Investigating Middlebox Deployment and Characteristics in Dutch Autonomous Systems

Bulut Ulukapi*, Anna Sperotto*, Ralph Holz†*
*University of Twente, Enschede, The Netherlands
†University of Münster, Münster, Germany
Email: {b.ulukapi, a.sperotto}@utwente.nl, ralph.holz@uni-muenster.de

***Abstract*—Middleboxes shape modern network behavior by enforcing security policies and optimizing traffic, but their opaque operations reduce network transparency and complicate digital sovereignty efforts. In this study, we analyze middlebox deployment and behavior across Dutch Autonomous Systems (ASes), motivated by the strategic position of the Netherlands in European network infrastructure. We classify ASes into sectors—governmental, private, educational, and digital infrastructure—and using active probing and third-party datasets, we examined 989 ASes and 5.1 million IPs, identified 310 middleboxes, with high confidence, registered to and located within Dutch ASes. Our results reveal several sector-specific interference patterns. ISPs and hosting providers show diverse modifications, governmental ASes exhibit consistent policy enforcement at the edge, and private ASes adopt hybrid strategies, combining TCP option stripping with deeper manipulation of TCP state. Exposed management interfaces and outdated software further increase operational risks, whether tied to the middleboxes themselves or co-located devices. Our findings highlight the value of AS-level investigation for understanding middlebox behavior and underscore the need for proactive auditing and secure configuration to support resilient and sovereign network infrastructure.**

***Index Terms*—Middleboxes, Network Interference, Network Analysis**

I. Introduction

Autonomous Systems (ASes) are the building blocks of the Internet. They influence the resilience, performance, and security of connectivity for both operators and end-users, as they determine how traffic is forwarded, filtered, or prioritized across networks [1]. The operation of ASes directly impacts the delivery and continuity of essential services, including government, healthcare, education, finance, and digital platforms.

One important factor that influences AS operations is the increasing global deployment of middleboxes, which are commonly used to optimize performance, improve efficiency, and enhance security by inspecting and modifying network packets according to established policies [2]. However, the proliferation of middleboxes introduces several challenges, including increased network complexity, reduced transparency, limited interoperability, and exposure to security risks [3]–[6]. These issues can undermine the end-to-end principle by obscuring traffic handling and increasing the risk of interference between endpoints. As a result, operators may lack visibility into how their traffic is handled, making it harder to ensure reliable delivery or to audit network behavior, raising concerns about data accountability and loss of operational control, key elements of digital sovereignty. For instance, operators might not be fully aware of the extent to which their traffic is routed through or modified by middleboxes, which could pose risks to the confidentiality or integrity of communications [6].

To gain deeper insights into the interplay of ASes and middleboxes, we focus on a national context in this paper, specifically the Netherlands as the first step. The Netherlands hosts a dense and critical segment of global Internet infrastructure. Given their important role, understanding the presence and behavior of middleboxes within Dutch ASes is essential for assessing infrastructure integrity, service resilience, and transparency. By systematically categorizing these ASes according to their primary purpose and usage—spanning governmental networks, digital infrastructure providers, educational institutions, and private sector entities—we aim to reveal the varying characteristics and behaviors of middleboxes deployed across different AS categories.

Our contributions are as follows. We provide the first large-scale, AS-level analysis of middlebox deployment in the Dutch Internet ecosystem, contextualize middlebox behavior across AS roles, and identify exposed services and vendor-specific patterns. These findings offer practical insight for operators and network managers into traffic control practices, infrastructure exposure, and operational risks across diverse network environments.

II. Background and Related Work

1) Middleboxes: A middlebox is any intermediary network device that performs functions beyond basic forwarding, unlike traditional routers or switches that preserve the end-to-end principle [3]. Middleboxes can alter, delay, or drop packets according to predefined rules and can perform real-time inspection. Examples include firewalls, proxies, IDS/IPS, load balancers, etc. They are used for security purposes, performance, compliance, traffic management, and even censorship. However, they also increase network complexity, reduce transparency, create new attack vectors, and interfere with protocol semantics [7], [8].

Detecting middleboxes is challenging, as their interference can be subtle. Early studies tested TCP compliance and congestion control using crafted packets [4], [9]–[12]. While these studies were not explicitly designed to detect middleboxes, they revealed them through deviations from expected TCP responses. These works showed that middleboxes often block or modify extensions, disrupt congestion control, and break

978-3-903176-75-1 ©2025 IFIP

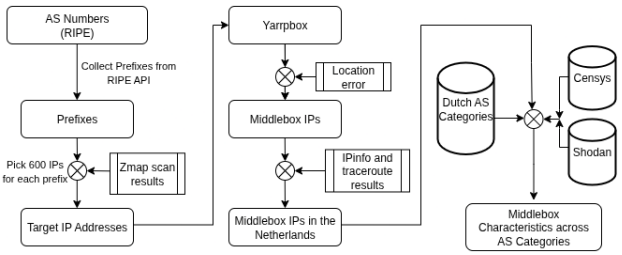

Fig. 1. Overview of our methodology

protocol compliance. Extending detection beyond TCP, several tools analyze broader traffic to capture middlebox interference in protocols like HTTP and DNS. Reis et al. introduced web tripwires to expose in-transit modifications, affecting over 1% of clients [13]. Glasnost detects traffic shaping by identifying BitTorrent differentiation [14], while Netalyzr uncovers anomalies such as DNS manipulation, DNSSEC stripping, HTTP caching, and MTU issues [15]. More recently, Sundara Raman et al. leveraged Cloudflare traffic to identify tampering signatures across networks, demonstrating how middlebox interference affects real users at scale [16]. Tracebox [17] is a tool to detect middleboxes by comparing outgoing packets with ICMP replies. Its sequential, stateful probing is slow, however. Yarrpbox [18] overcomes this limitation with randomized, stateless probes, also incorporating Paris Traceroute techniques.

Recent studies have used Yarrpbox to analyze middlebox deployments. In [19], researchers examined over 500 ASes, identifying 250 middleboxes and their vendors. The authors found middlebox distribution does not correlate with censorship practices, and uncovered security issues, highlighting the need for refined measurement techniques. In our preliminary study of Dutch ASes [20], we found that increasing the number of IP addresses sampled per prefix improved detection accuracy, though with diminishing returns beyond 600 addresses. We also observed that most middleboxes (56%) were located in hosting providers.

2) National and Regional Infrastructure Studies: Prior work has explored several aspects of Dutch network infrastructure. Jansen et al. [21] show that many Dutch and European government services still rely on foreign-hosted infrastructure despite digital sovereignty efforts. At the EU level, Ververis et al. [22] found widespread ISP use of middleboxes for state-mandated website blocking across all 27 member states. While these studies provide valuable insights, there is no work, except our preliminary study [20], that specifically examines middlebox deployment and behavior within Dutch ASes across multiple sectors.

III. Methodology

1) Target ASes and IP Addresses: We collect the AS numbers (ASNs) and associated IPv4 prefixes of Dutch ASes using the RIPE API [23], giving us a total of 1589 ASNs *registered* in the Netherlands. We then examined the RIPE database records for each ASN and identified 600 that had no registered IP prefixes, hence we retained 989 ASes for analysis with a total of 14 614 prefixes. One of the key challenges in middlebox detection is deciding how many IP addresses to sample from each prefix, as this choice directly affects detection coverage [20]. Following the methodology of [20], we sampled 600 IP addresses per prefix, yielding 5.1 million target IPs.

2) Middlebox Detection: We use yarrpbox [18] to detect middleboxes on the path to the targets. For a comprehensive description of the tool, we refer the reader to [18]. All scans were conducted from a single machine located at the University of Twente in the Netherlands. Also following the best practices from [20], we set the scan rate to 5 kpps, using only SYN probes to port 80. We use the same *location error metric* as suggested in the original publication [18] to obtain a confidence level for the detected middlebox IPs. The metric represents the number of hops between the suspected middlebox and the nearest earlier hop that returned an ICMP quote containing an equal or larger portion of the original probe packet. This helps to localize the point of traffic modification more accurately. Unless explicitly stated, we only consider those IPs in our analysis that the tool marks as *high-confidence middleboxes*, *i.e.,* those with a location error of at most one hop.

3) Geolocating Middleboxes: Given that accurate geolocation of network infrastructure is a well-documented and inherently challenging problem [24], we adopt a two-step validation approach to improve reliability. First, we use the IPinfo dataset [25] for geolocation. We then perform traceroutes and analyze round-trip latencies. Latencies significantly exceeding 18 ms—derived from the 95th percentile of our traceroute measurements—are used, together with geographic hints extracted from reverse DNS hostnames (when available), to assess whether a host is likely located in the Netherlands. Finally, we manually inspect cases where the IPinfo location and our latency-based inference diverge, to resolve inconsistencies and improve overall accuracy.

4) Categorization of ASes: We categorized Dutch ASes using classification data from IPinfo [25], which provides a coarse-grained taxonomy of ASes with four categories: ISP, hosting, business, and education. While useful as a starting point, these categories were not sufficiently granular for our purposes. To improve specificity, we extended the categorization to reflect the socio-technical role of each AS in the Dutch digital landscape. We drew conceptual inspiration from the Dutch "Basisbeveiliging" registry [26], which outlines sectoral responsibilities for critical services and infrastructure. However, this registry does not include AS-level identifiers, making it unsuitable as a primary source. Instead, we manually annotated ASes using a combination of publicly available descriptions (WHOIS data, company websites, and registry records), cross-referenced with known sector affiliations. Our final categories include *Governmental*, *Digital Infrastructure*, *Education*, and *Private Sector*, with several subcategories detailed in IV-B.

5) Vendor Attribution: We use data from Censys [27] and Shodan [28] (under their academic licences) to identify vendors of detected middleboxes. Shodan queries are performed via its API, while Censys data (Censys Universal Internet Dataset) is from a snapshot from September 2024, the most recent available to us at the time of writing. We aggregate information such as open ports, service banners, OS and software metadata, and vendor labels. When both platforms return results for the same IP, we compare them for consistency. If entries are outdated or conflicting, we manually verify host availability (ICMP pings) and open ports (fast port scans); in such cases, we prioritize the most recent and directly verified data. Shodan-only results are accepted if updated within two weeks.

6) Limitations: While we document our assumptions and design choices throughout this section, some limitations remain. First and most importantly, our findings may reflect transient network behaviors. Middlebox configurations can be updated dynamically in response to attacks, operational changes, or policy shifts. Therefore, our findings should be interpreted as a snapshot rather than a definitive inventory. Future longitudinal studies are needed to characterize the persistence and evolution of middlebox deployments in Dutch ASes.

Because our measurements target Dutch ASes from within the Netherlands, we may miss middleboxes active only on inbound international traffic. Internal segmentation (e.g., VLANs, subnets, per-service filtering) may also limit detection to specific flows, so our results may not capture full deployment. Our approach relies on Yarrpbox, which detects middleboxes that alter IP/TCP header fields. Devices filtering traffic without such modifications, or operating on other protocols, may evade detection. We also rely partly on IPinfo for geolocation and AS classification, enriched with manual categorization, but both have limitations. Accurate geolocation remains challenging, as IP addresses may be reassigned, routed through tunnels, or inaccurately recorded in registries, leading to mismatches between inferred and actual locations. AS-level classification is similarly complex, since ASes often span multiple roles (e.g., an ISP also offering hosting or enterprise services), and address space may be leased or reallocated. We assign categories based on the dominant role inferred from public sources.

7) Ethical Considerations: We followed the same ethical practices as in our prior works [19], [20].

IV. Results and Discussion

A. Overall Statistics

Our scan identified 205k modifications made by middleboxes across 5.1 million traces. About 4% of all scanned paths showed evidence of at least one actively interfering middlebox. These modifications originate from 1791 candidate middlebox IPs, of which 607 are classified as "high confidence". Only 1.32% of all middleboxes are located within the source AS (*i.e.,* the scanning AS), and nearly two thirds (65.9%) reside within the destination AS. The remaining 32.8% are distributed across ASes that are neither source nor destination. Geolocating the 607 middleboxes, we find that only 321 are actually located within the Netherlands. The remaining 286 were distributed across 34 other countries. Table I presents the top five countries, with the United States accounting for 35.7% of middleboxes located outside of the Netherlands. Traceroute paths support these geolocation results by showing early exits from Dutch networks, higher hop counts, and transit through Tier-1 or regional international carriers. Many exhibit significant latency jumps and reverse DNS hostnames with geographic markers (e.g., .ash, .nyc, .lon). Moreover, RTTs frequently exceed 100 ms, with some surpassing 300 ms, consistent with intercontinental routing. Of the 321 middleboxes, 11 belong to foreign entities with a physical presence in the Netherlands, such as Akamai (AS32787), Cloudflare (AS13335), and Global Secure Layer (AS7578). Excluding these results in 310 middleboxes considered for further analysis.

TABLE I
Middleboxes Attributed to Dutch ASes but Geolocated Abroad

Country	MB %	Country	MB %
United States	35.7%	Italy	5.9%
Japan	8.0%	Australia	5.9%
Great Britain	7.9%		

B. Deployment Across AS Categories

Table II shows in which AS categories our middleboxes appear.

1) Digital Infrastructure: This category comprises ISPs, hosting providers, and IXPs. Naturally, we observe the highest concentration of middleboxes here (88.1% are found in an AS in this category).

ISPs: We identify 127 middleboxes in ISPs, *i.e.,* access providers. They are responsible for 5307 packet modifications in total. Analyzing the position of middleboxes on the paths, we find that 82.3% are located within destination ASes and 17.7% in transit ASes, while no middleboxes were observed in the source AS. This aligns with earlier findings that middleboxes tend to cluster closer to the endpoint or access network, where ISPs apply some sort of traffic modification. Our results show that the most common modifications were TCP NOP insertions (36.5%) and removing the MPTCP MP CAPABLE option (35.9%). The insertion of TCP NOP options, typically used for alignment, is not inherently problematic. However, it frequently co-occurs with stripped or modified options, *e.g.,* MP CAPABLE. This suggests a possible strategy to preserve packet size after stripping options, that has also been documented in studies analyzing middlebox-induced TCP option rewriting [7], [18]. Distinguishing between benign alignment and policy-driven modification remains challenging. The removal of the MP CAPABLE option, which signals a host's intent to initiate a Multipath TCP connection, is more consequential. Prior work has shown that such behavior

TABLE II
MIDDLEBOX DEPLOYMENT ACROSS AS CATEGORIES

Category	Percentage	Subcategory	MB count	Most common modification
Digital Infrastructure	88.1%	ISP	127	NOP Addition
		Hosting	135	Urgent Pointer/Receiver Window Modification
		IX	11	Broad Interference
Governmental	2.3%	Ministries	6	MP Capable Modification
		Municipalities	1	Urgent Pointer/Receiver Window Modification
Education	4.5%	Institutional	10	Sequence Number Modification
		Personal	4	Urgent Pointer/Receiver Window Modification
Private Sector	5.1%	—	16	Sequence Number Modification

can hinder end-to-end MPTCP deployment or interfere with protocol evolution [4], [29]. Its removal suggests that the middlebox, most likely a firewall, either lacks support for MPTCP or has been configured to strip unknown or unsupported TCP extensions [30]. We examined the middleboxes (about 30 devices) that removed the MP CAPABLE option. Only 12 devices appear in Censys or Shodan. All were identified as either Palo Alto or Check Point firewalls.

Hosting providers: We find 135 middleboxes in this category, responsible for 7759 modifications that are different from those we observed in ISPs. Here, 64.6% involve changes to the TCP Urgent Pointer (UP) or Receiver Window (RW) fields, typically by overwriting the Urgent pointer (often to zero) or altering the advertised window size. Previous studies have shown that certain middleboxes—including performance-optimizing TCP accelerators and transparent proxies—may manipulate these fields to enforce local flow control or to mitigate perceived misbehavior in TCP streams [4]. Hence, hosting ASes appear to be more frequently associated with transport-layer field modifications related to connection state or congestion control. This is also supported by 17.4% of modifications impacting the TCP sequence number. Only 6.0% involve NOP additions. On the whole, our results are consistent with the use of middleboxes for regulating and optimizing traffic flows.

IXPs: We identify eleven middleboxes in Internet Exchange Points (IXPs), associated with 25 observed modifications. IXPs are meant to provide neutral interconnection; hence, this result is consistent with expectations [31]. However, we find the modifications to be different from the previous subcategories. They fall into the spectrum of modifications where yarrpbox's methodology (of hashing header values) cannot exactly pinpoint the modification to a single field but indicates a modification occurred in at least one field in a set that includes the IP Identifier (IP ID), TCP Timestamps (TSval, TSecr), RW, or UP [18]. Although rare, the presence of sequence number modification and changes to TCP timestamp fields within IXPs are noteworthy. Architectural proposals such as SDX [32] demonstrate that IXPs may support policy enforcement or header manipulation functions. Our observations may therefore reflect either emerging operational practices of this kind or modifications introduced by auxiliary equipment deployed at or near exchange points but attributed to IXPs. Further investigation is required to determine the exact origin of these modifications.

2) Governmental networks: We detect seven middleboxes in governmental ASes (six ministries, one municipality). They are collectively responsible for 10739 observed packet modifications, a high number in comparison, although there are only three types of modifications: NOP addition, removal of the MPTCP MP CAPABLE option (exactly the same number of occurrences), and again the kind of modifications that yarrpbox cannot pinpoint to a specific field. The first two types align with known firewall configurations that strip unsupported or unknown TCP options (see ISP category). Traceroute-based path analysis confirms that 100% of the detected middleboxes in this category are located within the destination ASes. These middleboxes reflect targeted configurations intended to enforce traffic controls and security policies.

3) Education: We identify ten middleboxes in ASes associated with education and research (453 modifications). The dominant interference type in this category was the modification of TCP Sequence Number, comprising 82.1% of all modifications. Again, this is different to the other subcategories. Further types of interference include changes to the Urgent Pointer or Receiver Window (11.3%) and suppression of the MP CAPABLE TCP option and corresponding NOP insertion (each at 3.1%). Interestingly, the majority (72.7%) of middleboxes in this category were located in the source AS. While this might seem counterintuitive, our measurements originated from SURF B.V., a Dutch educational and research network that serves multiple institutions. Further inspection confirmed that the observed middleboxes were not deployed at our host institution but at other connected educational networks within SURF. The remaining middleboxes were located in destination ASes (9.1%) and in transit ASes (18.2%), defined here as any intermediate networks between the source and destination. This distribution contrasts with the patterns observed in other AS categories such as ISPs or governmental networks, where middleboxes tend to concentrate at ingress points.

We also identify four middleboxes in other research ASes, typically smaller networks operated by individuals or hobbyist organizations. These account for 51 observed modifications. Nearly all (92.2%) involved changes to the TCP UP and RW fields. While the UP is largely deprecated in modern TCP stacks and often considered a legacy field, its modification may still indicate outdated packet normalization [33]. RW alterations, on the other hand, directly impact TCP flow control

by modifying the advertised receive capacity. Most of these middleboxes (75%) were located in destination ASes, with the remainder in transit ASes.

4) ASes in the Private Sector: ASes in this category are operated by commercial and business entities. We identify 16 middleboxes associated with 5420 modifications. Similar to the observations for ISPs and hosting providers, we observe a diverse set of modifications. The most prevalent interference type was TCP Sequence Number modification, accounting for 52.1% of all modifications. We also observed the removal of MPTCP MP CAPABLE options and simultaneous NOP additions in 14.5% of cases each. More nuanced interference patterns, such as the removal or rewriting of timestamp-related fields (TSval, TSecr) and the SACK Permitted option, were also sometimes observed. These could affect advanced congestion control features. All middleboxes were located in the destination AS, consistent with a deployment of perimeter security appliances or performance-optimizing network devices.

C. Middlebox Characteristics

We use Censys and Shodan to analyze open ports, services, vendors, and security posture of the detected middleboxes. However, these sources did not offer relevant data for 71 of 127 middleboxes in ISPs, 74 of 135 in hosting providers, 8 of 11 in IXPs, 5 of 7 in governmental networks, 10 of 14 in educational networks, and 11 of 16 private sector middleboxes. We proceeded with the analysis of the remainder to provide an initial exploration into the middlebox landscape within Dutch ASes.

Open Ports and Services: We analyze open ports to identify commonly exposed services on middleboxes. The most common ports we observed can be seen in Table III. The prevalence of open ports 80 (HTTP) and 443 (HTTPS) reflects exposed management interfaces, often hosting web-based administration panels for firewalls (e.g., Palo Alto, Check Point), as confirmed by probing. In some cases, these interfaces originate directly from middleboxes whether by design or misconfiguration, while in others they may stem from co-hosted virtual appliances or infrastructure components that share the same public IP. The presence of port 161 (SNMP) also indicates that many middleboxes expose administrative interfaces, which prior work [34] warns can leak configurations and metadata if unsecured. In our study, several devices revealed SNMP engine IDs, boot counters, and enterprise identifiers useful for reconnaissance. Port 22 (SSH) appeared in 17 cases, suggesting remote administration or co-hosted services, both of which pose security risks if improperly secured. Of 16 middleboxes with port 53 (DNS) open, most rejected recursive queries, suggesting local resolver use or co-hosted infrastructure rather than DNS filtering. Only one device functioned as an open resolver. Port 179 (BGP) suggests that some middleboxes may also operate as routers. A few devices exposed port 123 (NTP), which is notable since time synchronization is typically handled within internal infrastructure. The appearance of port 8443 reflects its role as an alternate HTTPS port commonly used for management interfaces. We also observed 14 vendor-specific ports, including port 2000 (MikroTik Bandwidth Test Server, 4 cases) and port 264 (Check Point firewalls, 10 cases). Our findings suggest that many middleboxes in Dutch ASes may serve multiple roles, though some observed service exposures could stem from co-hosted infrastructure, indirect visibility, or attribution inaccuracies. These results highlight the complexity of interpreting middlebox behavior and the need for cautious, context-aware analysis.

TABLE III
TOP 10 OPEN PORTS ACROSS MIDDLEBOXES

Port Number	Count	Percentage
80	32	16.5%
443	29	14.9%
161	28	14.4%
22	17	8.7%
53	16	8.2%
179	15	7.7%
123	11	5.7%
264	10	5.2%
8443	6	3.1%
2000	4	2.1%

Vendor Mapping: Using Censys and Shodan data for vendor attribution, we identify vendor or product signatures for 85 out of the 310 middleboxes. The identified devices span 27 distinct vendors or product families. The top five most commonly observed vendors can be seen in Table IV. These vendors provide both commercial and open-source solutions, indicating diverse deployment models. We also identify middleboxes from major network infrastructure providers (*e.g.,* 2 Juniper, 4 Brocade, and 3 Fortinet devices). This spread reflects the varying operational and security preferences. Although vendor information could only be determined for a subset of middleboxes (27%), the identified vendors offer a useful snapshot of the deployment landscape. While they reflect a mix of open-source and commercial solutions, US-based manufacturers remain dominant, hinting at market dominance, with implications for digital sovereignty.

Security Assessment: Our inspection of services and configurations on middleboxes reveals potential operational and security risks. In certain cases, the exposures can be attributed directly to the middleboxes, for example, if they run outdated software or expose management interfaces. In other cases, co-hosted virtual appliances or infrastructure components may account for the observed risks, similar to the earlier discussions. While we cannot always distinguish between the two, both scenarios are noteworthy: either the middlebox is misconfigured, or its presence leads to the exposure of vulnerable adjacent systems. In either case, our findings suggest that tools like Yarrpbox may help reveal components of the attack surface, raising concerns for network operators but also offering opportunities for improved asset management and security monitoring. Among the devices with identifiable software versions, we found instances of outdated or end-

TABLE IV
TOP 5 VENDORS ACROSS MIDDLEBOXES

Vendor	Count	Percentage
Check Point	16	18.8%
pfSense	9	10.6%
Cisco	8	9.4%
Mikrotik	8	9.4%
Palo Alto Networks	6	7.1%

of-life software. Most notably, we identify seven devices running NTPv3, an obsolete protocol version lacking essential security enhancements found in NTPv4, such as authentication and resistance to spoofing and amplification attacks. The persistence of NTPv3 is also concerning due to its known exploitable vulnerabilities. Several middleboxes were found to run outdated NTPv4 daemons (*e.g.,* versions 4.1.1a, 4.2.0-a, and 4.2.8p14), some of which are vulnerable to CVEs such as CVE-2020-13817 and CVE-2020-15025, involving denial-of-service and memory exhaustion. We also observed middleboxes or adjacent infrastructure operating unsupported operating systems and services such as Debian 9.0, FreeBSD 10.1, outdated firmware on an HP ProCurve 2626 switch, and BIND 9.9 combined with OpenSSL 1.1.1, each linked to known vulnerabilities such as CVE-2016-1286 and CVE-2022-0778. Although limited in number, these exposures highlight lagging patch management or reliance on legacy systems. Furthermore, we identified three devices supporting PPTP, an obsolete VPN protocol based on weak MS-CHAPv2 cryptography. Additional exposures included SNMP (28 cases), Check Point's port 264 (10), and a FortiGate device disclosing model and serial information. While not all constitute direct vulnerabilities, such interfaces facilitate reconnaissance.

V. OPERATIONAL CONSIDERATIONS

Our analysis of middleboxes across Dutch ASes shows differing interference behaviors and broader implications for infrastructure exposure and control. ISPs and hosting providers account for the largest number of middleboxes, typically exhibiting varied interference types to manage traffic in high-volume environments. Governmental ASes, by contrast, display narrowly scoped interference, consistently stripping specific TCP options at the network edge, possibly as part of some policy enforcement. Private sector ASes adopt a hybrid approach, blending stateful TCP manipulation with firewall-like filtering, reflecting operational priorities that balance performance and security. These findings illustrate the variety of middlebox deployment strategies observed and how middleboxes, depending on their context, shape network operations across different AS categories.

From a security perspective, our findings reveal risks extending beyond middlebox behaviors alone. By scanning for middleboxes, we obtained exposed auxiliary services, such as SNMP, SSH, and web-based administration interfaces, some running outdated or unsupported software (e.g., NTPv3, legacy OS/firmware). While further analysis is needed to determine whether these services belong directly to the middleboxes or to co-hosted virtual appliances, their strategic positioning at network ingress points makes them relevant from an operational risk standpoint. Unlike generic internet-wide scans (e.g., ZMap), our approach identifies vulnerable devices positioned at critical network chokepoints, offering attackers valuable context for targeted reconnaissance and follow-up attacks. Consequently, network operators should proactively use similar scanning techniques to regularly audit their middleboxes and associated virtual appliances, carefully tracking end-of-life statuses and known vulnerabilities. Moreover, we argue that monitoring strategies must also account for focused, stealthy reconnaissance attempts, not solely large-scale scanning activity, to better protect against this form of exposure.

Only 27% of middleboxes could be attributed to known vendors using the datasets we mentioned, yet even this limited sample reveals dependency patterns with implications for digital sovereignty, resilience, and regulatory control. Vendor mapping shows a heavy reliance on US-based platforms, with Check Point, Cisco, and Palo Alto dominating; only MikroTik (Latvia) appeared in the top five from outside the US. We also observed Dutch ASes deploying middleboxes abroad, as well as middleboxes belonging to foreign ASes within the Netherlands, underscoring the challenges of jurisdictional control in globally interconnected infrastructure. Such arrangements create potential risks, as the management, legal accountability, and data handling of these middleboxes may fall under foreign jurisdictions, complicating oversight and limiting the ability of authorities to enforce national or regional security, privacy, or governance standards.

Our findings show that middlebox deployment in Dutch ASes entails technical variation as well as operational and possibly jurisdictional risks. Addressing these issues requires regular audits of middleboxes and co-located systems, monitoring for stealthy reconnaissance, and reviews of supply chain and jurisdictional dependencies. Together, these measures are essential to ensure transparency, resilience, and effective governance of network infrastructure.

VI. CONCLUSION

This study provides an initial AS-level perspective on middlebox deployment in the Netherlands. Our results reveal different deployment strategies and interference patterns for different sectors. We also observed exposed management interfaces, outdated software, and vendor-specific ports, indicating tangible operational and security risks. These findings suggest that middleboxes should be regarded as elements of the broader network infrastructure, where their deployment and operation carry significant implications for security, reliability, and governance. Our work demonstrates the value of fine-grained AS-level measurements for making these dynamics visible. As middleboxes increasingly influence traffic handling and infrastructure control, transparency into their operation and tracking their deployment trends is essential to inform both network operations and evidence-based policymaking.

Acknowledgments

We thank IPinfo, Censys, and Shodan for providing us with academic licences. This work is supported by the research project CATRIN (NWA.1215.18.003) as part of the Dutch Research Council's (NWO) National Research Agenda (NWA) and partly financed by the Province of Gelderland and Centre for Safety & Digitalisation.

REFERENCES

[1] S. P. Gorman and E. J. Malecki, "The networks of the internet: an analysis of provider networks in the usa," *Telecommunications Policy*, vol. 24, no. 2, pp. 113–134, 2000.
[2] K. Edeline and B. Donnet, "A bottom-up investigation of the transport-layer ossification," in *TMA 2019*, pp. 169–176, 2019.
[3] B. Carpenter and S. Brim, "Middleboxes: Taxonomy and issues," tech. rep., 2002.
[4] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, M. Handley, and H. Tokuda, "Is it still possible to extend tcp?," IMC '11, p. 181–194, 2011.
[5] K. Bock, A. Alaraj, Y. Fax, K. Hurley, E. Wustrow, and D. Levin, "Weaponizing middleboxes for {TCP} reflected amplification," in *USENIX Security 21*, pp. 3345–3361, 2021.
[6] Internet Society, "Navigating digital sovereignty and its impact on the internet: A ten minute introduction," technical report, Internet Society, Dec. 2022.
[7] K. Edeline and B. Donnet, "A first look at the prevalence and persistence of middleboxes in the wild," in *ITC 29*, vol. 1, pp. 161–168, 2017.
[8] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, and A. Rayhan, "Middlebox communication architecture and framework," tech. rep., 2002.
[9] J. Pahdye and S. Floyd, "On inferring tcp behavior," SIGCOMM '01, p. 287–298, 2001.
[10] B. Hesmans, F. Duchene, C. Paasch, G. Detal, and O. Bonaventure, "Are tcp extensions middlebox-proof?," HotMiddlebox '13, p. 37–42, 2013.
[11] A. Medina, M. Allman, and S. Floyd, "Measuring the evolution of transport protocols in the internet," *SIGCOMM Comput. Commun. Rev.*, vol. 35, p. 37–52, Apr. 2005.
[12] R. Craven, R. Beverly, and M. Allman, "A middlebox-cooperative tcp for a non end-to-end internet," SIGCOMM '14, p. 151–162, 2014.
[13] C. Reis, S. D. Gribble, T. Kohno, and N. C. Weaver, "Detecting in-flight page changes with web tripwires.," in *NSDI*, vol. 8, pp. 31–44, 2008.
[14] M. Dischinger, M. Marcon, S. Guha, P. K. Gummadi, R. Mahajan, and S. Saroiu, "Glasnost: Enabling end users to detect traffic differentiation.," in *NSDI*, pp. 405–418, 2010.
[15] C. Kreibich, N. Weaver, B. Nechaev, and V. Paxson, "Netalyzr: illuminating the edge network," IMC '10, p. 246–259, 2010.
[16] R. Sundara Raman, L.-H. Merino, K. Bock, M. Fayed, D. Levin, N. Sullivan, and L. Valenta, "Global, passive detection of connection tampering," ACM SIGCOMM '23, p. 622–636, 2023.
[17] G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, and B. Donnet, "Revealing middlebox interference with tracebox," IMC '13, p. 1–8, 2013.
[18] F. Hilal and O. Gasser, "Yarrpbox: Detecting middleboxes at internet-scale," *Proc. ACM Netw.*, vol. 1, July 2023.
[19] B. Ulukapi, A. Sperotto, and R. Holz, "Tracing Vendors: A Middlebox-Centric Study of Network Interference," in *2025 IEEE EuroS&PW*, 2025.
[20] B. Ulukapi, A. Sperotto, and R. Holz, "Towards understanding middlebox deployments in dutch ases: Impact of ip sampling size," in *ANRW '25*, p. 3, July 2025.
[21] B. Jansen, N. Kadenko, D. Broeders, M. van Eeten, K. Borgolte, and T. Fiebig, "Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions," *Government Information Quarterly*, vol. 40, no. 4, p. 101862, 2023.
[22] V. Ververis, L. Lasota, T. Ermakova, and B. Fabian, "Website blocking in the european union: Network interference from the perspective of open internet," *Policy & Internet*, vol. 16, no. 1, pp. 121–148, 2024.
[23] RIPE Network Coordination Centre, "Ripestat data api documentation," 2025. Accessed: 2025-05-12.
[24] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye, "Ip geolocation databases: unreliable?," *SIGCOMM Comput. Commun. Rev.*, vol. 41, p. 53–56, Apr. 2011.
[25] IPinfo, "Ip to company database," 2025.
[26] "Basisbeveiliging." https://basisbeveiliging.nl, 2025. Accessed: 2025-05-04.
[27] Censys, "Censys scanning and data collection," 2024.
[28] Shodan, "Shodan: The search engine for internet-connected devices," 2025.
[29] C. Raiciu, C. Paasch, S. Barre, A. Ford, M. Honda, F. Duchene, O. Bonaventure, and M. Handley, "How hard can it be? designing and implementing a deployable multipath {TCP}," in *NSDI 12*, pp. 399–412, 2012.
[30] O. Bonaventure, C. Paasch, and F. Duchene, "Tcp extensions for multipath operation with multiple addresses." RFC 8684, 2020.
[31] R. Klöti, B. Ager, V. Kotronis, G. Nomikos, and X. Dimitropoulos, "A comparative look into public ixp datasets," *SIGCOMM Comput. Commun. Rev.*, vol. 46, p. 21–29, Jan. 2016.
[32] A. Gupta, L. Vanbever, M. Shahbaz, S. P. Donovan, B. Schlinker, N. Feamster, J. Rexford, S. Shenker, R. Clark, and E. Katz-Bassett, "Sdx: A software defined internet exchange," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 551–562, 2014.
[33] F. Gont and A. Yourtchenko, "On the implementation of the tcp urgent mechanism," tech. rep., 2011.
[34] B. Du, K. Izhikevich, S. Rao, G. Akiwate, C. Testart, A. C. Snoeren, and k. claffy, "Irregularities in the internet routing registry," IMC '23, p. 104–110, 2023.