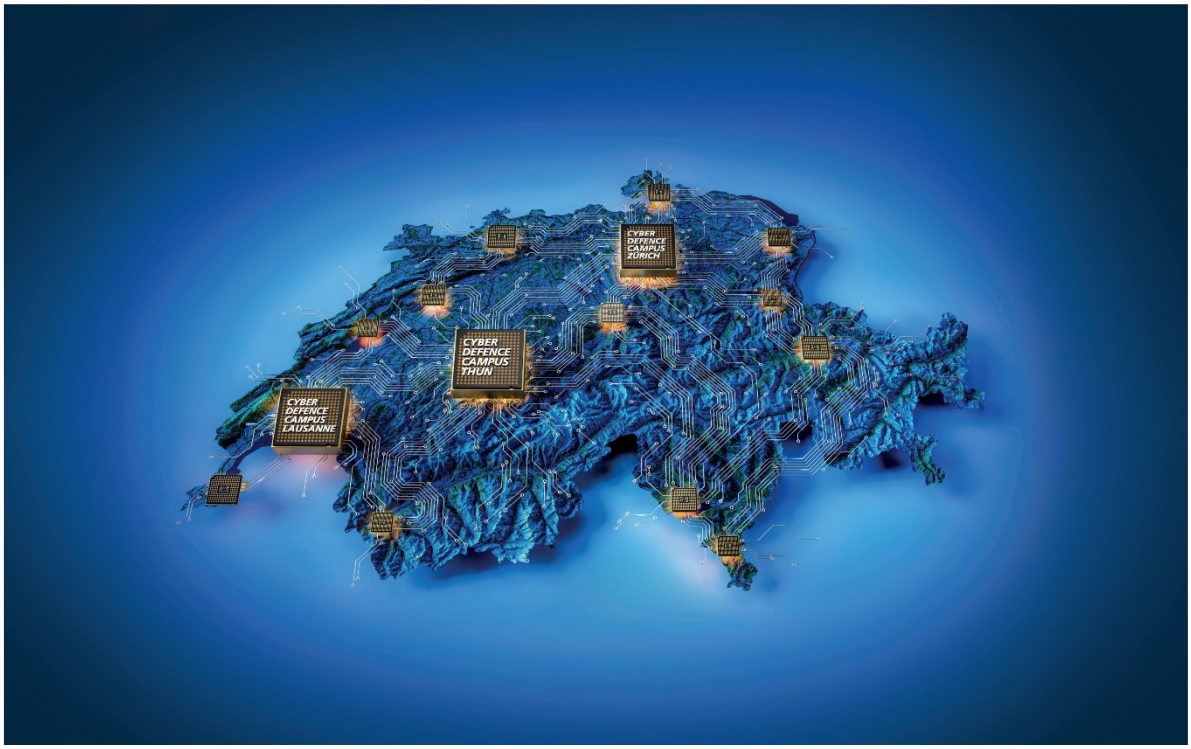
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence
Civil Protection and Sport DDPS

armasuisse
Science and Technology S+T



Lausanne, 14 May 2025

CYD Campus Technology Monitoring Review

DDoS Mitigation

Authors: Martin Sand, Valentin Mulder, Martin Burkhart

Table of contents

Executive Summary

From 2023 to 2025, the Swiss Federation was targeted by a series of DDoS (Distributed Denial of Service) attacks against multiple governmental websites. While these attacks did not massively affect the Federal Administration's operational capabilities, they raised much attention in the media. Questions surrounding these events have led to a broader interrogation of Switzerland’s general resilience against cyberattacks, specifically DDoS operations against critical infrastructure.

This report is intended for public institutions as well as private companies to help them foster DDoS resilience in Switzerland. It describes the different types of DDoS attacks along with trends in attacks, defence, and research. Many mature, ready-to-deploy DDoS mitigation solutions are available on the market, either as ISP service options, external cloud services, on-premises appliances or managed services.

Organizations have a vested interest in determining which mix of DDoS mitigation services best meets their needs depending on their business and own risk assessment. The various solutions are discussed and concluded with general recommendations.

1 Motivation

In June 2023, the Swiss Federation was targeted by a series of DDoS (Distributed Denial of Service) attacks against multiple governmental websites. These attacks were performed by the pro-Russian group “NoName057(16)” in response to decisions taken by the Parliament related to the Russian invasion of Ukraine [1]. In January 2024, “NoName057” repeated their actions due to President Zelensky’s attendance at the WEF (World Economic Forum) in Davos [2]. On the 15-16 of June 2024, the group re-iterated their operation during the Summit on Peace in Ukraine at the Bürgenstock resort [3]. In January 2025, the WEF in Davos was again attacked by the same group [4].

While these attacks did not massively affect the Federal Administration's operational capabilities, they raised much attention in the media. Questions surrounding these events have led to a broader interrogation of Switzerland’s general resilience against cyberattacks, specifically DDoS operations against critical infrastructure. As the threat of DDoS is growing both in frequency and intensity, the risk of victimization is especially felt by small businesses and public institutions. The potential damages are not limited to financial losses, but also to reputational setbacks.

A set of organizational and technical measures have already been recommended in the NCSC report on the June 2023 attacks [1]. The goal of this report is to provide a more detailed analysis of DDoS trends and mitigation solutions, preparing enterprises for deploying effective countermeasures against DDoS attacks.

2 DDoS Taxonomy

Distributed Denial of Service (DDoS) is a type of cyberattack that overwhelms the victim’s systems or network with a flood of internet traffic sent by a collection of multiple compromised or colluding machines, called a botnet. The objective might be ideological, in which case the denial-of-service may be an end in itself, e.g. the operation performed by NoName057(16) against Swiss infrastructure; otherwise, the end goal tends to be financial, where the attacker might ask the victim for a ransom in advance in exchange for not executing the attack, or use DDoS as a smokescreen to distract security teams while simultaneously performing another attack.

Since the first reported attack in 1996, where the attacker flooded an ISP’s server with malicious SYN packets (so-called “SYN-flood” attack) [5], DDoS has evolved into a wide variety of forms. While the sheer number of DDoS attack types makes categorization difficult, a common high-level way of classifying them has been as either

(1) volume-based attacks, where the victim’s bandwidth is flooded with requests, e.g. UDP floods, DNS amplifications,

(2) protocol attacks, where the victim’s server resources are exhausted, e.g. SYN floods, ping-of-death, and

(3) application-layer attacks, which targets vulnerabilities in applications, e.g. HTTP flood, slowloris [6] [7] [8].

Not all attacks fall neatly into these categories, but it provides a broad classification that is useful for determining appropriate defense mechanisms. To characterize these attacks, which are nowadays often used in unison, four dimensions need to be considered [9]:

- Exploited protocols: DDoS attacks exploit different protocols on different layers in the OSI model, e.g. ICMP, ARP (L3); TCP, UDP (L4); HTTP, DNS, NTP (L7). There is a more general distinction between L3/L4 attacks, which does not require the defender to consider the payload, and L7 attacks, which are harder to detect.
- Target resource consumption: A DDoS attack can target either the victim's resources, e.g. CPU, memory, I/O bandwidth, critical links where the attack could create a bottleneck, or even their financial capabilities (so-called Denial-of-Sustainability attacks).
- Attack capacity: A DDoS attack can be either volumetric, where the attack vector is a large amount of traffic, or non-volumetric, where the attack vector will be a small number of malicious packets.
- Temporal dimension: DDoS attacks can be sent either as a continuous flow, which is common for volumetric attacks, periodically, as pulse-waves or stealthily. The temporal dimension is more detached from the other traits since the same type of attack can be deployed in multiple modes of operations; however, some attacks do require a specific temporal mode of operation to be effective.

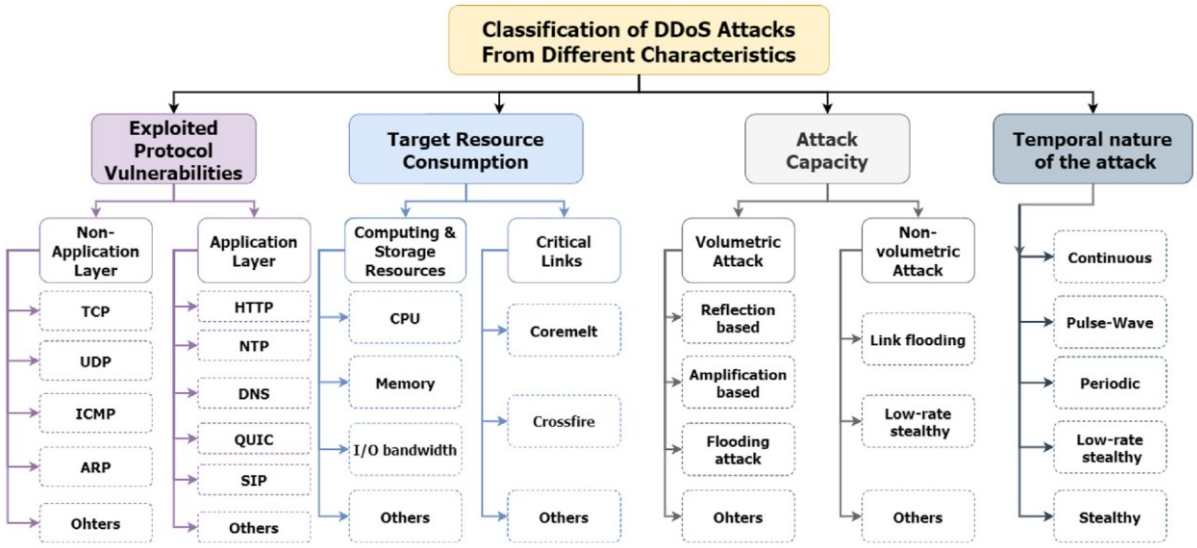


Figure 1 : Taxonomy which allows to characterize each type of DDoS attack, e.g. a SYN flood exploits TCP protocol, targets memory and is a volumetric attack [9].

3 DDoS Trends

For over 20 years now, DDoS attacks have remained one of the main cyberthreats on the Internet, both in terms of impact and prevalence. This section outlines recent attacks and defense trends.

Attack Trends

Continued developments and innovations of networking technologies open new ways for attackers to perform denials-of-service by introducing new attack surfaces, e.g. the current rise in number of unsecured IoT devices leading to larger and larger botnets, such as the Mirai botnet [10]. Attackers also constantly adapt to the newly implemented defense systems, e.g. using adversarial learning techniques, and exploiting new vulnerabilities in application layer protocols, such as the HTTP/2 Rapid Reset [9] [12] [10].

Over the past years, DDoS operations have grown both in volume and complexity, using multiple attack vectors to conduct their operations, with massive attacks exceeding 5 Tbps [13]. There has also been an increasing shift towards application-layer attacks, which are harder to detect than lower-layer attacks because they better mimic legitimate traffic. Furthermore, there has been increasing use of mitigation bypass techniques, such as header randomization or CAPTCHA solving [14].

According to the 2025 Global Threat Analysis Report published by Radware [15], DDoS attacks targeting networks and websites have increased significantly during the last years. Web DDoS attacks have increased almost 550% year-over-year since 2023. Applications were attacked with increasing sophistication, using, e.g., HTTP/2 Rapid Reset and Continuation Flow attacks. Also, the average volume of network DDoS attacks has risen by 120% from 2023 to 2024. An unprecedented number of DNS query flood attacks was visible, having increased by 87% since 2023. Telecommunications, finance, and technology sectors were the main targets, followed by transportation, e-commerce, and government. The rise of DDoS-for-hire platforms is a new trend, lowering the technical entry barrier for attackers.

A trend report by Akamai emphasizes the point that sophistication overshadows size [16]. While older attacks mainly grew in scale and volume, modern attacks have evolved to be more sophisticated: Multiple destinations, multiple attack vectors and AI-enabled tools are used to systematically check defenses.

Defence Trends

Malicious actors continue to find new vulnerabilities to exploit for DDoS attacks. Depending on the severity, few network packets may be enough to stop a vulnerable server completely. Therefore, security analyses of protocols and products will remain relevant for the years to come [9]. However, this task is beyond the scope of the average SME company. Here, companies must rely on research done in the security industry and academia.

Programmable networks have allowed for more DDoS detection and mitigation on the network side, through the deployment of software-defined networking (SDN) and network function virtualization (NFV). Programmable switches have increased the capabilities of DDoS defense systems in terms of throughput, real-time detection and attack vector coverage.

As manual rule creation is becoming increasingly obsolete in the face of modern complex DDoS attacks and as computing power keeps growing, using machine-learning to detect and

deter incoming attacks automatically has improved flexibility and accuracy of DDoS defense systems [9].

4 DDoS Mitigation Solutions

'DDoS mitigation' commonly refers to any process designed to protect a designated network, server or application from DDoS attacks. Thus, traditional solutions such as firewalls, Intrusion Prevention Systems (IPS) or Web Application Firewalls (WAF) qualify as a form of DDoS mitigation, notably with pre-established indicators of compromise (IoC) which can help identify malicious IP ranges. However, these have been shown to be insufficient against modern DDoS attacks [17] [18], and can even end up as bottlenecks in the network.

Since many organizations lack the financial means or the in-house capabilities to deploy scalable high-capacity networks with proprietary mitigation techniques and organizational measures to prevent DDoS attacks, they tend to rely on third-party actors to protect their assets. Therefore, this report will seek to provide a framework for the procurement of off-the-shelf DDoS mitigation solutions.

This section covers the following categories of established mitigation technologies (see Figure 2 for an illustration):

- On-premises anti-DDoS appliances
- ISP and third-party scrubbing centers
- Web Application Firewalls (WAF/WAAP)
- Content Delivery Networks (CDN)
- Remote Triggered Blackhole (RTBH) Filtering on edge routers

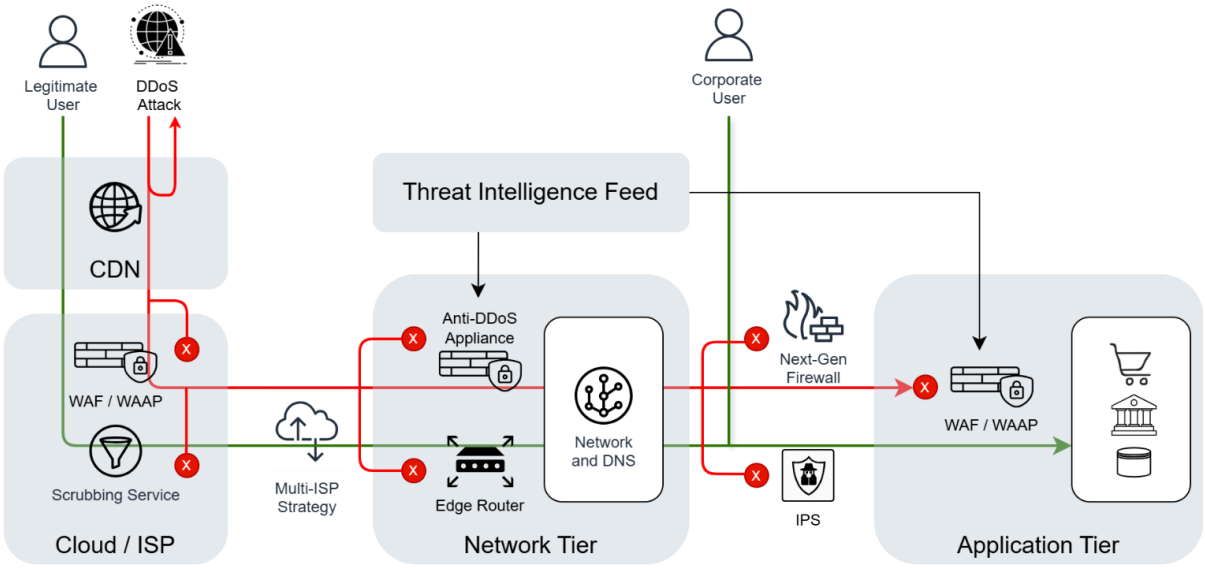


Figure 2: Overview of different DDoS mitigation solutions on the network and application tier. Most solutions can be deployed on-premises or in the cloud.

4.1 On-Premises Anti-DDoS Appliances

Anti-DDoS appliances are specialized hardware with high capacity and the ability to detect DDoS patterns. These can be installed in a network for better monitoring and to drop malicious traffic. These solutions provide on-premises and immediate attack detection and mitigation. Furthermore, by not delegating the monitoring to an external service provider, it allows for more confidentiality and control over one's assets, e.g. not sharing SSL/TLS keys for inspecting HTTPS traffic. However, on-premises hardware can be expensive, difficult to scale, requires maintenance and does not necessarily have the capacity to sustain modern volumetric attacks on its own [19].

Pros	Cons
+ Immediate mitigation + Direct control over the equipment + Traffic confidentiality + L3 protection	- Low capacity - Low scalability - In-house skills needed to maintain and configure - No L7 protection

4.2 ISP and Third-Party Scrubbing Centers

An alternative to on-premises DDoS protection is cloud-based mitigation. In this case, the clients divert their traffic to a scrubbing center hosted by an external service provider, which filters out malicious traffic and sends back legitimate traffic to the client's network through Generic Routing Encapsulation (GRE) tunneling [9] [19]. This solution is generally limited to network/transport layer (L3) threats.

There are two deployment methods: *on-demand* and *always-on*. The on-demand solution requires a notice from the client, either manual or automatic[1], that their network is reaching maximum capacity, after which the traffic is re-routed through DNS or BGP to the service provider's scrubbing centers. This solution is less expensive, but introduces latency in the mitigation response, since the DDoS attack needs to be detected before being deviated: this means that an attack has the potential to inflict many minutes of down-time before being diverted. Furthermore, this makes the system vulnerable to new types of DDoS techniques, such as the "Yo-Yo" attack: this type of attack exploits the business model of cloud service providers by sending high levels of traffic to the client, thus triggering the autoscaling with the incurring costs, then pausing for a while to let the system scale down, and then sending it again, and repeating the process over and over, causing costs to ramp up for the victim. This attack does not seek to bring down the victim's system *per se*, but to make its maintenance financially untenable [20].

[1] Automatic detection of malicious traffic requires flow monitoring on the client's side, and some service providers offer special appliances for this purpose.

As the name implies, the always-on solution provides 24/7 protection with no responsibility on the client's side. This offers an immediate response to DDoS attacks, but since all the traffic is routed through the service provider's scrubbing center, it can add latency for legitimate applications [21].

Scrubbing centers are used by ISPs to provide their clients with "clean pipe" solutions, which pass all the traffic through their scrubbers before sending it to their clients. Therefore, it is recommended that organizations check whether their current ISP is providing anti-DDoS solutions, which offers easy implementation and quick response time since the traffic is already being routed through their network. However, ISP scrubbing centers tend to have a lower bandwidth than third-party scrubbers [22].

If an organization has a low tolerance for allowable downtime, a multi-ISP strategy could be followed. Quickly switching the ISP network and IP ranges might prove to be an efficient countermeasure, depending on the attack type. Yet, this adds complexity and costs.

Cloud-based scrubbing center	
+ High bandwidth + High scalability + No in-house skills needed to maintain and configure + L3 protection - No L7 protection	
ISP	**Third-party**
+ Easy implementation (if already contracted with the ISP)	+ Higher bandwidth
On-demand	**Always-on**
+ Less costly - Response latency	+ Immediate mitigation - More costly - General latency

4.3 Web Application and API Protection (WAF/WAAP)

Most DDoS mitigation solutions focus on capacity and network layer (L3) inspections but lack application layer (L7) monitoring. Web Application Firewalls (WAF) serve as reverse-proxies that protect web applications from malicious traffic by monitoring and blocking HTTP/S

requests. WAFs with specific API protection features are referred to by the term WAAP (Web Application and API Protection).

Most WAFs also have basic load-balancing features and integrate threat intelligence feeds with collections of suspicious IP addresses that could be blocked (e.g. botnet clients, TOR exit nodes, spammers). A notable benefit of a WAF is the speed at which policies can be modified in the advent of an attack [23], e.g. blocking requests with a specific user-agent [1]. Many WAFs provide machine-learning based anomaly detection and can react automatically to suspicious changes in traffic characteristics. Some WAAP solutions can enforce proper authorization of requests, e.g., by enforcing valid API keys or access tokens. This provides strong protection against application layer DDoS attacks, as malicious requests are usually unauthenticated. Moreover, WAFs in reverse-proxy mode can terminate TLS connections, allowing them to offload the expensive TLS handshakes from applications. However, WAF/WAAP solutions are limited to HTTP/S traffic, so other protocols, such as SMTP or VPN, need alternative protection [24].

WAF solutions can be deployed either as on-premises appliances or as a cloud-based service. On-premises solutions are useful if the organization does not allow data processing in the cloud. Also, if there is no cloud data center in proximity to the web server, it can help mitigate latency. They provide more agency on the client's side, as they allow for unlimited and customizable policies. However, maintaining an on-premises WAF and defining relevant policies necessitate in-house expertise and monitoring. Furthermore, in terms of costs, acquiring the WAF hardware and license can be expensive and difficult to scale [25].

Cloud-based WAFs provides a lot of convenience for the client, notably with pre-configured policies, less maintenance and high scalability. However, it limits the control the client has over its own protection and requires trusting the service provider with the monitoring of the application layer (L7) traffic [23]. Furthermore, costs can ramp up, notably for high-traffic applications [25].

<table>
<tr><th colspan="2">WAF / WAAP</th></tr>
<tr><td colspan="2">+ L7 protection

+ Basic L3 protection (load-balancing, IP filtering)

- Only covers web traffic</td></tr>
<tr><th>On-premises WAF / WAAP</th><th>Cloud WAF / WAAP</th></tr>
<tr><td>+ Traffic confidentiality

+ Less latency

- Low scalability

- Attack reaches the company network

- In-house skills needed to maintain and configure</td><td>+ Convenience

+ High scalability

+ Attack may be stopped before it reaches the company network

- HTTP traffic monitored by third-party</td></tr>
</table>

4.4 Content Delivery Networks (CDN)

Some service providers offer adjacent functionalities to their cloud-based WAF. A notable example is the Content Delivery Network (CDN): a geographically distributed group of servers will cache copies of the web server's content on edge servers, also called "points-of-presence" (PoPs), to which DNS servers will redirect traffic based on geographical proximity. These networks help reduce latency by bringing the content closer to the users and perform load balancing by decentralizing access to the content [26].

Regarding DDoS mitigation, CDNs provide the highest capacity among the proposed market solutions [22], automatically drop network layer (L3) and transport layer (L4) traffic, instantly mitigating L3/L4 DDoS attacks, and can be coupled with cloud WAFs to inspect application layer (L7) traffic [27].

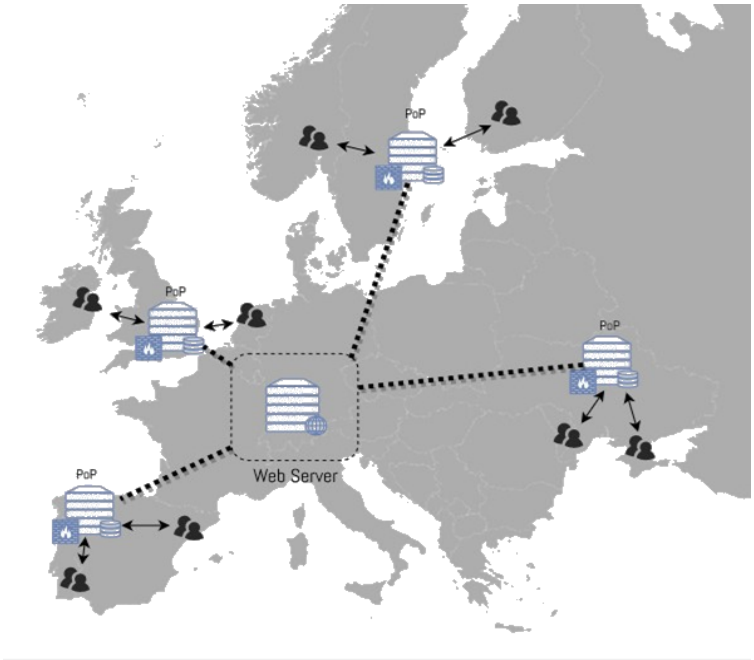


Figure 3: In a CDN network, the main server, here located in Switzerland, is replicated to multiple PoPs in Europe for quicker access and better load-balancing.

4.5 Remote Triggered Blackhole (RTBH) Filtering

As a last resort, organizations and ISPs may blackhole traffic by re-routing it to a reserved address space. This method has the advantage of being quick to implement and provide immediate relief for attacked networks [28]. However, its success relies on the availability of IP address patterns, e.g., a target server IP address. All traffic flowing to the target is then dropped at the network edge, preventing the internal network from collapsing. This may allow other services to be still accessible. However, the targeted server is essentially given up, because all users, also legitimate ones, are locked out. Finding specific patterns based on the source IP addresses may be difficult.

Organizations need to perform a cost-effectiveness calculation to determine whether the targeted assets are worth defending. If temporary unavailability of the attacked services is bearable, remote-triggered blackhole filtering may be the best solution for the benefit of other services in the client's network.

4.6 Route Control and Source Authentication (SCION)

In today's internet, DDoS attacks profit from a fundamental lack of security in routing protocols. Service providers trying to defend against these attacks fight an uphill battle, not being able to fix problems inherent in network protocols. Hence researchers argue that internet routing needs major revision. A prominent example is SCION, an internet architecture that is being actively researched at ETH Zurich and is rolled out by an increasing number of service providers.

In its DDoS incident report from June 2023, the National Cyber Security Center (NCSC) outlined the mitigation capabilities of the SCION Internet architecture against DDoS attacks [1]. In March 2025, they followed up with a technology review on SCION (only available in German) [29]. Continuously developed since 2009 by researchers at ETH Zürich, SCION aims to improve upon the current IP and BGP-based Internet architecture by providing "route control, failure isolation and explicit trust information for end-to-end communication" [30]. Additionally, SCION possesses a range of built-in properties that help to mitigate DDoS attacks:

Route Control: Under the current paradigm, the path taken by Internet traffic is dictated by the network provider, not the user. The former relies on BGP for inter-domain routing decisions. Unfortunately, this protocol works on the assumption that every edge router advertising its autonomous system's (AS) IP range is reliable. This has led to incidents affecting the global Internet, whether it be BGP route leaks, where misconfigurations have caused traffic to be redirected through certain AS-es, often causing global slow-downs, or BGP hijacks, where incorrect routes are leaked maliciously, often to prevent access to certain AS-es [31]. SCION serves as an alternative to BGP, allowing end hosts to control the path they want their traffic to pass through and isolate the routing process to trusted AS-es, ensuring that no accident or malicious entity will interfere with its routing process [30].

IP Spoofing Prevention: IP spoofing is commonly used by DDoS operations, either for masking the identity of the compromised machines or for launching reflection/amplification attacks. Standard IP packets only carry information regarding their routes in their lifetime field (IPv4: time-to-live/IPv6: hop limit); therefore, there is no way of assessing whether the source IP address is consistent with the path to the destination. On the other hand, in the SCION architecture, since path information is recorded in the SCION packet, the source address must be along the path in the packet [32].

Path Reservation: In addition, SCION offers the possibility of path reservation, where a host can retain some paths and use them for sources that are already authenticated. This guarantees bandwidth for a set of important legitimate users [32].

While SCION is still actively researched, commercial SCION-based solutions are offered by an increasing number of companies and Internet Service Providers (ISPs), including the Swiss ISPs Swisscom, Sunrise, Init7 and SWITCH [33]. Recently, also international providers have started offering SCION services. Therefore, the Cyber-Defence Campus was able to secure the connection of the Swiss team during the LockedShields exercise in 2024 all the way from Switzerland to Tallinn [34]. LockedShields is the world's largest live-fire cyber-defense

exercise, organized by the NATO Cooperative Cyber Defence Center of Excellence (CCDCoE).

5 General Recommendations

There is no one-size-fits-all approach to DDoS mitigation. Organizations are expected to conduct their own risk assessment to determine how DDoS attacks may impact the functioning of their business. This implies understanding the value of their assets, the costs of a successful DDoS attack on these assets, their current protection against DDoS and the attack trends against the organization [36]. Usually, the maximum allowable downtime is not the same for all services. Some of them may tolerate a downtime of hours or even days, while others must be online continuously. This evaluation helps determine adequate countermeasures for each organization. Business continuity planning and incident response must include successful DDoS attack scenarios along with tested plans on how to proceed.

Many organizations have decided to outsource their DDoS mitigation to cloud-based services or their ISPs, allowing them to offload the need for in-house expertise onto the service provider. A service provider's client list may help find a suitable provider, notably in size, sector, or specialization. Performing stress tests once or regularly helps identifying weak spots. Larger organizations, e.g., government organizations or ISPs, may have an interest in building their own scrubbing centers to avoid unnecessary costs, to mitigate latency and to maintain full control over the incoming traffic.

All organizations, even if they are contracted with a cloud provider, will have to accept a residual risk of a DDoS attack reaching their network: an attacker may find a way to bypass redirection protocols (DNS or BGP) or rely on short attacks to disrupt the client's network before mitigation becomes effective. It may therefore be beneficial for companies to somewhat overprovisioning their network and to maintain some degree of local DDoS protection, e.g. WAFs or specialized appliances.

The Swiss NCSC maintains a list of specific measures to prepare for and counter DDoS attacks. We recommend companies to use these pages as checklists:

- Measures to counter DDoS attacks
- DDoS attack - what next?

6 References

[1] «Downstream incident analysis DDoS attacks by NoName057(16),» 30 October 2023. [Online]. Available: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html. [Zugriff am 12 July 2024].

[2] «Several Federal Administration websites disrupted temporarily by DDoS attack,» www.admin.ch, 17 January 2024. [Online]. Available: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-99736.html. [Zugriff am 12 July 2024].

[3] «Summit on Peace in Ukraine: first NCSC report on Cyber Situation Network,» www.admin.ch, 20 June 2024. [Online]. Available: https://www.vbs.admin.ch/en/nsb?id=101528. [Zugriff am 12 July 2024].

[4] NCSC, «Expected DDoS attacks have begun,» 21 1 2025. [Online]. Available: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/ddos-2024-01-25.html. [Zugriff am 15 4 2025].

[5] «Five Most Famous DDoS Attacks and Then Some,» A10, 21 January 2022. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/. [Zugriff am 2024 July 12].

[6] «DDoS Attacks,» Imperva, [Online]. Available: https://www.imperva.com/learn/ddos/ddos-attacks/. [Zugriff am 15 July 2024].

[7] «What is a DDoS attack?,» Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Zugriff am 15 July 2024].

[8] C. Kime, «Complete Guide to the Types of DDoS Attacks,» eSecurity Planet, 19 December 2022. [Online]. Available: https://www.esecurityplanet.com/networks/types-of-ddos-attacks/. [Zugriff am 15 July 2024].

[9] Q. Li, H. He, R. Li, J. Lv, Y. Z. L. Ma, Y. Han und Y. Jiang, «A Comprehensive Survey on DDos Defense Systems: New Trends and Challenges,» *Computer Networks,* Bd. 233, Nr. 109895, 2023.

[10] «What is the Mirai Botnet?,» Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. [Zugriff am 12 July 2024].

[11] «What is the Mirai Botnet?,» Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. [Zugriff am 2 September 2024].

[12] «HTTP/2 Rapid Reset: deconstructing the record-breaking attack,» Cloudflare, 10 October 2023. [Online]. Available: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack. [Zugriff am 12 July 2024].

[13] «Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4,» Cloudflare, [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/.

[14] E. Arazi, «The 3 Trends Reshaping the DDoS Threat Landscape in 2023,» Radware, 24 April 2024. [Online]. Available: https://www.radware.com/blog/ddos-protection/2024/04/the-3-trends-reshaping-the-ddos-threat-landscape-in-2023/. [Zugriff am 12 July 2024].

[15] «Radware Threat Report Summary 2025,» Radware, 2025. [Online]. Available: https://www.radware.com/threat-analysis-report/. [Zugriff am 14 April 2025].

[16] Akamai, «DDoS Attack Trends in 2024 Signify That Sophistication Overshadows Size,» [Online]. Available: https://www.akamai.com/blog/security/ddos-attack-trends-2024-signify-sophistication-overshadows-size. [Zugriff am 15 4 2025].

[17] «WHY IPS AND FIREWALLS ARE NOT ANTI-DDOS SOLUTIONS?,» NSFocus, 24 March 2023. [Online]. Available: https://nsfocusglobal.com/why-ips-and-firewalls-are-not-anti-ddos-solutions/. [Zugriff am 12 July 2024].

[18] «On-Premise, Cloud or Hybrid? Approaches to Mitigate DDoS Attacks,» Radware, [Online]. Available: https://www.radware.com/getattachment/106d1801-ba4f-4339-b42e-71d781efe6b6/f23ad5ad-4b7f-4841-ab95-68d37e5686f5.pdf.aspx. [Zugriff am 12 July 2024].

[19] «DDoS Mitigation Technologies,» Rising Tide Cybersecurity, 19 June 2021. [Online]. Available: https://www.youtube.com/watch?v=hbNNneCThQ0. [Zugriff am 12 June 2024].

[20] A. Y. H. H. Meraj Mostam Kashi, «Mitigating Yo-Yo attacks on cloud auto-scaling,» in *2022 14th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2022.

[21] «Beyond on-demand for DDoS defense,» Cloudflare, [Online]. Available: https://cf-assets.www.cloudflare.com/slt3lc6tev37/5FOOwC3kns916rv8zQMgjJ/e04ec2387f8de10572e697897ffb208a/Always-on-vs-on-demand-DDoS-Protection.pdf. [Zugriff am 12 July 2024].

[22] M. Smith, «DDoS Mitigation Techniques and Technologies Part 2: ISP Scrubbing Centers,» Vercara, 25 January 2023. [Online]. Available: https://vercara.com/resources/ddos-mitigation-technologies-part-2-isp-scrubbing-centers. [Zugriff am 12 July 2024].

[23] «What is a WAF? | Web Application Firewall explained,» Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/. [Zugriff am 12 July 2024].

[24] M. Smith, «DDoS Mitigation Technologies Part 3: Third-Party Solutions,» Vercara, 1 February 2023. [Online]. Available: https://vercara.com/resources/ddos-mitigation-technologies-part-3-third-party-solutions. [Zugriff am 12 July 2024].

[25] «Cloud WAF vs. On-premises WAF: Which Option to Choose?,» Infopulse, 10 October 2023. [Online]. Available: https://www.infopulse.com/blog/cloud-waf-on-premises-waf. [Zugriff am 12 July 2024].

[26] «What Is a CDN (Content Delivery Network)?,» Akamai, [Online]. Available: https://www.akamai.com/glossary/what-is-a-cdn. [Zugriff am 12 July 2024].

[27] «What Is a DDoS Attack?,» Akamai, [Online]. Available: https://www.akamai.com/glossary/what-is-ddos. [Zugriff am 12 July 2024].

[28] «What Is Blackhole Routing?,» Akamai, [Online]. Available: https://www.akamai.com/glossary/what-is-blackhole-routing. [Zugriff am 15 July 2024].

[29] NCSC, «Technologiebetrachtung SCION,» 18 3 2025. [Online]. Available: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/technologiebetrachtungen/Technologiebetrachtung-SCION-DE.pdf.download.pdf/Technologiebetrachtung-SCION-DE.pdf. [Zugriff am 16 04 2025].

[30] «SCION Architecture: SCION Internet Architecture,» Network Security Group ETH Zürich, [Online]. Available: https://scion-architecture.net/. [Zugriff am 4 September 2024].

[31] D. Madory, «A Brief History of the Internet’s Biggest BGP Incidents,» Kentik, 6 June 2023. [Online]. Available: https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/. [Zugriff am 4 September 2024].

[32] Y.-C. Hu, «Next-generation DDoS defense with SCION,» 20 October 2023. [Online]. Available: https://www.youtube.com/watch?v=-JeEppbCZTw. [Zugriff am 6 September 2024].

[33] SCION Association, «SCION Providers Today,» 2025. [Online]. Available: https://www.scion.org/business/#providers.

[34] A. Thäler, «Swiss Team uses SCION to connect to Estonia during Cyber-Defense Exercise,» armasuisse, 28 June 2024. [Online]. Available: https://www.ar.admin.ch/en/cyd-campus-scion-en. [Zugriff am 6 Spetember 2024].

[35] «Remotely Triggered Black Hole Filtering in IP Version 6 for Cisco IOS, Cisco IOS XE, and Cisco IOS XR Software,» CISCO, [Online]. Available: https://sec.cloudapps.cisco.com/security/center/resources/ipv6_remotely_triggered_black_hole. [Zugriff am 11 September 2024].

[36] M. Smith, «DDoS Mitigation Technologies Part 5: Create Your Plan,» Vercara, 15 February 2023. [Online]. Available: https://vercara.com/resources/ddos-mitigation-technologies-part-5-create-your-plan. [Zugriff am 12 July 2024].

[37] «DDoS Attack Protection: A Complete Guide for Customers in 2023,» DDoS-Guard, 14 February 2023. [Online]. Available: https://ddos-guard.net/en/blog/ddos-protection-guide-for-customers. [Zugriff am 12 July 2024].

[38] «DDoS Mitigation: The Definitive Buyer's Guide,» Imperva, [Online]. Available: https://www.imperva.com/learn/ddos/ddos-mitigation-services/. [Zugriff am 12 July 2024].

[39] «Applications,» SCIONLab, [Online]. Available: https://docs.scionlab.org/content/apps/. [Zugriff am 6 September 2024].

[40] A. S. Mattijs Jonker, «Measuring exposure in DDoS protection services,» in *2017 13th International Conference on Network and Service Management (CNSM)*, 2017.

[41] S. W. Teresa Walsh, «Navigating Record-Breaking DDoS Attacks,» RSAConference, 24 July 2024. [Online]. Available: https://www.rsaconference.com/library/webcast/170-navigating-record-breaking-ddos-attacks. [Zugriff am 8 August 2024].

[42] «The Imperva Global DDoS Threat Landscape Report 2023,» Imperva, 2023. [Online]. Available: https://www.imperva.com/resources/reports/the-imperva-global-ddos-threat-landscape-report-2023.pdf. [Zugriff am 12 July 2024].