4 introduces the novel methodology proposed for conducting our research, delineating its key components and rationale. In Section 5, we present a synthesis of our findings, accompanied by a comprehensive analysis of the data gathered through our research endeavors. In Section 6, we detail the technical specifications of our test-bed and illustrate its practical application through an attack-and-mitigation scenario on one of the IPv6 translation technologies. Following this, Section 7 provides a detailed discussion of our findings, elucidating any patterns or common vulnerabilities observed across various IPv6 transition technologies. We draw upon our previous research to contextualize these findings within the broader scope of our work. Finally, Section 8 offers a concise summary of the paper's main contributions, highlighting its novelty and key insights gained. Additionally, we reflect on the lessons learned throughout our investigation.

2. HIGH-LEVEL OPERATION OF THE FIVE IPV4AAS TECHNOLOGIES

2.1. 464XLAT

As shown in Fig. 1, 464XLAT is categorized as a double-translation mechanism as it deploys two Network Address Translation (NAT) edges: Customer-side translator (CLAT) and Provider-side translator (PLAT). The CLAT performs a stateless NAT46 operation on the IPv4 packet, translates it into an IPv6 packet, and forwards it to the PLAT. The PLAT (known as a stateful NAT64 translator) performs a Network Address and Port Translation (NAPT) on the IPv6 packet, translates it back to an IPv4 packet, and forwards it to the IPv4 server. The reverse translation uses the information stored in the connection tracking table of the PLAT to filter packets and forward them accordingly. The PLAT saves all of the active sessions that are being processed in its connection tracking table, which includes IP addresses, port numbers, etc.

In a NAT64 environment, IPv6 devices communicate with IPv4 servers by mapping IPv6 addresses to IPv4 addresses. NAT64 uses an N:1 mapping system, where multiple IPv6 addresses can share a single IPv4 address. To understand the difference between stateful and stateless systems, consider the following analogies.

Stateful systems are like a receptionist who tracks visitors' entries and exits, maintaining a record of past interactions for future reference.

Stateless systems, on the other hand, are like a turnstile that grants access based on a valid pass but does not retain any information about previous entries or exits.

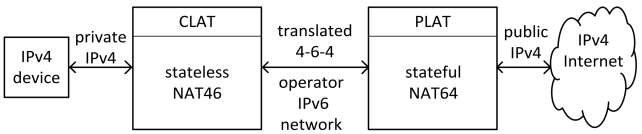

FIGURE 1. Overview of the 464XLAT architecture [26]

2.2. DS-Lite

As shown in Fig. 2, DS-Lite is characterized as an encapsulation-based technology: it employs a tunnel between its two primary routers, namely the Basic Bridging BroadBand (B4) and the Address Family Transition Router (AFTR) [12]. B4 is a router at the customer side that encapsulates an IPv4 packet into an IPv6 packet and sends it over to the AFTR, which does the reverse by decapsulating the packet, exacting the IPv4 packet out of it. Then (with some simplification), it performs stateful NAT44 on the IPv4 packet and forwards it to the IPv4 server. Similarly to the PLAT, the AFTR stores its active sessions' details in its connection tracking table.

It should be noted that both Fig. 2 and the above description contain a simplification. The connection tracking table of the AFTR also includes the IPv6 address of the B4 to be able to distinguish the packets of different users even if they use the very same private IPv4 address as the source address.

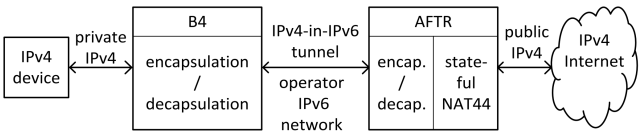

FIGURE 2. Overview of the DS-Lite architecture [26]

2.3. Lw4o6

As shown in Fig. 3, Lw4o6 is an encapsulation-based technology. It operates through two primary routers,

lwB4 and lwAFTR, and is considered to be an enhanced version of the DS-Lite technology because it tackles the DS-Lite scalability issue by removing the central NAT44 translation from the provider side and placing it in the customer-side router (lwB4). By doing so, the lwAFTR can scale better than the AFTR. Lw4o6 shares public IPv4 addresses among multiple subscribers by assigning a unique set of source port numbers to each subscriber (lwB4). As a result, the lwB4 performs a stateful NAT44 translation on the IPv4 packet of the subscriber in a way that its private IPv4 address is replaced by the public IPv4 address assigned to the subscriber, and the source port number is transformed into the range assigned to the subscriber. Then, it encapsulates the IPv4 packet into an IPv6 packet and forwards it over to the lwAFTR. The lwAFTR can distinguish the subscriber based on several parameters, such as the public IPv4 address and source port number of the incoming packets. Furthermore, the lwAFTR decapsulates the packet and forwards it to the IPv4 server. Therefore, the lwAFTR functions in a stateless manner [11].

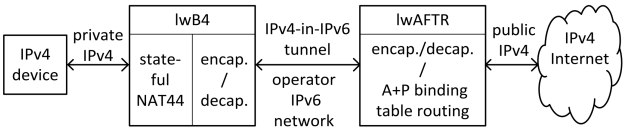

FIGURE 3. Overview of the Lw4o6 architecture [26]

2.4. MAP-E

MAP-E has some similarities to the Lw4o6 as it is an encapsulation-based technology. As shown in Fig. 4, MAP-E comprises two primary routers: CE and Border Relay (BR). The CE performs a stateful NAT44 on the IPv4 packet, converting the source IPv4 address and source port number to the assigned public IPv4 address and source port (out of the assigned ports range for the CE), encapsulates the IPv4 address packet into an IPv6 address packet and forwards it to the BR.

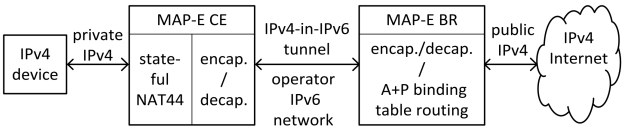

FIGURE 4. Overview of the MAP-E architecture [26]

The BR then decapsulates the IPv4 packet from the IPv6 packet and forwards it to the IPv4 Internet. Therefore, the MAP-E is considered to be stateless on the provider side.

2.5. MAP-T

MAP-T is under the umbrella of Mapping of Address and Port (MAP) technologies, where MAP-E lies. However, MAP-T is a translation-based technology. As illustrated in Fig. 5, MAP-T employs a double translation mechanism, where the CE router performs stateful NAT44 translation on the IPv4 packet having a private IPv4 source address, which results in an IPv4 packet having a public IPv4 source address and with source port number within the assigned range of ports for the CE. Next, the CE router performs a stateless NAT46 translation to convert the IPv4 packet into an IPv6 packet and forwards the resulting packet to the BR. Finally, the BR router performs stateless NAT64 on the packet and forwards the resulting IPv4 packet to the IPv4 Internet.

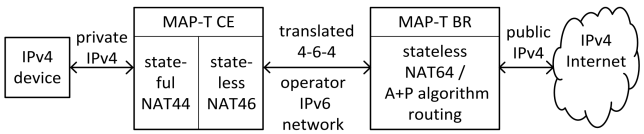

FIGURE 5. Overview of the MAP-T architecture [26]

3. LITERATURE REVIEW

3.1. General Methods

In Georgescu's 2016 study [18], the STRIDE methodology was employed to assess security vulnerabilities in IPv6 transition technologies. Within this research, a categorization scheme was devised to classify the multitude of IPv6 transition technologies into broader classifications, namely dual-stack, single translation, double translation, and encapsulation technologies. This systematic categorization facilitated a thorough examination of potential threats across various IPv6 transition technologies through the analysis of pertinent elements within Data-Flow Diagrams (DFDs) representing the aforementioned categories. The investigation focused particularly on aligning the identified threats with the corresponding threat categories delineated by the STRIDE model.

Subsequent to Georgescu's methodological framework as documented in [18], Lencse [23] proposed an extension, refining the analytical approach to encompass two discrete tiers of investigation. Firstly, attention is directed towards the individual IPv6 transition tech-

nologies, delineating them based on their distinct methods of facilitating the transition process, such as tunneling, translation, or dual-stack configurations. Secondly, a supplementary layer of analysis pertains to the implementation methodologies adopted by each technology, distinguishing between open-source and proprietary software solutions. This dual-tiered methodology thus facilitates a more refined examination, encompassing both the overarching characteristics of transition technologies and the specific nuances of their practical implementations.

However, Georgescu's [18] and Lencse's [23] approaches, which categorize IPv6 transitions based on core network traversal (dual-stack, single translation, double translation, encapsulation), have shown limitations in effectively capturing the diverse security vulnerabilities inherent in specific transition technologies. For instance, despite belonging to the same category of double translation, technologies such as 464XLAT and MAP-T exhibit markedly different vulnerabilities. Similarly, within the category of encapsulation, DS-Lite and Lw4o6 demonstrate distinct security risks. This discrepancy highlights the limitations of broad categorization methods in effectively addressing the complex security challenges associated with IPv6 transition technologies.

3.2. Security Issues of 464XLAT

Since 464XLAT is based on NAT46 and NAT64 translators, research by Hyunwook Hong [20] has focused on the IPv6 security issues as far as cellular networks are concerned, and it came up with different categories of possible attacks. The authors demonstrated three different Denial of Service (DoS) attacks on NAT64 block targeting features that only exist in IPv6 cellular networks: NAT overflow attack, NAT wiping attack, and NAT Bricking attack.

Before explaining those three attacks in detail, it is important to mention that an external IPv4 address refers to the public IP address used for communication outside the local network. In IPv4 mobile networks, each device typically uses a private IPv4 address assigned via NAT, which allows a maximum of 65,535 external mappings due to the limitation of the 16-bit port number space. However, in IPv6 cellular networks, a device can utilize a vast number of IPv6 addresses (2^{64} in practice).

NAT overflow attack: if a device creates mappings on NAT64 using all its potential 2^{64} IPv6 addresses, it results in $65{,}535 \times 2^{64}$ mappings. This massive number of mappings can potentially overload the NAT64 gateway, leading to service disruption. This occurs because the NAT64 gateway may become overwhelmed by the excessive number of mapping requests, which exceeds its capacity to manage the translations.

NAT wiping attack: this attack targets the mapping entries within NAT64. Since NAT64 uses N:1 mapping, attacking the external IPv4 address of the NAT64 gateway can affect multiple hosts sharing the same external IPv4 address. An adversary sends malicious Transmission Control Protocol (TCP) packets with the RST flag to wipe out the target mappings, causing a DoS attack for those users. To execute this attack, the attacker must know the TCP 4-tuple of the targeted service (Destination IP address, port number, External IP address of NAT64, and External port number of NAT64) [20].

NAT Bricking attack: this DoS attack exploits the N:1 mapping algorithm of NAT64. The adversary sends a large number of requests using the external IPv4 addresses of the NAT64 gateway. Although large vendors, like Google, have IP blocking mechanisms for excessive requests, the attack can still cause significant disruption. In an experiment targeting Google Scholar, the adversary triggered Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) request by changing the source IP address repeatedly, ultimately triggering CAPTCHA requests for 631 external IPv4 addresses, including one of the victim's addresses [20].

As for building a test-bed for 464XLAT topology, several attempts were conducted by researchers to build an efficient test-bed to test the 464XLAT transition technology, its weak spots, and vulnerabilities. A successful test-bed was built by Marius Georgescu [17], in which he measured the latency, throughput, and packet loss by adopting 464XLAT transition technology and some other methods as well.

On a personal level, we published research work regarding the security analysis of 464XLAT technology by applying the STRIDE method and building a test-bed using Debian-based virtual machines. We applied several attacking scenarios against the NAT64 and NAT46 translators, where we found that 464XLAT infrastructure is susceptible to several attacks such as DoS and source port exhaustion [2].

3.3. Dual-Stack Lite

A limited amount of experiments have been published regarding DS-lite and its security analysis. A survey of the most prominent IPv6 transition technologies and their security analysis was carried out in [24], where DS-

Lite was mentioned, and its security analysis has been classified as important but replaceable due to several issues mentioned by [22], such as the following:

- The need for two separate physical interfaces at the AFTR;
- The need for high scalability at the AFTR side due to the fact that many B4 routers may be connected to the same AFTR [22];
- The location of deploying AFTR router within the Internet Service Provider (ISP) network and the trade-off it creates between the high operation cost and installing an extremely powerful AFTR [22]. The trade-off can be explained by dividing the issue at hand into two options:
  - Deploying AFTR at the edge of the network to cover a small area serves few B4s and requires less-powerful AFTR;
  - Deploying AFTR at the core of the network to cover a big area covers more B4s and requires extremely powerful AFTR (or even more than one AFTR);
- The complexity of deploying a proxy Domain Name System (DNS) resolver, which will proxy every DNS query stemming from all IPv4 clients heading towards a DNS server that resides in an IPv6 network [22].

Another study [15] conducted a security analysis of DS-Lite's Management Information Base (MIB), which is a module that can be used for configuration and monitoring of AFTR in a Dual-Stack Lite scenario. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). The analysis identified several vulnerable MIB objects:

- Notification threshold objects: an attacker can manipulate these thresholds to either flood the system with useless alarms by setting them too low or disable effective monitoring by setting them too high:
  - Dslite-AFTR-Alarm-Connect-Number: triggers an alarm when the number of current DS-Lite tunnels reaches the threshold, requiring a separate tunnel for each B4 router.
  - Dslite-AFTR-Alarm-SessionNumber: sends an alarm when the number of sessions per IPv4 user reaches the threshold, in accordance with RFC-6333 [12], which requires logging of softwire-ID, IP, ports, and protocol.
  - Dslite-AFTR-Alarm-Port-Number: triggers an alarm when the number of ports used by a user reaches or exceeds the threshold.

TABLE 1. Dual-Stack Lite Carrier-Grade NAT Translation Table

Softwire-ID/IPv4/Protocol/Port	IPv4/Protocol/Port
2001:db8:0:1::2/10.0.0.1/TCP/10000	192.0.2.1/TCP/5000

- Table entry objects: an attacker can alter these entries to either drop legitimate entries or add harmful ones:
  - Dslite-Tunnel-Table: contains mapping entries of B4 addresses to AFTR addresses.
  - Dslite-NAT-Bind-Table: contains entries about the current active bindings within the NAT table of the AFTR.

Table 1 entries pose security risks by potentially revealing the number of hosts served by a single AFTR router, compromising DS-Lite infrastructure privacy [15]. RFC-6334 [19] suggests IP firewall implementation to thwart Man-in-the-Middle (MITM) attacks on DS-Lite softwire connections.

In addition, we conducted a research study aimed at analyzing the security of DS-Lite using the STRIDE methodology. Through the implementation of various attacking scenarios against a constructed test-bed environment, the investigation yielded insights into potential security vulnerabilities [3].

3.4. Lightweight 4over6

Despite the scarcity of published research on Lw4o6, several efforts have been made to explore its functionality and implementation. Ahmed Al-hamadani proposed a benchmarking test environment aimed at achieving RFC-8219 compliance, focusing on Lw4o6's core components [6]. Meanwhile, Omar D'yab constructed a test-bed demonstrating Lw4o6's operations but did not analyze its security aspects [13].

Marcel Wiget's implementation of lwB4 provided a functional machine with NAT44 and IPv4-in-IPv6 tunneling, offering isolation within its network namespace for enhanced flexibility and efficiency [16]. Despite prior attempts with OpenWrt software, which were deemed complex and unreliable, these efforts have contributed to the understanding of Lw4o6's operational challenges [16].

Utilizing the STRIDE method, we conducted a comprehensive vulnerability assessment of Lw4o6, identifying and cataloging multiple weaknesses. These findings, detailed in a table, include severity ratings and

insights into mitigation strategies [4].

3.5. MAP-E / MAP-T

In [25], performance and scalability testing of 464XLAT and MAP-T IPv6 transition technologies were conducted. A test-bed on Debian-based machines using Jool open-source software [21] was established to evaluate scalability, revealing that BR routers outperformed CE routers [25].

Another test environment for MAP-T infrastructure was developed by researchers in Brazil [10], focusing on connectivity testing of applications using the MAP-T translation mechanism. However, security analysis was not addressed. Furthermore, Ahmed Alhamadani designed a MAP-T tester aimed at RFC-8219 compliance, utilizing Jool software for CE and BR router implementation [7]. Additionally, Georgescu conducted penetration testing for MAP-T, exploring various attacking scenarios [18].

As for our research into this matter, we conducted an in-depth analysis of MAP-T vulnerabilities using the STRIDE method and building a test-bed for the technology. We uncovered multiple susceptibilities such as MITM and Address Resolution Protocol (ARP) Cache Poisoning [5].

3.6. STRIDE Method

The STRIDE method is widely used in cybersecurity and software development for identifying and mitigating security threats. It involves categorizing potential risks and vulnerabilities within a system or application and formulating effective countermeasures. Security professionals use this method to analyze potential attack vectors and enhance the security of systems throughout their development and operational phases. Building a Data-Flow Diagram (DFD) and applying the STRIDE method is an effective way to test system vulnerabilities, as it helps identify vulnerabilities based on data processing and storage activities [34]. A DFD is a visual representation of how data moves through a system. It helps in understanding the interactions between different components, such as users, devices, and processes.

4. NEW PROPOSED METHOD

Our proposed methodology aims to refine and enhance existing approaches by considering the unique characteristics and topologies inherent to IPv6 transition technologies. We define three layers that form the foundation of our new method. These layers are detailed in the following three subsections.

4.1. IPv4aaS Technologies

This layer focuses on the five most important IPv4aaS technologies for the reasons explained in the Introduction. These technologies share a common architectural pattern, consisting of Client, CE device, PE device, and Server components, resulting in analogous DFDs as shown in Fig.6. This categorization is a foundational step in our methodology, facilitating a structured approach to evaluate the security posture of IPv4aaS transition technologies.

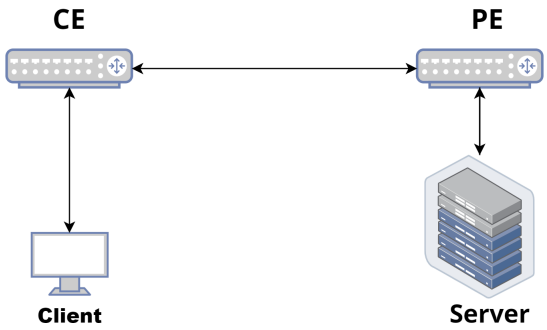

FIGURE 6. Abstract Layer: Client, CE, PE, and Server

4.2. Place of Statefulness

Generally, 464XLAT and DS-Lite technologies are referred to as "stateful" ones, as their PE devices (PLAT and AFTR) store information about every single network flow that traverses them. Conversely, Lw4o6, MAP-T, and MAP-E are referred to as "stateless" ones, as their PE devices (lwAFTR and BR) do not store information about every single network flow that traverses them. However, they are stateful in their CE devices. Table 2 gives a summary of the high-level operation of the five IPv4aaS technologies regarding their statefulness and method used for service provider network traversal. Please refer to [27] for more details.

Therefore, we distinguish the two groups based on where the given technology has a state. The "stateful" ones have a state in their PE device, and they do not have a state in their CE device. The so-called "stateless" ones do not have a state in their PE device, but they have a state in their CE device. The DFDs of the stateful and stateless technologies are shown in Fig. 7 and Fig. 8, respectively.

TABLE 2. Classification of IPv6 transition technologies based on the newly proposed method [27]

Technology is stateful on the	Service provider network traversal technology	
	Double translation	Encapsulation / Decapsulation
Operator Side	464XLAT	DS-Lite
Client Side	MAP-T	Lw4o6 / MAP-E

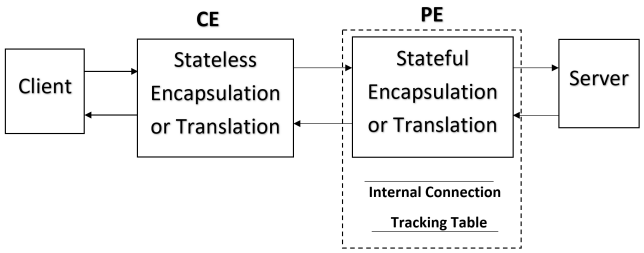

FIGURE 7. DFD for *stateful PE*-based technologies

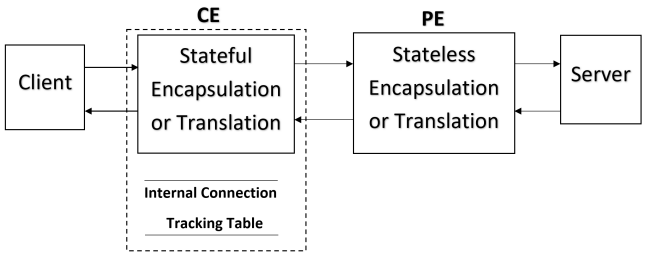

FIGURE 8. DFD for *stateless PE*-based technologies

4.3. Individual IPv6 Transition Technology Analysis

We further refine our analysis by examining each IPv6 transition technology individually. Each technology may be susceptible to different sets of vulnerabilities and may require specific deployment environments. By conducting a detailed analysis of each technology, we can better understand its unique security challenges and requirements.

Figure 9 illustrates the layered structure of our proposed method for the security vulnerability analysis, which comprises three hierarchical layers of categorization. At the initial layer of general categorization, termed "IPv4aaS Technologies," the selected technologies are grouped into a single overarching category based on their shared architectural pattern.

Subsequently, an in-depth analysis is conducted, focusing on the statefulness of IPv4aaS technologies (stateless or stateful) and exploring its implications for potential attacks.

Finally, at the third layer, the analysis investigates individual technologies such as DS-Lite, MAP-T, etc., each presenting a unique set of vulnerabilities.

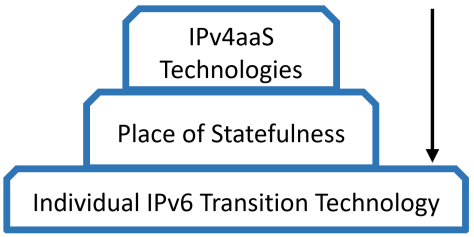

FIGURE 9. New proposed method hierarchy

5. RESULTS AND ANALYSIS

While our methodology typically advocates for a top-down analytical approach, we opted to reverse this sequence in this instance due to the availability of results concerning the bottom layer from our prior research endeavors. This approach involved a form of abstraction whereby vulnerabilities at higher layers were inferred by leveraging insights derived from the examination of vulnerabilities at lower layers. This section provides the outcomes of our prior research endeavors, wherein we conducted a comprehensive security analysis of the five leading IPv4aaS technologies. Employing the STRIDE method, we systematically evaluated the security posture of each technology. Furthermore, we constructed a test-bed environment tailored to each technology and executed various attack scenarios targeting the specific CE and PE devices of the given technology.

5.1. Method of Abstraction

In this subsection, we define a formal method for abstraction to derive the potential vulnerabilities of a more general level (higher layer) from the potential vulnerabilities discovered at a more specific level (lower layer). Let us denote the set of the considered IPv4aaS technologies (T) by the below formula:

$$T = \{t_i\} = \{464XLAT, DS-Lite, Lw4o6, MAP-E, MAP-T\} \quad (1)$$

As a result, the set of the DFD elements of technology t_i can be categorized by the below formula:

$$E_i = \{e_{i,j}\} = \{\text{the j-th DFD element of technology } t_i\} \quad (2)$$

Furthermore, the attack sets of the individual IPv4aaS technologies have already been determined in our previous research efforts and can be denoted by the below formula:

$$A_i = A(t_i, e_{i,j}) = \{a_{i,j}\} = \{\text{ Potential attacks identified for technology } t_i \text{ at } DFD \text{ element } e_{i,j}\} \quad (3)$$

The general DFD of the IPv4aaS technologies contains only those elements that occur in the DFDs of all IPv4aaS technologies. Formally:

$$E_{\text{IPv4aaS}} = \{e_k\} = \cap_i \{E_i\} \quad (4)$$

Finally, the potential attacks against the general DFD of the IPv4aaS technologies can be expressed as:

$$A_{\text{IPv4aaS}} = \{a_k\} = \cap_i \{a_{i,k}\} \quad (5)$$

5.2. Individual IPv4aaS Level

At this level, we identify the potential security vulnerabilities within each of the targeted individual IPv4aaS technologies.

5.2.1. 464XLAT Security Analysis

As shown in Fig. 10, we built a DFD for 464XLAT, where we pointed out the potential security vulnerabilities (points 1-11), every single point of them represents a DFD element. Furthermore, in [2], we summarized the potential security vulnerabilities in Table 3, where we correlated the attacks with the DFD element numbers.

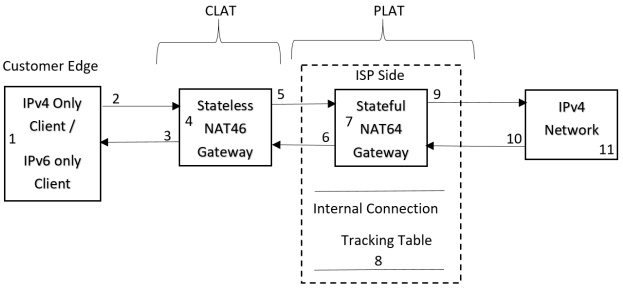

FIGURE 10. DFD for the Threat Analysis of 464XLAT [2]

5.2.2. DS-Lite Security Analysis

In [3], we constructed a DFD for DS-Lite, as depicted in Fig. 11, to delineate potential security vulnerabilities identified as points 1 through 11. Moreover, we summarized the potential security vulnerabilities and presented them in Table 4 with corresponding correlations drawn between the attacks and the DFD element numbers.

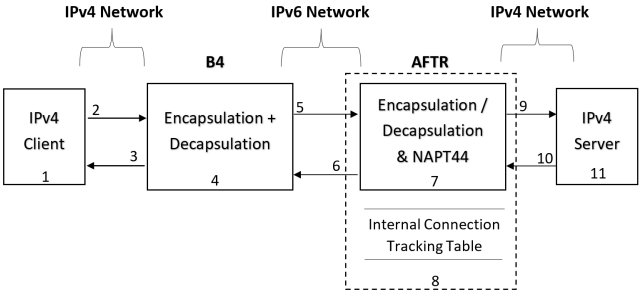

FIGURE 11. DFD for the Threat Analysis of DS-Lite [3]

5.2.3. Lightweight 4over6

Using the STRIDE method, we comprehensively assessed vulnerabilities within the Lw4o6 technology, uncovering multiple weaknesses [4]. We gathered security vulnerabilities of the Lw4o6 in Table 5, where we rated the attack's severity, considering how complex each is to carry out and how hard it is to mitigate it. A DFD was constructed for Lw4o6, as depicted in Fig. **??**, to delineate potential security vulnerabilities, identified as points 1 through 12.

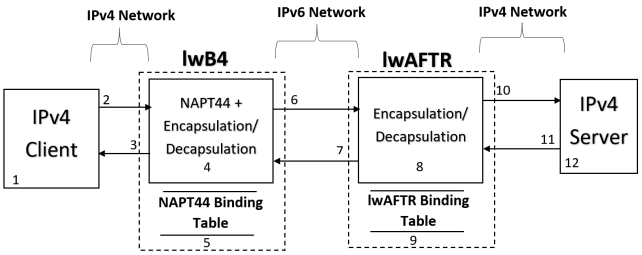

FIGURE 12. DFD for the Threat Analysis of Lw4o6 [4]

5.2.4. MAP-T

We conducted an in-depth analysis of MAP-T technology vulnerabilities employing the STRIDE method, uncovering multiple susceptibilities including potential MITM, ARP Cache Poisoning attack, etc. [5]. As shown in Fig. 13, we identified 11 points of vulnerabilities. Additionally, we summarized these potential attacks in Table 6.

Table 6 presents a detailed classification of threats, categorizing them based on the complexity of execution, the difficulty of mitigation, and the severity of their impact on the targeted system or data. The column labeled 'Intricacy

TABLE 3. Summary of 464XLAT Threats [2]

DFD Element	Threat	Possible Attacks
1	Spoofing & Repudiation	DoS attack against the CLAT
2, 3	Tampering, Information Disclosure and DoS	Failure of Service (FoS), collecting unauthorized information and DoS
4	All STRIDE Elements	FoS, DoS and unauthorized access
5, 6	Tampering, Information Disclosure and DoS	FoS, collecting unauthorized information and DoS
7	All STRIDE Elements	FoS, DoS and unauthorized access
8	Only indirect attacks	Tampering with Connection Tracking Table and DoS
9, 10	Tampering, Information Disclosure and DoS	FoS, collecting unauthorized information and DoS
11	Spoofing & Repudiation	DoS attack against the PLAT

TABLE 4. Summary of DS-Lite Threats [3]

DFD Element	Threat	Possible Attacks
1	Spoofing & Repudiation	Spoofing against the IPv4 Client
2, 3	Tampering, Information Disclosure and DoS	DoS against the B4 & Information Disclosure against the IPv4 Client
4	All STRIDE Elements	Spoofing the B4, DoS and unauthorized access
5, 6	Tampering, Information Disclosure and DoS	Information Disclosure against the B4 and the AFTR
7	All STRIDE Elements	Spoofing the AFTR, DoS, and unauthorized access
8	Only indirect attacks	DoS against the Connection Tracking Table or Tampering with it
9, 10	Tampering, Information Disclosure and DoS	Information Disclosure attack against the traffic between AFTR and IPv4 Server
11	Spoofing & Repudiation	Spoofing against the IPv4 Server

of Performing the Attack' indicates the level of difficulty an attacker encounters when attempting to execute a specific attack. This measure takes into account the required technical expertise, resources, and effort needed to carry out the attack successfully.

On the other hand, the column labeled 'Intricacy of Mitigation' evaluates the complexity associated with detecting and counteracting the identified threats. It considers the challenges and difficulties faced by defenders in identifying and effectively neutralizing these threats once they have manifested.

5.3. Place of Statefulness Level

In this layer, attacks have been classified according to the statefulness of edge-routers (CE & PE), as well as informed by findings from our previous research endeavors documented in [2], [3], [4], and [5]. While recognizing the potential existence of supplementary attack vectors, our analysis emphasizes the inclusion of prominent attacks identified through the STRIDE methodology and practical attack scenarios.

Building on formula (5), which we presented in Subsection 5.1, we continued the same path by splitting the main set into two unique sets of attacks.

TABLE 5. Summary of the Potential Vulnerabilities of Lw4o6 [4]

Attack Name	Intricacy of Performing the Attack	Intricacy of Performing the Mitigation	Attack Impact (Severity)
TCP RST Signal	Average	Average	Low
IP Address Spoofing	Average	Difficult	Medium
Packet Injection	Average	Difficult	Medium
Information Disclosure	Average	Easy	Medium
Packet's Payload Tampering	Difficult	Difficult	Medium
ARP Poisoning	Average	Difficult	High
Source Port Exhaustion	Easy	Average	High
TCP Session Hijacking	Easy	Average	Medium
Network Mapping	Easy	Easy	Low
DoS using TCP SYN Flood	Easy	Difficult	Critical

TABLE 6. Summary of the potential vulnerabilities of MAP-T [5]

Attack Name	Intricacy of Performing the Attack	Intricacy of Performing the Mitigation	Attack Impact
DoS	Easy	Difficult	Critical
Man-in-the-Middle	Average	Difficult	High
Information Disclosure	Average	Average	Medium
Source IP address Spoofing	Easy	Difficult	Critical
Source Port exhaustion	Average	Average	Medium
TCP RST Signal	Easy	Easy	Low
TCP SYNC Flood	Easy	Average	High
Packet's Payload Tampering	Average	Difficult	High
ARP Poisoning	Average	Difficult	High

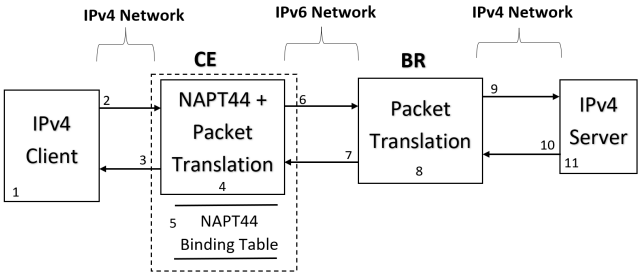

FIGURE 13. Data Flow Datagram of MAP-T

Furthermore, we differentiate between those attacks based on the statefulness of edge-routers (CE & PE). For example, the set of potential vulnerabilities of stateful PE-based technologies can be described as below:

$$A_{\text{IPv4aaS, stateful}} = \cap_{i \in \text{ Stateful-PE}}\{a_{i,k}\} \tag{6}$$

Similarly, the set of potential vulnerabilities of stateless PE-based technologies can be represented as:

$$A_{\text{IPv4aaS, stateless}} = \cap_{i \in \text{ Stateless-PE}}\{a_{i,k}\} \tag{7}$$

The results of the last two equations are illustrated in Tables 7 and 8, respectively, which are categorized based on the statefulness of the edge-routers (CE & PE).

TABLE 7. Summary of potential vulnerabilities *stateful PE*-based technologies

Attack Name
DoS against the PE device
Tampering with PE Connection Tracking Table
Source port exhaustion attack against the PE
MITM attack against the PE & CE
Source IP Address spoofing against the PE & CE
Information Disclosure against the CE–PE Traffic
Packet's Payload Tampering
ARP cache poisoning against the PE
Buffer overflow attack against the PE
Network Mapping against the CE
Packet redirection against the CE–PE Traffic

TABLE 8. Summary of potential vulnerabilities of *stateless PE*-based technologies

Attack Name
DoS against the CE device
Tampering with CE Connection Tracking Table
Source port exhaustion against the CE
Source IP Address spoofing against the PE & CE
Information Disclosure against the CE–PE Traffic
MITM against the CE & PE
TCP Session Hijack against the CE
Network Mapping against the CE
Packet's Payload Tampering against CE–PE Traffic
ARP cache poisoning against the CE
Packet Injection against the CE–PE Traffic
Packet redirection against the CE–PE Traffic

5.4. IPv4aaS Level

In this layer, we provide a concise summary of attacks at the IPv4aaS level, where we identify common attack vectors shared among the targeted technologies. These technologies exhibit a parallel structure comprising Client, CE, PE, and server components.

To identify the common potential vulnerabilities between the stateful and stateless PE-based technologies, we intersected the two subsets that we gathered in formulas (6) & (7) in Subsection 5.3:

$$A_{\text{IPv4aaS, common}} = A_{\text{IPv4aaS, stateful}} \cap A_{\text{IPv4aaS, stateless}} \quad (8)$$

The results of this intersection, which include only the common attacks among the two subsets, are illustrated in Table 9. Those results are also represented by intersecting the common attacks from Table 7 and 8, where they can be considered as outcomes of our current analysis.

As a result, Table 9 shows common attacks identified across several technologies on the IPv4aaS level.

The severity categorization presented in Table 9 was determined through an assessment of two pivotal metrics: the intricacy inherent in executing the attack and the complexity involved in its mitigation. These metrics were informed by empirical data acquired from our practical engagements with attack scenarios and mitigation strategies, as documented in our previous research contributions [2], [3], [4], and [5].

As a real-life scenario, there was a Distributed Denial of Service (DDoS) attack against Cloudflare, which is a major North American cybersecurity company that provides a wide range of services aimed at improving the security, performance, and reliability of websites [8]. This attack occurred in September 2022 and it was one of the largest and most sophisticated DDoS attacks ever recorded because it reached an unprecedented scale, with peak traffic hitting 3.8 terabits per second (Tbps) and surpassing two billion packets per second (Bpps) [9]. The attack was characterized by a high volume of User Datagram Protocol (UDP) traffic, using compromised devices to flood the network infrastructure. While there were no direct financial losses reported by Cloudflare, the attack serves as a warning about the potential consequences if such DDoS attacks were to overwhelm less-prepared infrastructures. Similarly, IPv6 transition technologies like DS-Lite and 464XLAT rely on translating and encapsulating IPv4 traffic over IPv6 networks, and attackers could exploit these mechanisms by sending large volumes of UDP or fragmented IPv4 traffic encapsulated within IPv6 packets, overwhelming the translation devices (e.g., AFTR in DS-Lite) and causing service disruptions. As a mitigation method, implementing rate limiting at the AFTR (for DS-Lite) or CLAT/PLAT (for 464XLAT) can help control the excessive flow of traffic, even when it originates from numerous distributed sources during a DDoS attack.

6. ATTACK IMPLEMENTATION SAMPLE

The test-bed was deployed on a "P" series node from NICT StarBED in Japan [29], utilizing a Dell PowerEdge 430 server. This machine features dual Intel Xeon E5-2683v4 processors, each operating at 2.1GHz with 16 cores, and is supported by 348 GB of 2400MHz DDR4 memory. The system was configured with Windows 10 Pro as the operating system.

TABLE 9. Summary of the Potential Vulnerabilities at IPv4aaS Level

Attack Name	Targeted Area	Severity
DoS	CE & PE	High
IP Address Spoofing	CE & PE	Average
Information Disclosure	CE–PE Traffic	Average
Packet's Payload Tampering	CE–PE Traffic	High
MITM	PE & CE	Average
Tampering with Connection Tracking Table	CE & PE	Average
Packet redirection	CE–PE Traffic	Average
Packet Injection	CE–PE Traffic	Average
ARP Cache Poisoning	CE & PE	High
Network Mapping	CE & PE	Low

As an attack sample, we selected the source port exhaustion attack against lwB4 router in Lw4o6 IPv6 transition technology. The lwB4 router, limited to a port range of [1024-2047], was vulnerable to port exhaustion. Using dns64perf++, a tool that generates a high volume of DNS queries to an IPv4 server (see Fig. 14) [14], we exploited this limitation. Since each DNS query requires a unique UDP port, the router's ports were depleted in less than a second as dns64perf++ sent 2500 packets per second. The script used for this attack, "`port-exhaust.sh`," is available in our GitHub repository [1].

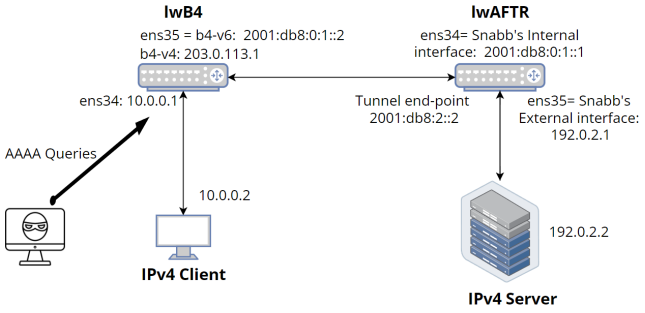

FIGURE 14. Source Port exhaustion [4]

Figure 15 captures the final three entries from Wireshark on the ens35 interface of lwB4, demonstrating the rapid depletion of the source port range [1024-2027] in under a second. Traffic processing came to a halt after approximately half a second and only resumed at the 30th second. This delay corresponds to the default 30-second timeout for UDP connections, after which the ports were made available again for new traffic.

To mitigate the attack, we implemented rate limiting on DNS queries, capping the rate at 100 packets per second. This was achieved by configuring "`iptables`" rules to drop incoming DNS queries by default while allowing traffic at the specified rate. With this limit in place, the allocated port pool on the lwB4 router remained unaffected, preventing exhaustion. The full script, named `exhaust-mitigate.sh`, is available in our GitHub repository [1]. A full description of this attack and more attacking/mitigation scenarios can be accessed in [4]. In addition, similar attacks against other IPv6 transition technologies are presented throughout our previous experiments in [2], [3] and [5].

7. DISCUSSION

7.1. Statefulness and Security in IPv4aaS

As we examined various IPv4aaS technologies, we discovered common vulnerabilities across all of them. We found that, while these vulnerabilities are similar across these technologies, their impact and location differ; some vulnerabilities affect the ISP side, while others affect the customer side. Although some technologies are marketed as stateless, they maintain states within their infrastructure. For instance, Lw4o6, MAP-T, and MAP-E, while labeled as stateless, hold states at the customer edge. Consequently, DoS attacks in such cases are more likely to affect specific customers rather than the entire system.

In contrast, a DoS attack on a technology with statefulness at the ISP side, like DS-Lite or 464XLAT, can impact all subscribers, causing more extensive damage and network downtime. In Table 10, we summarized the impact (severity) of the DoS attack on the customer and ISP sides based on the statefulness of the technology itself.

In synthesis, our research underscores the complexities and opportunities inherent in IPv6 transition technologies. As network administrators, policymakers, and researchers strive to embrace IPv6, addressing security concerns and refining implementations will be paramount.

Moving forward, our work sets the stage for future exploration, fostering a more secure and interconnected digital landscape. By contributing to the discourse surrounding IPv6 transition, we pave the way for enhanced network connectivity and resilience in an evolving technological landscape.

While each IPv6 transition technology has its own set of advantages and disadvantages, including considerations related to security, it is important to acknowledge the nuanced nature of these evaluations. However, after careful analysis, we have concluded that stateless technologies are the optimum choice for security reasons.

As demonstrated in Table 10, stateless technologies offer distinct advantages over stateful ones. A stateless approach, exemplified in this context, ensures heightened resilience against certain attacks such as DoS. Unlike stateful implementations, which concentrate state information on centralized devices, stateless architectures distribute this

No.	Time	Src. IP	Dst. IP	Protocol	Src. port	Dst. port	Info.
1028	0.561305919	203.0.113.1	192.0.2.2	DNS	2045	53	Standard query 0x03fd AAAA 000-000-003
1029	0.562221123	203.0.113.1	192.0.2.2	DNS	2046	53	Standard query 0x03fe AAAA 000-000-003
1030	0.562592491	203.0.113.1	192.0.2.2	DNS	2047	53	Standard query 0x03ff AAAA 000-000-003
1046	30.010075937	203.0.113.1	192.0.2.2	DNS	1024	53	Standard query 0xd524 AAAA 000-000-213

FIGURE 15. Wireshark Capture on lwB4 ens35.

TABLE 10. DoS impact based on the technology statefulness

State at Provider Side	DoS Impact at Client Side	DoS Impact at ISP Side
Stateful	Low	High
Stateless	High	Low

information across the network. Consequently, in the event of a DoS attack, targeting a stateful central device would have broader repercussions, potentially affecting a larger number of end-users due to packet loss or service shutdown. In contrast, stateless architectures mitigate such risks by dispersing the impact, limiting it to individual clients rather than compromising the entire network.

7.2. Effect on Modern IDS / IPS

Our findings indicate that modern Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) implementations face significant challenges with IPv4aaS IPv6 transition technologies due to their unique vulnerabilities. Traditional IDS/IPS systems may partially mitigate risks but struggle with encapsulated traffic (IPv4 address packet in IPv6 address packet) and differ in effectiveness based on whether the technology is stateful or stateless. For stateful technologies (e.g., DS-Lite, 464XLAT), the presence of a centralized connection tracking state at the PE makes them particularly vulnerable to targeted attacks like DoS. In these cases, conventional IDS/IPS solutions that focus on detecting anomalies in traffic patterns at central network nodes might still be effective. However, the centralization of the state can lead to a single point of failure, making traditional mitigation less reliable if the stateful PE is compromised. As a result, modern IDS/IPS implementations need to incorporate specific modules or extensions that understand the complexities of IPv4aaS transition technologies, which include the following:

- Ability to recognize and interpret encapsulated traffic (e.g., 4in6 packets) and identify patterns unique to IPv4aaS environments.
- Adaptive and Decentralized Security: adapting strategies based on the type of IPv4aaS and incorporating edge-based monitoring can better address stateless attack scenarios.
- Contextual Anomaly Detection: IDS/IPS systems should implement behavioral analysis specific to the transition technology in use to detect subtle, dispersed attacks.

In summary, while existing IDS/IPS solutions can address some threats, new adaptations are essential for effectively securing IPv4aaS in IPv6 transition environments.

8. CONCLUSION

Our novel approach, which involves dividing the security analysis into three layers, has demonstrated its effectiveness in streamlining the identification of common attacks and presenting them in a simplified yet comprehensive manner. By categorizing attacks based on the statefulness and the position of the edge router, we enhanced our understanding of the complexities inherent in IPv6 transition technologies. Notably, the location of the edge router significantly influences the severity (impact) of potential attacks. While our study may not encompass all existing IPv6 transition technologies due to their vast number, we propose that this methodology can be readily extended and applied by other researchers to analyze each of the remaining technologies individually, thereby contributing to a more thorough examination of this domain.

Ultimately, our analysis led to the conclusion that targeting a technology featuring a stateful PE presents a higher potential for effectiveness and severity in comparison to technologies employing a stateless PE. This assertion is rooted in the inherent characteristics of stateful devices, which encompass the retention of information regarding active connections. This repository of connection data serves as a vulnerability that malicious actors can exploit to disrupt legitimate traffic with greater efficiency, rendering such technologies more susceptible to various attacks, including DoS and Information Disclosure.

FUNDING

This work was not supported by any organization.

DATA AVAILABILITY

The data underlying this article are available in three different public repositories: [DS-Lite builder] at [https://github.com/ameen-mcmxc/DS-Lite_Test_Bed], [Lw4o6 builder] at [https://github.com/ameen-mcmxc/lw4o6-automation] and [MAP-T-builder] at [https://github.com/ameen-mcmxc/MAP-T-builder]. They can all be accessed by publicly accessing the GitHub database; no special account is needed.

LIST OF ACRONYMS

464XLAT Combination of Stateful and Stateless Translation

AFTR Address Family Transition Router

ARP Address Resolution Protocol

B4 Basic Bridging BroadBand

Bpps billion packets per second

BR Border Relay

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart

CE Customer Edge

CLAT Customer-side translator

DFD Data-Flow Diagram

DFDs Data-Flow Diagrams

DNS Domain Name System

DS-Lite Dual-Stack Lite

DoS Denial of Service

DDoS Distributed Denial of Service

FoS Failure of Service

IDS Intrusion Detection System

IETF Internet Engineering Task Force

ISP Internet Service Provider

ISPs Internet Service Providers

IPS Intrusion Prevention System

IPv4aaS IPv4-as-a-Service

Lw4o6 Lightweight 4over6

MAP Mapping of Address and Port

MAP-E Mapping of Address and Port with Encapsulation

MAP-T Mapping of Address and Port using Translation

MIB Management Information Base

MITM Man-in-the-Middle

NAPT Network Address and Port Translation

NAT Network Address Translation

PE Provider Edge

PLAT Provider-side translator

SNMP Simple Network Management Protocol

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

TCP Transmission Control Protocol

Tbps terabits per second

UDP User Datagram Protocol

REFERENCES

[1] Al-Azzawi, A. 'Lightweight 4 over 6 test-bed', online. available: https://github.com/ameen-mcmxc/lw4o6-automation.

[2] Al-Azzawi, A. and Lencse, G. 2021, 'Identification of the Possible Security Issues of the 464XLAT IPv6 Transition Technology', *Infocommunications Journal* **13**(4), 10–18.

[3] Al-Azzawi, A. and Lencse, G. 2023, 'Analysis of the Security Challenges Facing the DS-Lite IPv6 Transition Technology', *Electronics* **12**(10).

[4] Al-Azzawi, A. and Lencse, G. 2023, 'Lightweight 4over6 Test-bed for Security Analysis', *Infocommunications Journal* **15**(3), 30–41.

[5] Al-Azzawi, A. and Lencse, G. 2024, 'Security Analysis of the MAP-T IPv6 Transition Technology', *The Computer Journal* p. bxae059.

[6] Al-hamadani, A. and Lencse, G. 2021, Design of a Software Tester for Benchmarking Lightweight 4over6 Devices, *in* '2021 44th International Conference on Telecommunications and Signal Processing (TSP)', Brno, Czech Republic, August, pp. 157–161, IEEE, Piscataway, NJ.

[7] Al-hamadani, A. and Lencse, G. 2022, 'Towards Implementing a Software Tester for Benchmarking MAP-T Devices', *Infocommunications Journal* **14**(3), 45–54.

[8] *Cloudflare* [online]. available: https://www.cloudflare.com/.

[9] Cloudflare 'How Cloudflare auto-mitigated world record 3.8 Tbps DDoS attack', [online]. available: https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/.

[10] RFC 7703, 2015, Experience with Testing of Mapping of Address and Port Using Translation (MAP-T), IETF, Wilmington, DE.

[11] RFC 7596, 2015, Lightweight 4over6: An extension to the dual-stack lite architecture, IETF, Wilmington, DE.

[12] RFC 6333, 2011, Dual-stack lite broadband deployments following IPv4 exhaustion, IETF, Wilmington, DE.

[13] D'yab, O. and Lencse, G. 2022, Testbed for the Comparative Analysis of DS-Lite and Lightweight 4over6 IPv6 Transition Technologies, *in* '2022 45th International Conference on Telecommunications and Signal Processing (TSP)', Prague, Czech Republic, August, pp. 371–376, IEEE, Piscataway, NJ.

[14] Dániel, B. 'DNS64perf++ Measurement Tool', online. available: https://github.com/bakaid/dns64perfpp.

[15] RFC 7870, 2016, Dual-Stack Lite (DS-Lite) Management Information Base (MIB) for Address Family Transition Routers (AFTRs), IETF, Wilmington, DE.

[16] García, D. P. 'The B4 network function', [online]. available: https://blogs.igalia.com/dpino/2018/02/15/the-b4-network-function/.

[17] Georgescu, M., Hazeyama, H., Kadobayashi, Y. and Yamaguchi, S. 2014, Empirical analysis of IPv6 transition technologies using the IPv6 Network Evaluation Testbed, *in* 'Testbeds and Research Infrastructure: Development of Networks and Communities: 9th International ICST Conference', Guangzhou, China, May, pp. 216–228, Springer, USA, NY.

[18] Georgescu, M., Hazeyama, H., Okuda, T., Kadobayashi, Y. and Yamaguchi, S. 2016, The STRIDE Towards IPv6: A Comprehensive Threat Model for IPv6 Transition Technologies, *in* '2nd International Conference on Information Systems Security and Privacy', Rome, Italy, 02, SCITEPRESS, Setúbal.

[19] RFC 6334, 2011, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite, IETF, Wilmington, DE.

[20] Hong, H., Choi, H., Kim, D., Kim, H., Hong, B., Noh, J. and Kim, Y. 2017, When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks, *in* 'IEEE European Symposium on Security and Privacy (EuroS&P)', Paris, France, February, pp. 595–609, IEEE, Piscataway, NJ.

[21] ITESM 'Jool, Open Source IPv4/IPv6 Translator', [online]. available: https://www.jool.mx/en/index.html.

[22] RFC 6908, 2013, Deployment considerations for dual-stack lite, IETF, Wilmington, DE.

[23] Lencse, G. and Kadobayashi, Y. 2018, 'Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64', *Computers & Security* **77**, 397–411.

[24] Lencse, G. and Kadobayashi, Y. 2019, 'Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis', *IEICE Transactions on Communications* **102**(10), 2021–2035.

[25] Lencse, G. and Nagy, N. 2022, 'Towards the scalability comparison of the Jool implementation of the 464XLAT and of the MAP-T IPv4aaS technologies', *International Journal of Communication Systems* **35**(18), e5354.

[26] RFC 9313, 2022, Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS), IETF, Wilmington, DE.

[27] Lencse, G. and Ádám Bazsó 2024, 'Benchmarking methodology for IPv4aaS technologies: Comparison of the scalability of the Jool implementation of 464XLAT and MAP-T', *Computer Communications* **219**, 243–258.

[28] RFC 7599, 2015, Mapping of Address and Port using Translation (MAP-T), IETF, Wilmington, DE.

[29] *Making a synthesis emulation in IOT ERA possible Starbed5 Project. StarBED5 Project website* online. available: https://starbed.nict.go.jp/en/equipment/.

[30] RFC 6877, 2013, 464XLAT: Combination of Stateful and Stateless Translation, IETF, Wilmington, DE.

[31] RFC 4213, 2005, Basic Transition Mechanisms for IPv6 Hosts and Routers, IETF, Wilmington, DE.

[32] RFC 8585, 2019, Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service, IETF, Wilmington, DE.

[33] RFC 2460, 1998, Internet Protocol, Version 6 (IPv6) Specification, IETF, Wilmington, DE.

[34] Shostack, A. 2014, *Threat Modeling: Designing for Security*, John Wiley & Sons. Hoboken, NJ.

[35] RFC 7597, 2015, Mapping of Address and Port with Encapsulation (MAP-E), IETF, Wilmington, DE.