QRATOR LABS

NimbusDDOS

Protecting Enterprise Infrastructure Against DDoS Attacks

1 Introduction

Document's Objective: To establish effective design for protecting corporate networks against DDoS attacks.

Target Audience: IT directors, system administrators, and information security specialists.

Problem Overview: The primary challenge is the need to develop a unified, comprehensive strategy for DDoS attack protection.

2 Types of Infrastructure and Their Features from a Network Security Perspective

Web application only in a public cloud.

Web application with L3-L4 services in a public cloud.

On-premises data center or private cloud environment.

3 Comprehensive Approach to DDoS Attack Protection

Protecting web applications in the cloud.

Protecting web applications and corporate services in the cloud.

Protecting infrastructure, including the on-premises data center or private cloud.

4 Maintaining DDoS Resiliency

Regular DDoS testing.

Certification and compliance assurance.

Ongoing personnel training and skill development.

5 Conclusions

1. Introduction

Document's Objective

This document describes effective methods for protecting corporate networks against DDoS attacks. It considers the complexity and diversity of the infrastructure, while also emphasizing the importance of regular testing, certification, and personnel training to ensure resilience against modern threats.

The document was created by two companies: NimbusDDoS and Qrator Labs. The document is based on the experience of the companies and reflects current trends and best practices developed in practice, in the process of implementing projects to create and maintain secure infrastructures in the commercial and public sectors.

Target Audience

This document is intended for IT directors, system administrators, information security professionals, and other specialists responsible for managing and safeguarding corporate networks and cloud infrastructure. By providing clear strategies for DDoS protection, it aims to make their work more effective.

Problem Overview

Modern corporate networks are characterized by significant complexity and infrastructure diversity. Most organizations utilize a combination of different infrastructure types: web applications in the cloud, network services hosted both in the cloud and on-premises, and private cloud solutions. Due to this diversity, protection methods must vary, as each component of the infrastructure has its own specific vulnerabilities and encounters unique threats.

The primary challenge, therefore, is to develop a unified and comprehensive DDoS protection strategy that accounts for all components of the infrastructure and ensures adequate protection for each. Achieving this goal is further complicated by the fact that many organizations lack regular DDoS resiliency testing and a clearly defined incident response plan. Without these measures, companies risk critical malfunctions, data loss, operational disruptions, and significant financial damage.

Key issues:

1. Infrastructure diversity:

> *Each part of the infrastructure, whether it's a web application in the cloud or a local network, requires a unique approach to DDoS protection. Methods that work well for one part of the infrastructure may not be effective or even applicable for another.*

2. Challenges in defense coordination:

> *The integration of various tools and technologies necessary to protect all infrastructure components increases the risk of vulnerabilities, often due to system incompatibilities or misconfigurations.*

3. Lack of regular testing and risk assessment:

> *Many organizations neglect to regularly test their infrastructure for DDoS resiliency. As a result, potential vulnerabilities can go unnoticed until an actual attack happens, at which point it may be too late to respond effectively.*

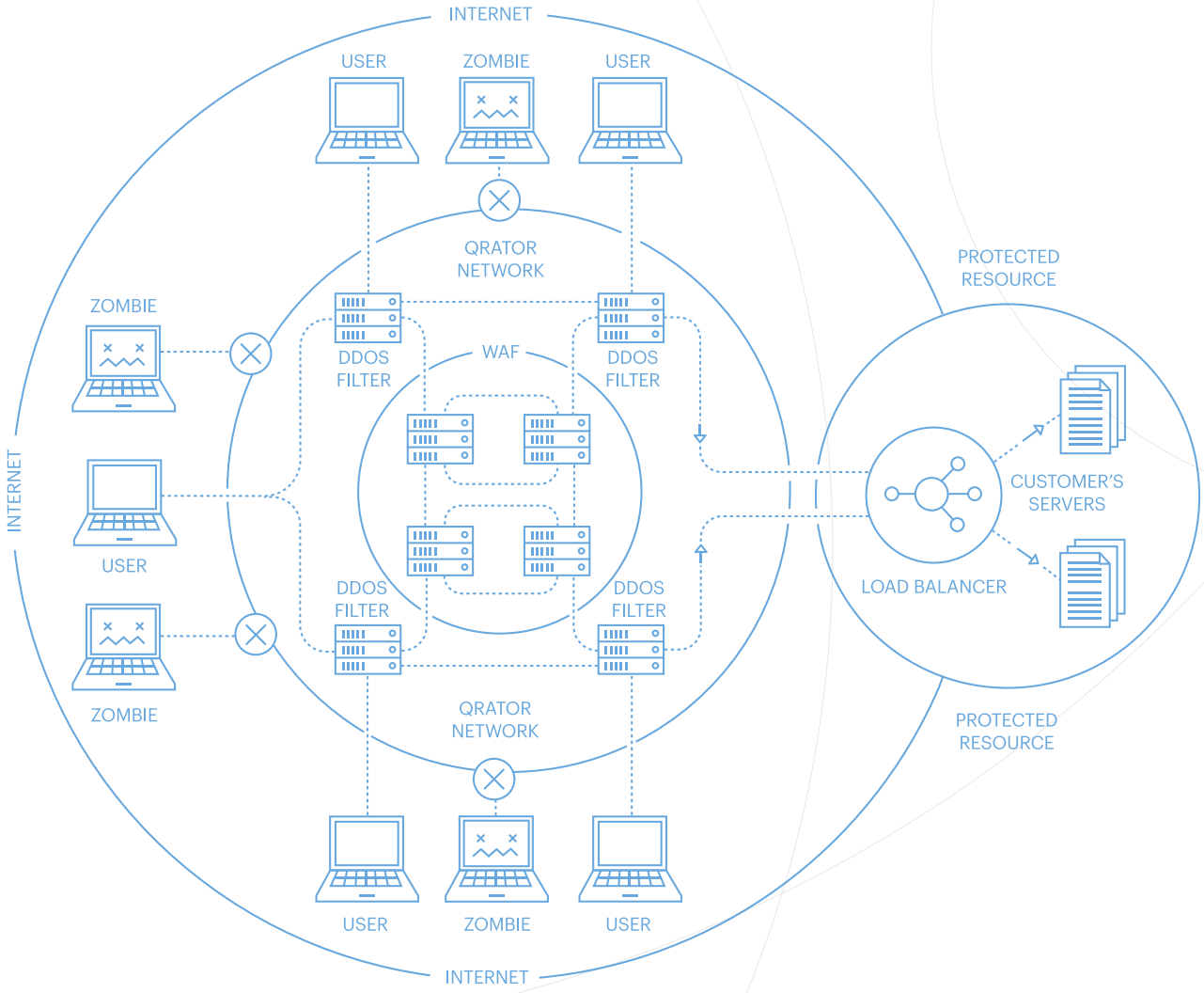
4. Absence of an incident response plan:

> *In a crisis, the absence of a pre-developed and tested incident response plan can lead to chaotic and ineffective actions, worsening the impact of the attack.*

2. Types of Infrastructure

AND THEIR FEATURES FROM A NETWORK SECURITY PERSPECTIVE

Web Application Only in a Public Cloud



Description: *Web applications and APIs for mobile applications are hosted entirely in the cloud.*

The cloud provider offers Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

Features: *Flexibility and scalability: Resources can be easily scaled to meet changing workloads.*

Automation and updates: Providers regularly deliver updates and patches for infrastructure, reducing the risk of vulnerabilities.

Shared responsibility: Cloud security operates on a "shared responsibility" model, where the provider handles the security of the cloud, while the customer is responsible for securing data and applications within the cloud.

Availability and fault tolerance: Cloud providers offer tools to ensure high availability and fault tolerance.

Web Application with L3-L4 Services in a Public Cloud

Description: *Applications, websites, and certain network functions (such as routing and load balancing) are hosted in the cloud.*

Both IaaS/PaaS and network services (such as virtual networks and VPNs) are utilized.

Features: *Networking integration: Cloud providers offer tools to manage network resources and traffic, such as AWS VPC and Azure VNets.*

Network policies: Ability to configure complex network policies and security rules to control traffic at OSI layers 3 and 4.

Network segmentation: Virtual networks enable the isolation of different infrastructure components to enhance security.

Monitoring and logging: Tools for network monitoring and traffic logging help detect anomalies and incidents.

On-premises Data Center or Private Cloud Environment

Description: *The infrastructure is hosted on-premises in a corporate data center or in a private cloud*

This setup provides complete control over both hardware and software..

Features: *Complete control over infrastructure: The organization independently manages and configures all aspects of security, including the physical security of the data center.*

Customization and configuration: Network and server components can be fully customized and configured to meet the organization's specific needs.

Internal segmentation: Enables the creation of internal security zones and network segmentation to protect against internal threats.

Restricted access: Provides stricter control over access to resources and data compared to public clouds.

Redundancy and fault tolerance: The ability to create backup systems and implement fault-tolerant mechanisms to ensure high availability, though this requires substantial investment.

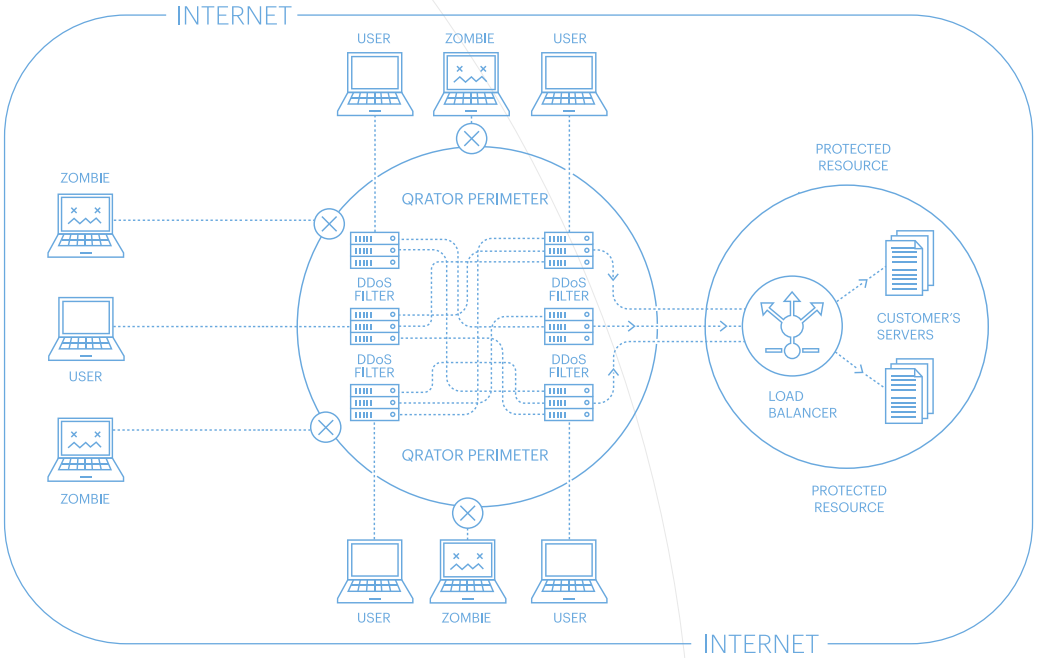
Patch and update management: The organization is responsible for timely updates and patching of the infrastructure.

Dedicated security team: Requires a qualified team to ensure security and respond to incidents effectively.

Each type of infrastructure has its own characteristics and demands specific approaches to network security. Web applications in the cloud offer high flexibility and automation, while web applications with L3-L4 services in the cloud add network function management capabilities. In contrast, on-premises or private cloud environments provide full control and customization, but require significant resources to maintain security. The choice of approach depends on business requirements, risk tolerance, and available resources.

3. Comprehensive Approach to DDoS Attack Protection

(QRATOR LAB'S APPROACH AND RECOMMENDATIONS)



Protecting Web Applications in the Cloud

When hosting web applications in a public cloud, the key task is to ensure their availability and protection against DDoS attacks. However, it is important to understand that, in this case, the responsibility for protection is shared between the application owner and the cloud provider.

The application owner is responsible for security and protection at the web application level (L7), including filtering unwanted traffic, configuring security policies, and defending against application-targeted attacks.

The cloud provider is responsible for the stability and availability of the infrastructure (L3-L4), including protecting network and computing resources, ensuring client isolation, and mitigating the impact of infrastructure-level attacks.

This distributed model of responsibility requires a comprehensive approach to risk management to minimize the impact of attacks and ensure the reliable operation of applications.

Protecting Web Applications at L7: Qrator Labs approach

Qrator Labs recommends a holistic approach to protecting web applications from DDoS attacks, effectively addressing all risks within the application owner's responsibility. This approach includes several layers of protection:

Protection against L7 DDoS attacks

Real-time traffic filtering to automatically block DDoS attacks targeting protected applications.

Advanced traffic analysis powered by machine learning to minimize false positives.

Scalable defense mechanisms that adapt to fluctuating workloads.

Managed Web Application Firewall (WAF)	*Protection of web applications from targeted attacks that exploit specific vulnerabilities.*
	Predefined security rules designed to address current threats.
	Flexible customization options tailored to your application's unique requirements.
Bot management (Anti-bot)	*Detection and blocking of malicious bots used for attacks, data theft, or performance degradation.*
	Identification and analysis of user fingerprints to distinguish real visitor actions from automated requests.
	Protection against content scraping and other bot-related attacks.

How Qrator Labs approach Address Application Owner Risks

From a risk management perspective, Qrator Labs recommended approach enable application owners to effectively address the following challenges:

L7 DDoS attacks:	*comprehensive management of incoming traffic, including attack filtering, adaptation to emerging threats, and minimizing the impact on legitimate users.*
Configuration errors and insufficient protection:	*flexible WAF configuration and automated defense requiring minimal human involvement.*

Bot-driven attacks: *prevention of vulnerability exploitation, data scraping, and excessive resource consumption.*

This approach provides protection while simultaneously improving the performance and availability of web applications, which is especially important for businesses facing modern threats.

Protecting Web Applications and Corporate Services in the Cloud

Let's consider a more complex scenario where, in addition to web applications, a company also hosts other infrastructure elements in the cloud. These may include a DNS server, corporate video conferencing or telephony services, various custom applications that use TCP and UDP protocols, a corporate VPN, and more.

In this case, the application layer threats outlined in the previous section still apply. Additionally, new threats at the network and transport layers (L3-L4) arise, as these corporate services are publicly accessible.

In this scenario, there are two possible approaches to protection:

> *Use a specialized provider for L7 DDoS protection, WAF, and anti-bot solutions while relying on the cloud's built-in mechanisms to mitigate L3-L4 attacks. However, this approach has a limitation: the cloud provider will only ensure traffic delivery to the custom-*

er, but it does not guarantee the availability of cloud-hosted applications that use TCP and UDP under an SLA.

Engage a specialized provider for comprehensive protection across both L7 and L3-L4 layers.

Here, it is important to consider that TCP traffic, like HTTP/HTTPS, can be protected using a reverse proxy. However, this approach is not well-suited for UDP traffic due to the nature of the protocol. Since UDP is stateless, verifying the authenticity of packet sources is not possible. This can lead to unpredictable application issues that are difficult to troubleshoot.

Protecting Corporate Services at L3-L4: Qrator Labs approach

Qrator Labs implements approach that consists of two connectivity options for L3-L4 DDoS protection, each with its own advantages and trade-offs:

DNS-based protection (reverse proxy)	*Effectively filters TCP traffic.*
	Suitable for organizations without their own autonomous system.
	Does not require dedicated communication channels.
BGP-based protection	*Filters all protocols, including UDP.*
	Designed for organizations with their own prefixes and autonomous system.

A reverse proxy connection effectively protects services using the TCP protocol but is unsuitable for UDP-based applications. For large organizations with their own prefixes and autonomous system, Qrator Labs recommends a more robust BGP-based solution that enables rerouting all traffic through a filtering network.

This approach enables the development of authentication and whitelisting mechanisms for UDP-based applications. This way, UDP traffic can be blocked by default and only accepted from addresses where users have previously authenticated via HTTP/HTTPS.

This approach ensures real-time UDP traffic authorization without delays, preventing any negative impact on user experience.

How Qrator Labs approach Address Corporate Service Owner Risks

Thanks to multiple connectivity options, Qrator Labs approach is effectively protected against a wide range of threats:

Application layer attacks:	*From a risk management perspective, using a single provider to protect the entire infrastructure — both at L3-L4 and the application layer — offers significant advantages, especially against multi-vector DDoS attacks.*
DDoS attacks targeting TCP-based services:	*Based on Qrator Labs' experience, this approach allows to effectively filter TCP traffic regardless of the connection method, whether via DNS or BGP.*

DDoS attacks targeting UDP-based services:

If the customer operates their own autonomous system, BGP-based protection can be implemented to safeguard UDP traffic as well.

This flexibility sets the approach apart from built-in DDoS protection offered by cloud providers.

Protecting Hybrid Infrastructure, Including the On-Premises Data Center or Private Cloud

Let's move on to the most complex configuration. As in the previous case, the organization's infrastructure includes both web applications and services running on TCP and UDP protocols — such as DNS, telephony, video conferencing, VPN, and custom-developed applications. However, in this scenario, the organization hosts infrastructure elements both in the cloud and in its own data center.

In this case, the organization often maintains full control over all infrastructure components, both on-premises and in the cloud, including routers and firewalls. Such organizations typically have their own prefixes and autonomous systems, allowing them to build a resilient architecture that leverages their data centers while using the cloud as a provider of computing and network resources.

> *In this setup, the organization bears full responsibility for mitigating network attacks and ensuring availability.*

The worst approach to securing a hybrid infrastructure is using two independent protection providers — one for the cloud and another for the organization's own data center. Since each provider sees only a portion of the traffic, this configuration either leads to uncoordinated defense measures or incurs high costs for coordination between them.

For example, a powerful DDoS attack could render the cloud unavailable, forcing all traffic — including legitimate requests — to be redirected to the organization's on-premises infrastructure (or vice versa). Since the protection provider overseeing that part of the network has not previously observed this traffic pattern, it may struggle to distinguish between normal and malicious activity.

This can lead to a surge in false positives and false negatives: legitimate traffic may be blocked, while harmful traffic slips through undetected.

Protecting Hybrid Infrastructure: Qrator Labs approach

For hybrid infrastructures that use both on-premises data centers and the cloud, Qrator Labs recommends connectivity to a unified filtering network from all points of presence where BGP routers are deployed:

BGP-based protection	*Provides the most effective traffic filtering for hybrid infrastructures.* *Compatible with all protocols, including UDP.* *Ensures comprehensive infrastructure protection with guaranteed availability of all applications, regardless of attack scale or type.*

At the same time, organizations can maintain a backup protection provider for traffic rerouting if needed.

Using two different protection providers simultaneously may be acceptable if the on-premises data center and cloud infrastructure serve completely independent applications. For example, if the core infrastructure operates in the organization's own data center while web resources are hosted in the cloud, each can be secured by a separate provider.

How Qrator Labs approach Address Hybrid Infrastructure Owner Risks

Using a single network protection provider for all elements within a hybrid infrastructure significantly improves risk management. This approach ensures the availability of all applications under any circumstances, backed by an SLA.

Network and transport layer attacks:	*BGP-based connectivity and full traffic rerouting through the Qrator Labs filtering network provide effective protection for all traffic, including UDP.*

Application layer attacks:

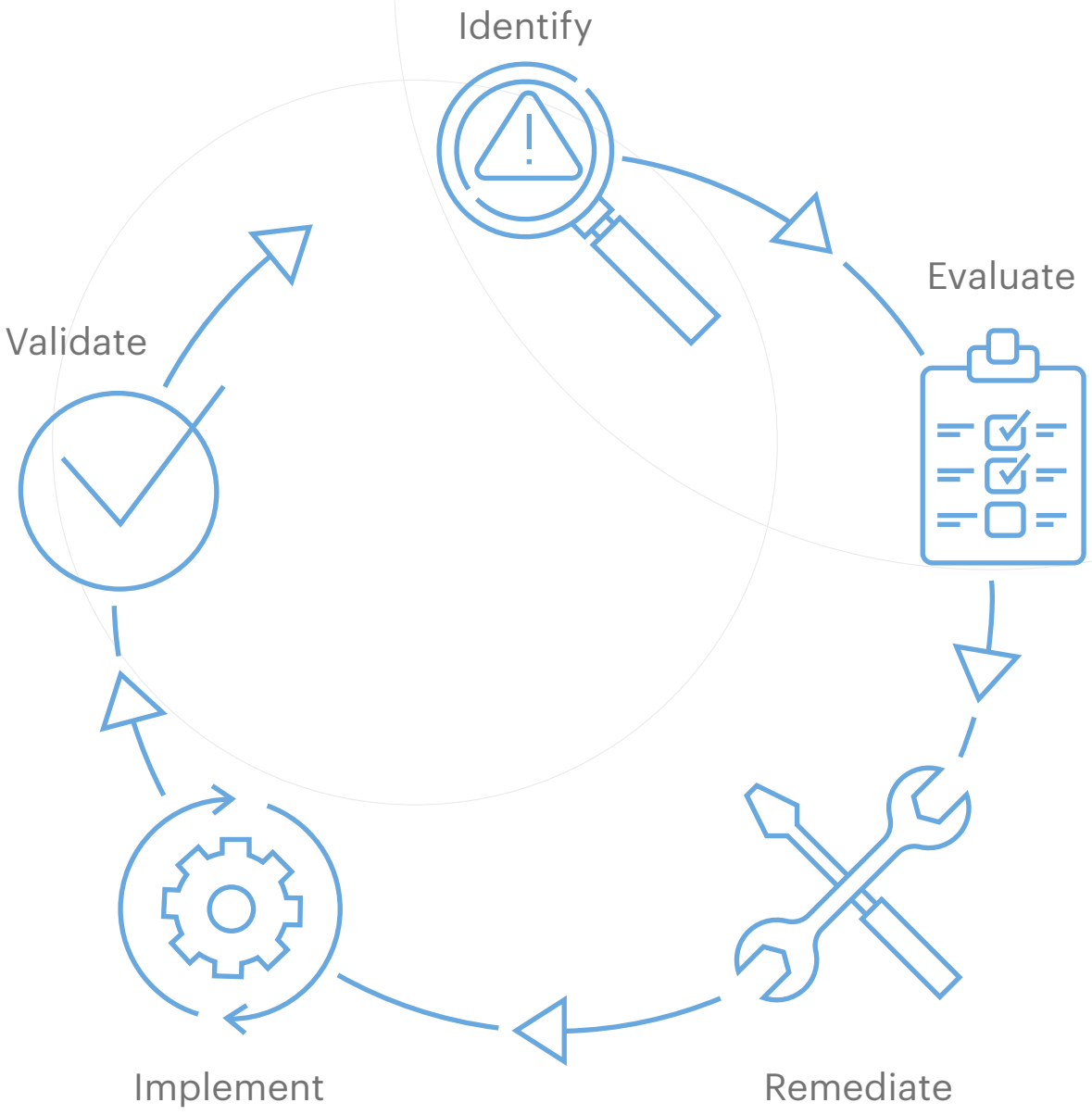
Securing the entire infrastructure with a single provider across L3-L4 and L7, both on-premises and in the cloud, offers significant advantages, especially against large-scale multi-vector DDoS attacks.

The Qrator Labs network consists of 15 filtering centers worldwide, connected to Tier 1 or leading regional providers. With global coverage and over 4,000 Gbps of bandwidth, Qrator Labs ensures the availability of protected resources, even during the most extensive and sophisticated DDoS attacks.

4. Maintaining DDoS Resiliency:

NIMBUSDDOS APPROACH AND RECOMMENDATIONS

Corporate infrastructure is constantly evolving, as is the threat landscape alongside it. For this reason, a one-time effort to implement modern tools and technologies is not enough for effective protection against DDoS attacks. Below are four major hurdles we have identified that every company must engage with to create a holistic defense:



Choosing the right combination of services.

As a business, choosing vendors and products is a challenge. The long terms of contracts and the large variety of offerings in every space makes getting the right products into an environment a difficult process.

Preparing the solutions to function optimally.

Improper configurations can mean the difference between a successful mitigation, an attack slipping through unchallenged, or suddenly taking your entire environment offline when the mitigation kicks in.

Maintaining security over time.

Attackers work to get around security measures with as much determination as vendors work to develop them, this is why regular maintenance is required to maintain a properly secured DDoS posture.

Developing personnel to support services.

DDoS is a niche corner of cyber security that many engineers are unfamiliar with. A lack of education and experience can lead to longer outages and less complete mitigations, even with the correct mitigation tooling in place.

With the help of trained engineers and a platform capable of replicating any kind of DDoS, NIMBUSDDOS can facilitate the following key processes:

Proof of Concept

The engineers at NIMBUSDDOS have over a decade of experience testing and configuring DDoS mitigation solutions for clients. That expertise can help narrow the options to a tight list that can then be used in a proof of concept test. Conducting a PoC test to compare options can ease difficult decisions by giving stakeholders an apples to apples comparison. Doing these comparative tests helps build confidence in the final choice and can highlight potential issues before a contract is signed.

Baseline Creation

The first step to producing a resilient DDoS mitigation strategy is baselining the efficacy of the existing technology. This initial test arms stakeholders with data produced by a senior engineer and acts as a ruler against which all further efforts can be measured.

Configuration validation

Once a baseline is understood, the work of closing identified gaps begins. In addition, every change made to network infrastructure has the potential to impact the efficacy of DDoS mitigation. The configurations of these protections must be regularly validated. NimbusDDOS suggests adding regular DDoS testing as a part of maintenance to ensure that new vulnerabilities are not introduced as a result of infrastructure changes. Most clients test between one and four times per year, depending on the level of risk DDoS poses to their operations.

Process Validation

After a current defense's technical capability is proven by configuration testing, it is vitally important to test the human element of the defense. These red team engagements give employees real world experience and can reveal weaknesses in processes that were not apparent in writing or during tabletop exercises.

Emergent Threats

The DDoS landscape is ever changing. While technology companies work tirelessly to close gaps in their products to protect their customers, attackers hunt for new vulnerabilities, attack vectors and delivery methods to thwart them. NimbusDDOS' testing experts monitor the news, dark web forums and have frequent check-ins with their customers to stay ahead of these threats and avoid costly surprises.

Ongoing Personnel Training and Skill Development

NimbusDDOS offers training for all levels of staff to develop awareness of modern threats and best security practices, significantly reducing the risk of a successful attack. It is important that all levels of related staff have some understanding of DDoS attacks and mitigation.

For Executive Staff

> *Understanding DDoS Fundamentals & Trends*
>
> *Business Impacts of DDoS Attacks*
>
> *Mitigation Systems & Strategies*

For Technical Staff

> *Identifying Attack Vectors (Volumetric, Protocol and Layer-7)*
>
> *Incident Response Practices*

Certification and Compliance Assurance

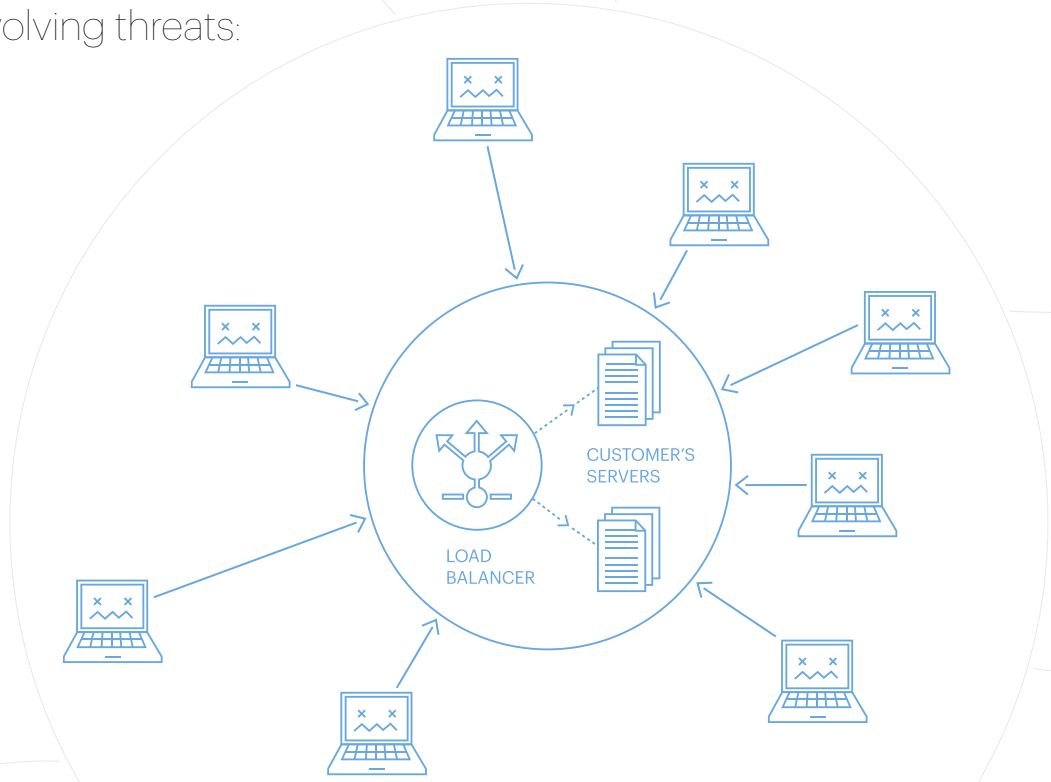
To maintain an adequate level of security, the infrastructure and processes must comply with recognized standards and certification requirements, such as ISO/IEC 27001, PCI DSS, and regional or industry-specific regulations.

Certification not only confirms adherence to high security standards but also helps improve risk management processes, thereby increasing overall resilience to attacks.

5. Conclusions

Key points at a glance

A robust DDoS defense strategy requires a multi-faceted approach that combines advanced technology, continuous monitoring, and well-prepared personnel. The following key aspects are essential for ensuring resilience against evolving threats:



Comprehensive protection is a must:

Given the diversity of modern corporate infrastructure — ranging from web resources in public clouds to custom applications in local data centers — a unified and well-coordinated DDoS defense strategy is essential.

Layered defense approach:

Effective network protection must cover multiple layers, from L3-L4 DDoS defense to application layer security. At the application level, this includes L7 DDoS protection, a web application firewall (WAF), and anti-bot measures. Ideally, these solutions should work together as a unified system.

The role of continuous monitoring and advanced threat detection:

Constant threat analysis, automated filtering, and adaptive response mechanisms are key to effective traffic filtering with minimal false positives.

Regular DDoS testing and compliance:

To maintain DDoS resilience, it is essential to regularly conduct infrastructure DDoS tests and ensure compliance with security standards.

Personnel training and incident response planning:

Since the human factor remains critical, ongoing training, simulated attack exercises, and predefined incident response protocols play a major role in reducing the risk of disruption.

The importance of a proactive approach

As DDoS attacks grow more sophisticated, defense mechanisms must continuously evolve. A proactive security strategy should include:

Anticipating new attack methods:	*Adversaries constantly refine their techniques and develop new ones, making it essential to regularly update and enhance defense mechanisms.*
Regular testing and resilience assessments:	*Simulated attack scenarios and load testing help verify that security systems can withstand large-scale threats before they materialize.*
Using unified, scalable protection solutions:	*Whether in a cloud-based, on-premises, or hybrid environment, it is important to establish a unified defense approach. Relying on a single security provider for comprehensive protection reduces inconsistencies and enhances overall defense efficiency.*

DDoS defense is not a one-time implementation but an ongoing process of adaptation, evaluation, and improvement. By staying ahead of evolving threats, businesses can ensure operational continuity, minimize financial risks, and maintain user trust in an increasingly hostile cyber environment.

QRATORLABS

The document created by NIMBUSDDOS (Newton, Massachusetts, United States, www.nimbusddos.com) and Qrator Labs (Prague, Czech Republic, www.qrator.net)