Case Study

A Complete Guide for Telecom DDoS Mitigation

Contents

DDoS Attack Landscape

DDoS is among the most frequently observed attacks and remains persistent. The simplicity of executing DDoS has led to sustained growth in attack scale, accompanied by continuous evolution of attack techniques.

According to the Verizon Data Breach Investigations Report (DBIR), since 2018, the median size of DDoS attacks has increased by 200 percent in bps (bytes per second), while upper tier attacks have recorded increases exceeding 1,000 percent.

In 2025, a DDoS attack against a Japanese telecommunications provider caused service disruptions across websites and mobile payment services for approximately 11 hours, affecting more than 90 million users. Another DDoS attack targeted a Russia-based telco, resulting in service delays that impacted 44 million users.

As such, DDoS attacks can be especially damaging to telecommunications providers with the large number of users. These organizations typically implement systematic response frameworks, but DDoS-related incidents continue to grow every year. Security leaders have been seeking more practical and effective mitigation strategies.

This case study examines the major DDoS attack types, the common mitigation approaches employed by telecommunications providers, and how AhnLab DPX can effectively address ever-evolving DDoS attacks.

What is DDoS?

A DDoS attack compromises multiple devices into a botnet and simultaneously directs traffic at a target server to cause service disruption.

DDoS attacks vary depending on attack techniques and traffic volume.

DDoS Attack Types

First, let's explore types of DDoS attacks.

Attack Techniques	Description
DoS (Denial of Service)	▪ The most basic form of attack ▪ An attack from a single client toward a server (1:1)
DDoS (Distributed Denial of Service)	▪ A simultaneous attack through a botnet (infected devices) ▪ An attack from multiple clients toward a single server (N:1)
DRDoS (Distributed Reflection DoS)	▪ A UDP attack using a reflector ▪ Causing ultra high volume, Tbps attacks
APDoS (Advanced Persistent DoS)	▪ DDoS attacks used to facilitate APT attacks ▪ Diverting admin's attention prior to launching APTs ▪ Also referred to as multi-vector DDoS attacks
Ransom DDoS (DDoS Extortion)	▪ Financially motivated DDoS attacks ▪ Demonstrative attacks to show off attack capability
DDoS as a Service	▪ A third-party adversary executing DDoS for its client ▪ Pricing varies depending on attack scale and methods

Table 1. DDoS attack techniques

DDoS attacks can also be classified based on the volume and characteristics of the traffic.

Volumetric DDoS

TCP flooding: TCP flooding abuses multiple components of the TCP protocol, primarily through SYN and ACK packets. Attackers also use TCP-based techniques such as XMAS and NULL floods.

UDP flooding: UDP flooding exploits the disconnected and unreliable nature of the UDP protocol, which makes such attacks relatively easy to execute. Attacks involving protocols such as Memcached, SNMP, CHARGEN, DNS, and NTP are generally categorized as UDP flooding.

SSL flooding: SSL flooding is a high-volume DDoS attack that exploits SSL or TLS. Due to the characteristics of SSL and TLS, it is challenging to generate large-scale traffic.

HTTP flooding: A DDoS attack that abuses the HTTP protocol. Attacks can be carried out based on specific HTTP request methods, such as GET and POST.

Fragmentation flooding: A DDoS attack executed by exploiting IP packet fragmentation mechanisms.

How is a DDoS mitigation solution deployed?

DDoS mitigation solutions can be deployed either inline or out-of-path. Inline deployment offers greater responsiveness, while out-of-path deployment provides higher operational stability.

Low-volume DDoS

Low-volume precision attack: Low-volume precision attacks bypass threshold-based DDoS mitigation by persisting connections or gradually exhausting server resources. Adversaries commonly use exhaustion attacks which typically require authentication-based mitigation.

Abnormal protocol: This attack violates protocol specifications and exploit vulnerabilities in target systems. Effective mitigation requires an integrated approach combining web application firewall (WAF), intrusion prevention systems (IPS), and DDoS mitigation solutions. Common attack types include Ping of Death, TearDrop, Slowloris, Slow Read, LAND, RUDY, and Smurf.

Solution Deployment

DDoS mitigation solutions support two deployment architectures: inline and out-of-path.

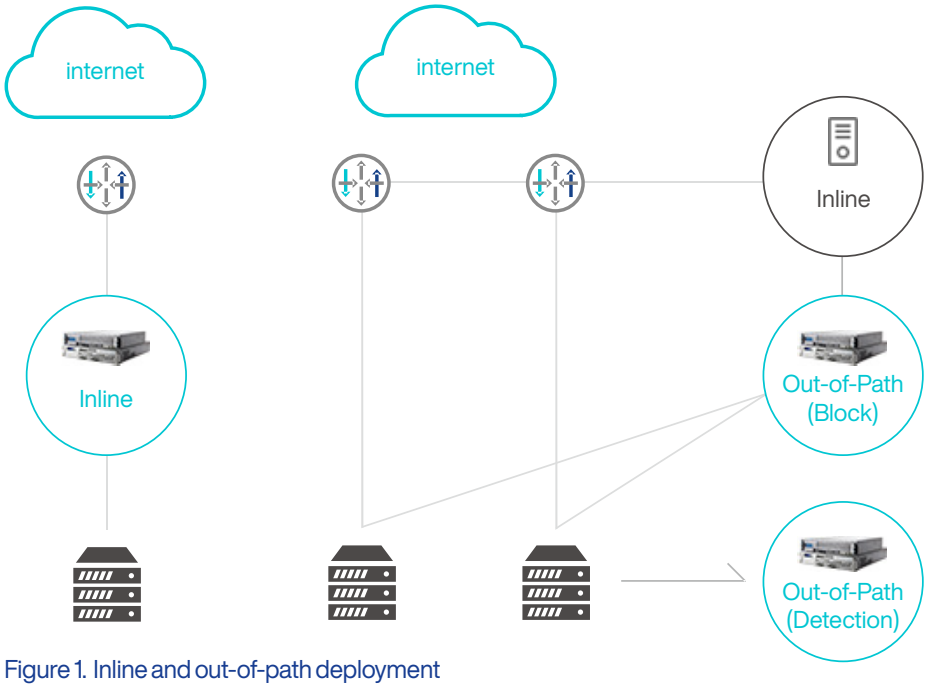

Figure 1. Inline and out-of-path deployment

The table compares the key characteristics of the two deployment models.

Category	Inline	Out-of-Path
# of Appliances	1 (detection & response)	2 (Detector: detection & Guard: block)
Difficulty	Easy	Difficult
Speed	Very Fast	Fast
Industry	Public institution, finance, and education	ISP and IDC

Table 2. Inline and out-of-path comparison

Method 1: Threshold-based rule

A technique that detects and mitigates DDoS attacks when traffic exceeds predefined thresholds. This approach carries the risk of blocking legitimate users and is less effective against low-volume attacks.

Advances in DDoS mitigation solutions have reduced the differences between inline and out-of-path deployment models in terms of attack detection and response. Despite these improvements, fundamental architectural differences remain a key factor in deployment decisions across different industries and operational environments.

DDoS Mitigation Methods

Effective DDoS mitigation requires a multi-layered approach.

Step 1: Threshold rule-based mitigation

All DDoS mitigation solutions deliver threshold-based rules. These rules detect and respond to DDoS attacks by counting packets and identifying traffic that exceeds predefined thresholds. Rules are classified into DoS and DDoS rules.

DoS rules measure packet volume based on a single source IP address. Since excessive traffic originates from a single IP, it can be easily blocked or isolated with minimal risk.

DDoS rules detect attacks by measuring traffic volume from multiple source IPs. However, similar traffic patterns may appear during certain events, which means that a holistic prevention may deny service for legitimate users. To mitigate this risk, DDoS solutions apply additional validation mechanisms, such as authentication or QoS (Quality of Service).

Category	DoS Threshold Rules	DDoS Threshold Rules
Measure	Volume of packets entering the protected target from a single source IP	Volume of packets entering the protected target from multiple source IPs
Mitigation	Blocking, Isolation	Authentication, QoS, Isolation
Example	DoS_TCP_SYN: 500 pkts/sec	DDoS_UDP: 10,000 pkts/2 sec
Description	Traffic exceeding 500 TCP SYN packets per second from a single source IP	Traffic exceeding 10,000 UDP packets within 2 seconds from multiple source IPs
Unit	PPS(Packet Per Second) / BPS(Bit Per Second) / CPS(Connection Per Second)	

Table 3. Threshold rules for DoS and DDoS

Our DDoS mitigation solution, AhnLab DPX, provides four types of threshold-based rules, comprising approximately 60 predefined rules, along with support for user-defined threshold-based rules.

※ Note: Threshold rules effectively mitigate general large-scale volumetric attacks. However, they are less effective against low-volume precision attacks and abnormal protocol-based attacks.

Method 2: Authentication

This approach mitigates DDoS attacks by using authentication mechanisms to identify bot-driven traffic. Given that most DDoS attacks are executed by automated bots, it is an effective mitigation strategy.

Step 2: Authentication-based mitigation

Threshold-based mitigation is a common feature of DDoS mitigation solutions and can typically be operated with relatively low complexity. However, a substantial number of real-world DDoS attacks bypass threshold detection, making authentication-based mitigation essential for powerful response.

Authentication-based mitigation addresses automated and bot-driven attacks by validating behaviors through authentication mechanisms. Because adversaries rely on automated bots rather than manual execution, this approach counters a broad range of DDoS patterns. Even in low-volume attack scenarios, authentication mechanisms identify bot-generated traffic and mitigate attacks.

Here, authentication leverages the characteristics of the TCP and HTTP protocols for defense. AhnLab DPX provides six authentication mechanisms, consisting of three TCP and HTTP methods, respectively. These mechanisms are widely recognized as standard DDoS mitigation techniques.

For TCP authentication, the solution responds to an initial SYN packet with a SYN ACK containing a cookie. It then verifies whether the client returns an ACK that includes the same cookie. It also supports an alternative method using RST packets. For HTTP authentication, the solution triggers HTTP 302 redirection and verifies whether the client correctly processes it.

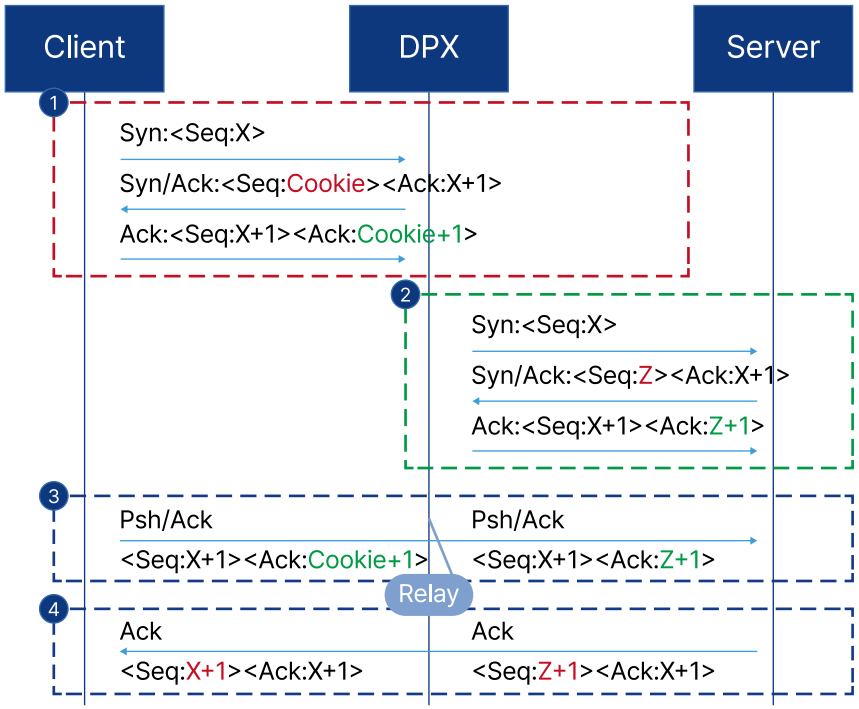

Figure 2. TCP Authentication

Effectiveness of Authentication

Authentication mechanisms are effective in countering low-volume and high-volume DDoS campaigns, including brute-force attacks.

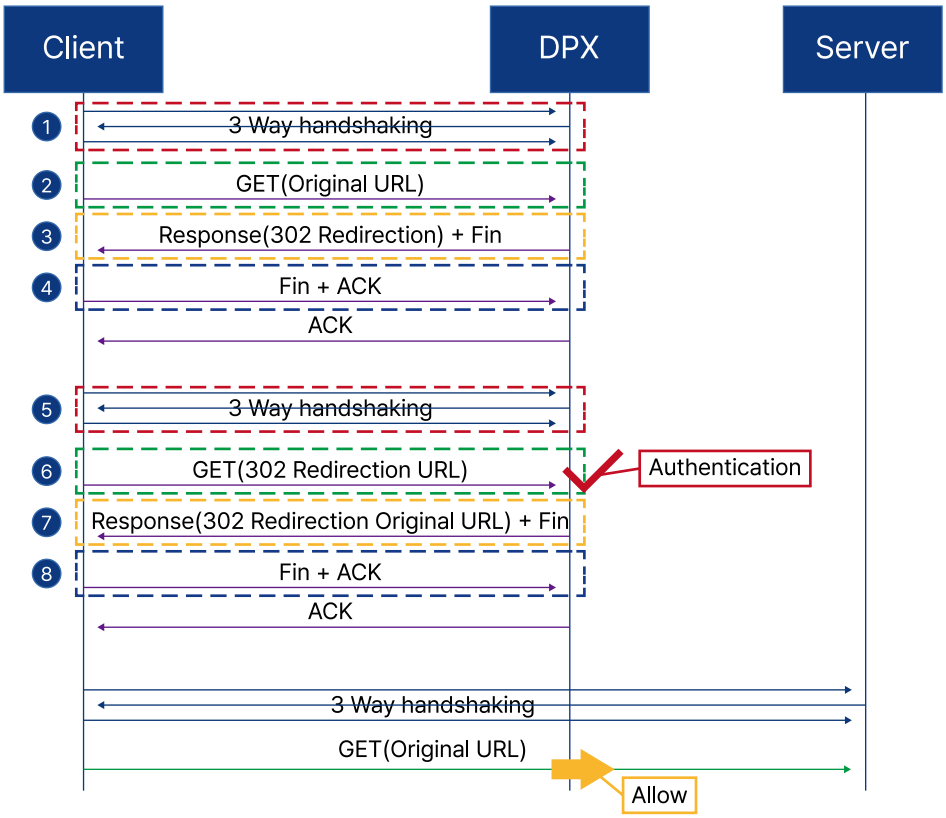

Figure 3. HTTPS authentication mechanism

Using the authentication approach, the system can distinguish legitimate users from bots conducting DDoS attacks. By adding authentication capabilities, organizations can raise the level of protection from bot-driven DDoS attacks.

Authentication is also effective in addressing brute-force attacks, a form of HTTP-based DDoS attack that relies on repeated password attempts. The table below compares server response lengths with authentication enabled and disabled. When authentication is enabled, the solution can identify automated attack behavior and consistently returns a fixed-length response to complicate password inference processes.

Category	Description
Condition	Password → password
Authentication Disabled	The actual password can be inferred by observing differences in server responses
Authentication Enabled	The system returns an answer with the same length, preventing inference of the actual password.

Table 4. Brute-force attack mitigation via authentication

Method 3: Scrubbing Center

There are limitations to addressing ultra-large-scale DDoS attacks using authentication. Organizations should consider rerouting DDoS traffic for business-critical services to a scrubbing center.

Request ▲	Payload	Status	Error	Timeout	Length
1	passqwer	200	☐	☐	4584
2	passqwww	200	☐	☐	4584
3	passwedd	200	☐	☐	4584
4	passwfgg	200	☐	☐	4584
5	password	200	☐	☐	4627
6	passcwer	200	☐	☐	4584
7	passwora	200	☐	☐	4584
8	passworb	200	☐	☐	4584
9	passworc	200	☐	☐	4584
10	passwork	200	☐	☐	4584

Request ▲	Payload	Status	Error	Timeout	Length
1	passqwer	302	☐	☐	203
2	passqwww	302	☐	☐	203
3	passwedd	302	☐	☐	203
4	passwfgg	302	☐	☐	203
5	password	302	☐	☐	203
6	passcwer	302	☐	☐	203
7	passwora	302	☐	☐	203
8	passworb	302	☐	☐	203
9	passworc	302	☐	☐	203
10	passwork	302	☐	☐	203

Figure 4. Brute force attack mitigation using authentication

TCP and HTTP authentications mitigate bot-driven low-volume precision attacks, abnormal protocol attacks, and other forms of automated DDoS activity. AhnLab DPX implements six authentication techniques while maintaining performance in operational environments.

※ Note: Ultra-large-scale attacks exceeding 100 Gbps to 1 Tbps exceed the mitigation capacity of threshold-based rules and authentication mechanisms alone.

Step 3: Scrubbing center

A few years ago, adversaries launched a DDoS attack exceeding 1 Tbps against GitHub, a widely used source code repository service. Once DDoS traffic exceeds available bandwidth capacity (1 Gbps or 10 Gbps), on-premises mitigation no longer remains effective.

The telecommunications industry is one of the sectors frequently exposed to ultra-large-scale DDoS attacks. In particular, their business-critical services that require continuous availability require mitigation methods capable of handling ultra-large-scale DDoS attacks. A DDoS mitigation in form of SECaaS (Security-as-a-Service), commonly known as a scrubbing center, addresses this requirement by redirecting DDoS traffic to an external infrastructure for large-scale mitigation.

Why AhnLab DPX

- Advanced DDoS traffic and bot detection
- Zone management
- Seamless log management and API integration
- Proven scrubbing center use cases
- Flexible hardware options

Most telecommunications companies operate scrubbing centers to defend against ultra-large-scale DDoS attacks, and AhnLab DPX has experience collaborating with multiple telecom operators by integrating the product with their scrubbing centers to mitigate DDoS campaigns.

In summary, telecommunications service providers generally maintain robust in-house DDoS mitigation frameworks. These internal frameworks primarily rely on threshold-based rules and TCP and HTTP authentications. In addition, they leverage signature-based detection, quality of service (QoS) controls, TCP stateful inspection, protocol anomaly prevention, and access control lists (ACLs).

Address DDoS with AhnLab DPX

AhnLab DPX provides all required DDoS mitigation capabilities and supports the deployment of a robust security across diverse network environments. The solution supports 40G and 100G network interface cards (NIC) and operates on a high-performance packet processing architecture based on the data plane development kit (DPDK). By performing full packet inspection instead of sampling-based analysis, it enables more comprehensive and accurate DDoS detection.

Our solution leverages a 13-stage multi-layer filtering architecture to detect and mitigate a wide range of DDoS attack techniques. Using TCP and HTTP authentications, AhnLab DPX precisely distinguishes legitimate user traffic from automated bot traffic and mitigates attacks accordingly.

AhnLab DPX is available in three hardware models, AhnLab DPX 5000C, 10000C, and 20000C, allowing organizations to select an appropriate model based on scale and operational requirements.

The following are the key strengths of AhnLab DPX for telecommunications companies.

1. Zone feature (multi-tenancy)

Organizations can configure logically separated virtual spaces, referred to as zones, enabling security management for each asset to be protected. AhnLab DPX supports up to 328 zones, allowing independent policy configuration and log monitoring on a per-zone basis.

2. Flexible policy management

AhnLab DPX can manage policies across up to 20 appliances without a separate central management solution. It synchronizes zone policies, valid IP information, and self-learning results, truly simplifying multi-appliance management.

This capability is well suited for telecommunication service providers who handle numerous assets and large-scale traffic. As AhnLab DPX enables efficient operations without additional management systems or operational overhead, it ultimately helps customers reduce total cost of ownership (TCO).

AhnLab DPX with the Telco's Scrubbing Center

AhnLab has been collaborating with major telecommunication service providers and public institutions in Asia for optimal DDoS mitigation and scrubbing center operation.

3. Integration with log management systems

AhnLab DPX seamlessly integrates with SIEM and other data platforms to improve log visibility and support advanced data analysis. The solution exports all generated logs to external systems, allowing it to operate as a high-performance traffic sensor for DDoS monitoring and mitigation. More specifically, the integration provides real-time visibility into traffic status and attack timelines, supporting analysis of abnormal or suspicious traffic patterns.

In addition, AhnLab DPX supports automated policy deployment via REST APIs for SOAR and other management solutions such as AhnLab TMS. It also integrates with threat intelligence platforms to incorporate intelligence and stay up-to-date against ever-evolving DDoS attacks.

4. Strong use case of scrubbing center

AhnLab has been collaborating with major telecommunication service providers and public institutions in Asia for optimal operation of scrubbing centers. A common architecture looks like the figure 5 below.

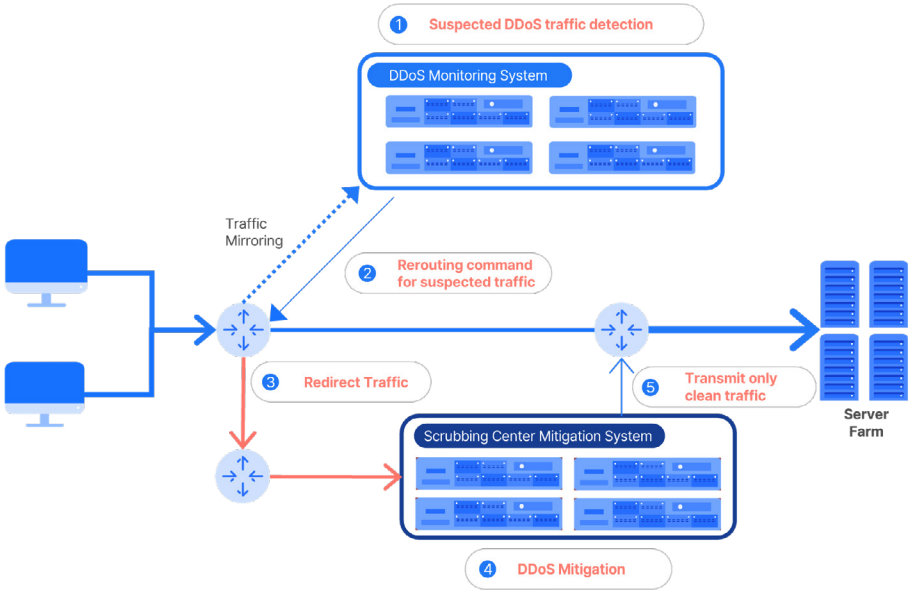

Figure 5. AhnLab DPX and scrubbing center architecture

In simple terms, when AhnLab DPX Detector identifies the DDoS traffic, the detector issues an alert to AhnLab DPX Guard. Then, the guard sends command to the backbone router to redirect the traffic to central sinkhole. Then, the sinkhole discards DDoS traffic, and only valid packets go to the customer server farm through AhnLab DPX Guard and the switch. In the end, users receive the post attack report.

To learn more about AhnLab DPX:

▶Visit our website
▶Watch video

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com