LINK11

DDOS PROTECTION BUYER'S GUIDE

What to look for in a DDoS Protection Solution

www.link11.com

Choosing the right solution to protect your company against Distributed Denial of Service (DDoS) attacks, which can result in harmful business disruptions, is crucial in today's digital landscape. An effective solution not only mitigates attacks but also ensures uninterrupted availability and performance of your critical services. With the increasing complexity and frequency of DDoS threats, selecting the right protection is more important than ever.

The products offered by DDoS service and solution providers can differ considerably, making it challenging to select the right protection solution. This Buyer's Guide tells you what to look for when evaluating DDoS protection options and highlights the benefits of working with an external protection provider. It also details the basic functions of modern DDoS protection solutions —questions you should raise with potential providers.

In this guide, we will discuss best practices for evaluating DDoS protection solutions and selecting the one that provides a holistic approach to securing your workloads, is scalable to meet future business needs and will adapt to new threats as they emerge.

Key Criteria for Evaluating DDoS Protection Solutions

When reviewing DDoS protection solutions, consider these criteria:

1. Available DDoS protection solutions
2. Routing solutions: Redirection of data traffic
3. Availability: 'Always-On or 'On-Demand'
4. Filter options
5. Automation in attack detection and filtering
6. Protection for OSI layers
7. Multi-cloud support
8. Compliance
9. Monitoring and visualization
10. Integrated platform for DDoS-related services
11. Support and managed Services

1. AVAILABLE DDOS PROTECTION SOLUTIONS

Organizations use several approaches to defend against DDoS attacks, including hardware appliances (On-Premises), cloud-based and cloud-native solutions, and hybrid protection models.

a) Appliance / On-Premises

The appliance monitors data traffic and restricts or blocks malicious requests upon detecting anomalies, such as a surge in traffic. Some deployment models require manual intervention from IT Teams or external security providers.

- **Customization:** Offers tailored adjustments to -specific IT infrastructure and traffic patterns.
- **Data Privacy:** Keeps sensitive information within the organizations network, reducing third-party exposure.
- **Scalability Limitations:** Hardware appliances may struggle with large-scale attacks exceeding their capacity.
- **High Cost:** Involves significant upfront investment for procurement, maintenance, and updates.
- **Maintenance Complexity:** Requires in-house expertise to manage and update.
- **Limited Coverage:** Effectiveness may be decrease for geographically distributed infrastructures or external assets.

b) Cloud-based DDoS Protection:

In this approach, the website's data traffic is routed through the provider's external filter, enabling multi-layered analysis to detect and block attackers. Only legitimate data traffic is forwarded.

- **Scalability:** Manages large-scale attacks using distributed cloud infrastructure.
- **Ease of Deployment:** Quick set up with minimal technical effort.

- **Global Reach:** Protects assets across multiple regions without additional hardware.
- **Comprehensive Attack Detection:** Effective against volume, application, and protocol-based attacks, as well as unknown vectors.
- **Data Sovereignty Issues:** May pose regulatory concerns due to third-party data routing.
- **Vendor Lock-In:** Switching providers can be difficult post integration.

c) Cloud-Native DDoS Protection

Cloud-native DDoS protection solutions are designed for fast implementation, with a basic set of options and security settings. In practice, however, these solutions often prove insufficient **for fully protecting** applications and data in production environments. Since users remain responsible for security and data protection when relying on third parties, significant customizations and specialized expertise are require.

- **Built-In Integration:** Designed specifically for cloud environments, integrating seamlessly with cloud-native applications.
- **Dynamic Scalability:** Adjusts automatically to counter growing attack volumes.
- **Low Latency:** Reduces rerouting delays through integration with cloud provider's network.
- **Regulatory Alignment:** Some providers offer compliance-ready solutions tailored to specific regional laws and regulations.
- **Protection Costs:** Advanced protection often incurs high expenses beyond basic coverage.
- **Limited Vendor Options:** Often tied to specific cloud providers, limiting flexibility.
- **Cost Dependency on Cloud Usage:** Pricing scales with cloud usage, which may increase expenses for high-traffic applications.

d) Hybrid Protection

This combined approach integrates hardware and cloud-based solutions for comprehensive protection against both application and network-level attacks.

- **Comprehensive Coverage:** Provides robust defense by combining On-premise and cloud-based capabilities.
- **Flexibility:** Handles smaller attacks On-premises, while scaling cloud solutions scale for large scale threats.
- **High bandwidth strength:** Effective for scaling but limited by the hardware's capacity.
- **Integration Complexity:** Challenging to integrate into existing IT infrastructures.
- **Switching Delays:** May result in latency or downtime during attacks.
- **Compliance Issues:** Must adhere to the country's data protection standards.
- **Higher Total Cost:** Combining solutions increases expenses compared to standalone approaches.

2. ROUTING SOLUTIONS: REDIRECTION OF DATA TRAFFIC

DDoS protection can be implemented via DNS forwarding, or during an attack, by routing data traffic via BGP to the protection provider or its scrubbing centers for filtering. The structure of the company's IT systems plays a critical role in choosing between these two routing solutions.

a) DDoS Protection via DNS Forwarding

DNS protection aims to secure a company's web applications without the need to expand the server infrastructure, add bandwidth, or buy new router technology. It can be implemented starting with just one IP address. This method protects applications based on domain names from DDoS attacks on layers 7. To do so, the DNS A-record entries of the affected application are modified to redirect the data transfer to the scrubbing center. Infected clients query the DNS servers for the IP address, receive the scrubbing center's IP address via the DNS change, and thus avoid sending the attack to the original server. Protection is active once the DNS serve change has been made.

b) DDoS Protection via Border Gateway Protocol (BGP)

BGP DDoS protection, also known as layer 3 and 4 DDoS protection, can be used in a hot-standby mode, which maintains normal data flow when no attack is detected. In the event of an attack, data traffic is routed through the scrubbing center. Filtered data packets are then sent back to the customer's network via a protected tunnel (VPN, IPsec, GRE). Once the attack is mitigated, the traffic is redirected to the original route. A BGP solution requires a 24 IP network or larger for redirection. Complete protocols can also be forwarded according to customer specifications. During an attack, both the customer and the security operations center can announce the network in a standby integration.

c) Possible Combinations: Web DDoS and Infrastructure Protection

As companies' IT infrastructures become increasingly complex, consisting of web servers, databases, Internet telephony, and cloud applications, a combination of DNS forwarding and BGP redirection is often recommended for maximum DDoS protection. The choice should always be tailored to the company's specific needs and based on a thorough analysis conducted with the DDoS protection provider.

3. AVAILABILITY: ALWAYS-ON OR ON-DEMAND

When selecting a DDoS protection solution, one of the key decisions is whether to choose Always-On or On-Demand protection. Both approaches offer unique advantages and suit different business needs, industries, and threat landscapes. Always-On protection ensures continuous, automated defense against all types of DDoS attacks, providing maximum uptime and reliability. On the other hand, On-Demand protection activates only when a threat is detected, offering cost-efficiency while maintaining robust security. Understanding the differences between these approaches is essential to making an informed choice that aligns with your organization's security priorities and budget.

a) On-Demand Protection

On-Demand DDoS protection is a flexible solution designed to mitigate volumetric and protocol-based attacks (Layer 3/4). Under normal conditions, customer traffic flows uninterrupted and is continuously monitored using flow data, telemetry, or other analytics. When an attack is detected, the service provider or client is alerted, and traffic is rerouted to a scrubbing center for mitigation.

This rerouting is facilitated via Border Gateway Protocol (BGP) announcements, which can be triggered manually by the client or automatically by the provider. Once redirected, the scrubbing center filters out malicious traffic, ensuring only clean traffic is returned to the client through pre-configured tunnels, such as Generic Routing Encapsulation (GRE) tunnels.

A key advantage of On-Demand protection is its flexibility. Clients maintain greater control over network routing, enabling them to manage the initiation and termination of mitigation based on their specific needs. This control is particularly valuable for organizations with complex or dynamic routing requirements.

While On-Demand protection may reduce costs by minimizing throughput charges or avoiding overage fees, its primary benefit is the ability to activate protection only when necessary. This approach minimizes disruption and optimizes network performance during non-attack periods.

As with any On-Demand solution, there is typically a brief delay—often a few minutes—before protection is fully activated, due to the time required for network rerouting. During repeated or prolonged attacks, traffic must be re-announced for each new assault. Once the attack subsides, normal traffic flow resumes, ensuring minimal operational impact. This makes On-Demand DDoS protection an ideal choice for businesses seeking responsive and customizable mitigation.

b) Always-On Protection

With Always-On protection, both via DNS forwarding and BGP redirection, data traffic is continuously routed through a scrubbing center. This approach ensures reliable protection for the company's IT 365 days a year, 24/7.

Permanent filtering and cleansing of data traffic also reduces the burden in the company's IT infrastructure. This continuous monitoring minimizes downtime risk, ensuring uninterrupted business operations and maintaining user trust. Additionally, Always-On protection enables a faster response to threats, effectively neutralizing attacks before they can impact the organization's network or services.

DDoS protection providers should offer flexible deployment models. A combination of Always-On and On-Demand solutions can address the diverse protection needs of complex infrastructures. For example, organizations can use Always-On protection for their applications and pair it with event-driven, On-Demand protection for email and database servers.

4. FILTER OPTIONS

There are two primary methods for filtering traffic: static heuristics-based filtering and dynamic heuristics-based filtering.

a) Static Analysis

Static filters use predefined rules (blacklists) to check data traffic. The blacklist contains filter rules for known attack types. If, when comparing the behavior patterns of certain requests, matches with blacklist heuristics occur, the traffic is classified as DDoS.

Typical static filter rules include:

- Protocol (TCP, UDP, ICMP etc.)
- TCP flags, ICMP type
- Source and destination IP
- Rate limit per IP or network area

Filtering DDoS traffic using static rules is only as effective as the blacklist it relies on. For certain or new types of attacks, the system may fail to detect them as threats.

b) Dynamic Analysis

DDoS attackers are constantly discovering new vulnerabilities and open services that can be exploited for overload attacks. Recent Memcached and CLDAP attacks, as well as the emergence of the vectors WS-Discovery, Apple Remote Control, and DVR DHCP Discovery, show that companies face new attack techniques regularly.

The future of filtering lies in methods that proactively search for suspicious but undefined behavior patterns. During normal traffic periods, the protection solution learns the legitimate traffic profile of a website or network and derives normal ranges (whitelist). Deviations and unusual behaviors are then detected automatically through machine learning, preventing damage before it occurs.

5. AUTOMATION IN ATTACK DETECTION AND FILTERING

Human error is a leading cause of security breaches. With the increasing volume of alarm messages, critical events can easily be overlooked. To achieve real-time response and 100% detection of both known and previously unknown attacks, fast and reliable analysis processes must be highly automated. An effective DDoS protection solution employs advanced, adaptive filters calibrated to legitimate website traffic. Rather than relying on static exclusion methods, these filters utilize statistical behavior models to detect and block abnormal IP activity, ensuring minimal false positives. While blacklisting once the standard, whitelisting is gaining prominence by flagging traffic that deviates from established legitimate patterns as potentially harmful.

DDoS protection solutions should analyze incoming traffic at a granular level, offering a more refined approach than simple IP-based identification. This allows regular users to access systems seamlessly during an attack, without even noticing the filtering process.

Incoming traffic should be compared against historical attack data. Upon detecting an attack, only the malicious traffic is blocked, while legitimate data continues to pass through global filter clusters. These offloads traffic entirely, enabling seamless filtering in the background, unnoticed by users. To improve future detection, new attack patterns should be stored as dynamic filter rules.

6. PROTECTION FOR OSI LAYERS

DDoS attacks can be broken down based on the layers of the Open Systems Interconnection (OSI) model they target. Most attacks occur at the network (layer 3), transport (layer 4), and application (layer 7) levels. Efficient DDoS protection must extend to layer 7.

Application Layer (#7)

Detecting attacks at layer 7 is challenging because DDoS traffic mimics legitimate data. For example, It can attempt to overload CPUs and databases by targeting login pages or executing manipulated search queries on dynamic websites and feedback pages. However, if the DDoS protection solution performs deep packet inspection, the information can be used to filter traffic using machine learning and artificial intelligence.

Examples: GET, TLS, HTTP GET, HTTP Post

Network Layer (#3)

Similar to transport layer floods, these attacks aim to overwhelm firewall bandwidth and rate limiting capabilities.

Examples: ICMP floods, IP Fragmentation, Amplification Attacks (DNS, NTP, SSDP)

Transport Layer (#4)

Volumetric attacks, or floods, consume bandwidth and slow down or stop web server performance.

Examples: SYN Flood, UDP Flood, ACK Flood, Connection Exhaustion Attacks (Sockstress, TCP)

7. MULTI-CLOUD SUPPORT

Companies increasingly rely on hybrid IT landscapes that consist of their own data centers, web services, and applications in private and public cloud. To mitigate risk, organizations should aim for consistent security standards across all digital work and business environments. However, the differing DDoS protection standards across clouds can create complex, distributed security challenges in multi-cloud set-ups. This often leads to high administrative overhead and inconsistent protection, ultimately weakening IT security. Comprehensive DDoS protection solutions from a single source are an effective way to manage the complexity and high demands on availability and performance. Deploying protection across all utilized cloud platforms is a proven strategy.

From technical, security, and compliance perspectives, this ensures consistent and reliable protection of the entire corporate IT environment. These solutions are intendent of cloud providers, customized for the organization, and flexible enough to scale within the cloud. Multinational companies with global operations also benefit from low latency when protecting their infrastructures.

8. COMPLIANCE

When securing digital business processes, companies must comply with various national and international regulations, such as the GDPR and the German Federal Data Protection Act (BDSG). An all-encompassing solution ensures both DDoS protection and legal compliance is essential. Challenges often arise if the protection providers have server locations outside the EU's GDPR jurisdiction. Additionally, if a provider outsources services to subcontractors, it can significantly reduce transparency, especially regarding compliance with legal requirements.

To ensure data and IT security, organizations should choose a provider based in Germany or Europe, eliminating the risk of data transfers to the US. European and German legislators impose strict data protection and security requirements, offering robust safeguards and simplifying regulatory compliance. To further reduce risk, select a provider with no branch offices in the US, to avoid potential access by US entities. Beyond legal considerations, EU-based providers often deliver technological advantages and have a deeper understanding of the European market and customer needs.

9. MONITORING AND VISUALIZATION

A web-based dashboard should offer comprehensive transparency and real-time monitoring of website and network traffic.

These dashboards offer extensive functionality, including the ability to configure customized protection parameters, conduct real-time traffic analysis, and log details of mitigated DDoS attacks.

Key features of a comprehensive dashboard include:

- Detailed reporting
- Blacklist/whitelist configuration
- Setup of static filter rules
- Management of globally distributed protection infrastructures and diverse protection profiles
- Alert notifications
- Flexible customization options

10. INTEGRATED PLATFORM FOR DDOS-RELATED SERVICES

Integrating DDoS protection with other IT security solutions ensures comprehensive performance and availability protection at both network and application levels. A 360-degree approach, incorporating tools such as web application firewall or secure DNS services, further strengthens security. A fully integrated solution from a single vendor eliminates critical security gaps offering benefits such as:

- Coordinated and interconnected services
- Scalable protection features
- API integration for seamless compatibility with existing IT infrastructure
- Reduced training and administrative efforts

Choosing a unified platform eliminates inefficiencies and costs associated with managing multiple parallel solutions, streamlining and strengthening the overall security strategy.

11. SUPPORT AND MANAGED SERVICES

Comprehensive DDoS protection depends on reliable, expert support that ensures uninterrupted operations. Essential support features include:

- **24 / 7 Availability:** A dedicated support team reachable via email and phone to resolve incidents, answer questions, and address other needs.
- **Proactive Monitoring:** A SOC team that monitors platform health, detects anomalies and incidents and resolves them promptly.
- **SLA:** Defined response times, ranging from minutes to hours, as outlined in service level agreements (SLAs).
- **Onboarding Assistance:** Experts teams to facilitate seamless onboarding, including deployment, configuration, and integration with SIEM/SOC and CI/CD pipelines.

CONCLUSION

Selecting the right DDoS protection solution is a critical decision that directly impacts the security, resilience, and availability of your organization's IT infrastructure. As DDoS attacks grow more sophisticated and large-scale, businesses must prioritize solutions that address current security needs while remaining adaptable to future threats.

This Buyer's Guide outlines the essential features and criteria to consider, from scalability and automation to multi-cloud support and compliance. By thoroughly evaluating your organization's unique requirements—whether it's Always-On protection, hybrid deployment models, or integration with broader IT security frameworks—you can ensure comprehensive defense against DDoS attacks.

Partnering with a trusted, experienced DDoS protection provider brings peace of mind, allowing your organization to focus on core operations without compromising security or compliance. Investing in a robust, tailored solution will safeguard critical digital assets, maintain user trust, and enhance resilient in an evolving threat landscape.

ABOUT LINK11

Link11 is a global cloud security provider offering Network Security, Application & API Protection, and Application Performance solutions to a wide range of industries. From comprehensive Network DDoS protection to an advanced WAAP solution, our platform includes Web Application Firewall (WAF), Web DDoS Protection, Bot Management (including ATO), API Protection, and Secure CDN & DNS.

Link11's DDoS protection solution defends organizations against even the most sophisticated attacks, providing zero-time-to-mitigate for known threats and mitigation in less than 10 seconds for unknown attack vectors.

Get a Demo

LINK11