Case Study

AhnLab

Building a Service-Specific DDoS Mitigation Architecture with AhnLab DPX

Industry
Public

Company Size
100-1000 employees

Solutions
AhnLab DPX
AhnLab TMS

DDoS mitigation is no longer simply about handling high-volume attack traffic. It requires the ability to respond to increasingly complex attack patterns without disrupting service availability for legitimate users. These requirements prompted the public institution "L" to seek for a protection framework capable of responding to persistent DDoS attacks, along with a mitigation architecture capable of handling large volumes attacks and centralized management for multiple appliances and policies.
To address these needs, they deployed AhnLab DPX to improve its response capabilities against various DDoS attacks and built a protection framework that could help maintain stable service operations.

Key Results

- Minimized impact on legitimate traffic
- Large-scale DDoS response with parallel AhnLab DPX deployment
- Centralized management with AhnLab TMS

Challenges

The customer needed to improve its DDoS response capabilities while ensuring operational efficiency, minimizing the impact on legitimate traffic, and maintaining service availability.

Mitigation Architecture Tailored to Service Characteristics

The institution provides services to customers across multiple service networks, each with distinct traffic characteristics. Applying a uniform mitigation policy without accounting for these differences can also affect legitimate traffic.
To apply mitigation policies tailored to each service, the agency needed to segment its service networks, define service-specific mitigation criteria, and build an architecture that minimized the impact on legitimate traffic.

Architecture for Processing Large-Scale DDoS Attack Traffic

As DDoS attacks increase in scale, a single mitigation appliance may not have enough capacity to handle surging attack traffic, increasing the risk of service disruption. Effective mitigation requires not only sufficient processing capacity but also a resilient architecture that can continue operating even if an appliance fails. The customer therefore needed to deploy multiple DDoS mitigation appliances in parallel for each service network so that services could remain stable during traffic surges.
However, segmenting service networks and deploying multiple appliances in each network could make policy and log management more complex. They needed an integrated management environment that could centralize operations across multiple networks and maintain consistent policy and log management.

Solutions

The institution segmented its networks based on service characteristics and deployed AhnLab DPX appliances in parallel within each network. They also deployed and configured AhnLab TMS to enable centralized management of multiple appliances.

1. Network Separation by Service Type

The customer segmented their service networks based on the characteristics of the assets they needed to protect. Destination-based routing allowed the agency to direct traffic to the appropriate network and apply DDoS mitigation policies tailored to each service.

2. Parallel Deployment of AhnLab DPX

They deployed multiple AhnLab DPX appliances in parallel within each service network. This gave each network the capacity to handle large volume attacks and ensured that services could remain available even if one or more appliances failed.

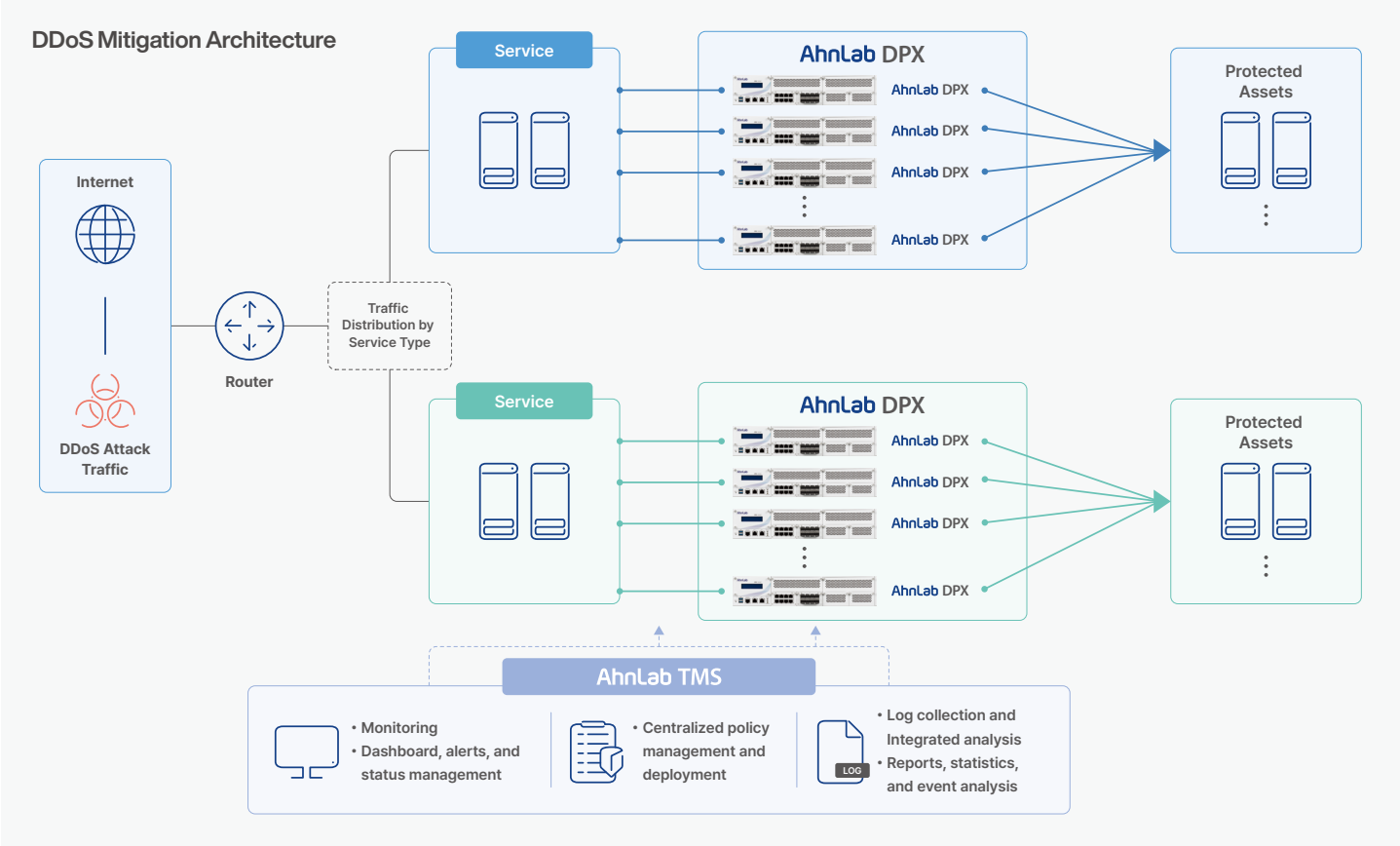
3. Integrated Management with AhnLab TMS

They also deployed AhnLab TMS to centrally manage multiple AhnLab DPX appliances across its service networks. This simplified policy and log management by eliminating the need to manage each appliance separately, while ensuring consistent operations across the environment.

Service-Specific Mitigation Policies

TCP Service Network

- Lowered behavior-based thresholds
- Anti-Spoofing
- Segment Protection
- HTTP access authentication
- QoS processing



Benefits

The institution strengthened its DDoS mitigation capabilities, improved service stability, and increased operational efficiency by building an architecture tailored to each service network and managing it through a centralized framework.

1. Applying Mitigation Policies by Service Type

By segmenting its networks, they could apply DDoS mitigation policies tailored to the characteristics of each service. For services types that did not run on protected assets, the agency set lower behavior-based thresholds to detect and block attack traffic more aggressively. This improved the effectiveness of its DDoS response while reducing the risk of affecting legitimate traffic.

2. Strengthening response capability against large-scale DDoS attacks

The customer deployed AhnLab DPX appliances in parallel to ensure sufficient mitigation capacity during large-scale attacks. This reduced reliance on a single appliance and helped maintain stable service delivery even when attack traffic surged. If one or more appliances failed, the remaining appliances could continue processing service traffic, improving service continuity and resilience.

3. Improving Operational Efficiency Through Integrated Management

They used AhnLab TMS to centrally manage AhnLab DPX appliances deployed across multiple networks. Instead of checking policies and logs on each appliance separately, operators could manage them consistently through a single framework. This reduced operational overhead and improved visibility across the entire mitigation architecture.

DDoS mitigation is not only about blocking attack traffic. If mitigation controls affect legitimate traffic or make operations more complex, service availability can be disrupted. With AhnLab DPX and AhnLab TMS, a public institution built a service-specific mitigation architecture for segmented networks while centralizing management across the environment. This enabled the agency to respond more effectively to large-scale DDoS attacks, reduce the impact on legitimate services, and improve operational stability. This case shows that service-specific mitigation architecture combined with integrated management provides a practical approach for responding to larger and more complex DDoS attacks.

AhnLab DPX protects customers from DDoS attacks through specialized technology, proven experience, and deep expertise.
DDoS remains one of the oldest and most frequent types of cyberattack. Because DDoS attacks are relatively easy to launch, DDoS has evolved into various forms, making them difficult to block with a single detection method. AhnLab DPX is an industry-leading DDoS mitigation solution designed to address DDoS attacks. Built on our dedicated DDoS mitigation technology, AhnLab DPX delivers advanced traffic analysis and multiple detection techniques.

Before vs. After AhnLab DPX

Before	After
Single mitigation policy	Service-specific mitigation
Risk of legitimate traffic disruption	Optimized thresholds and policies
Individual appliance management	integrated management through TMS