RED BUTTON
DDoS Experts

WHITEPAPER

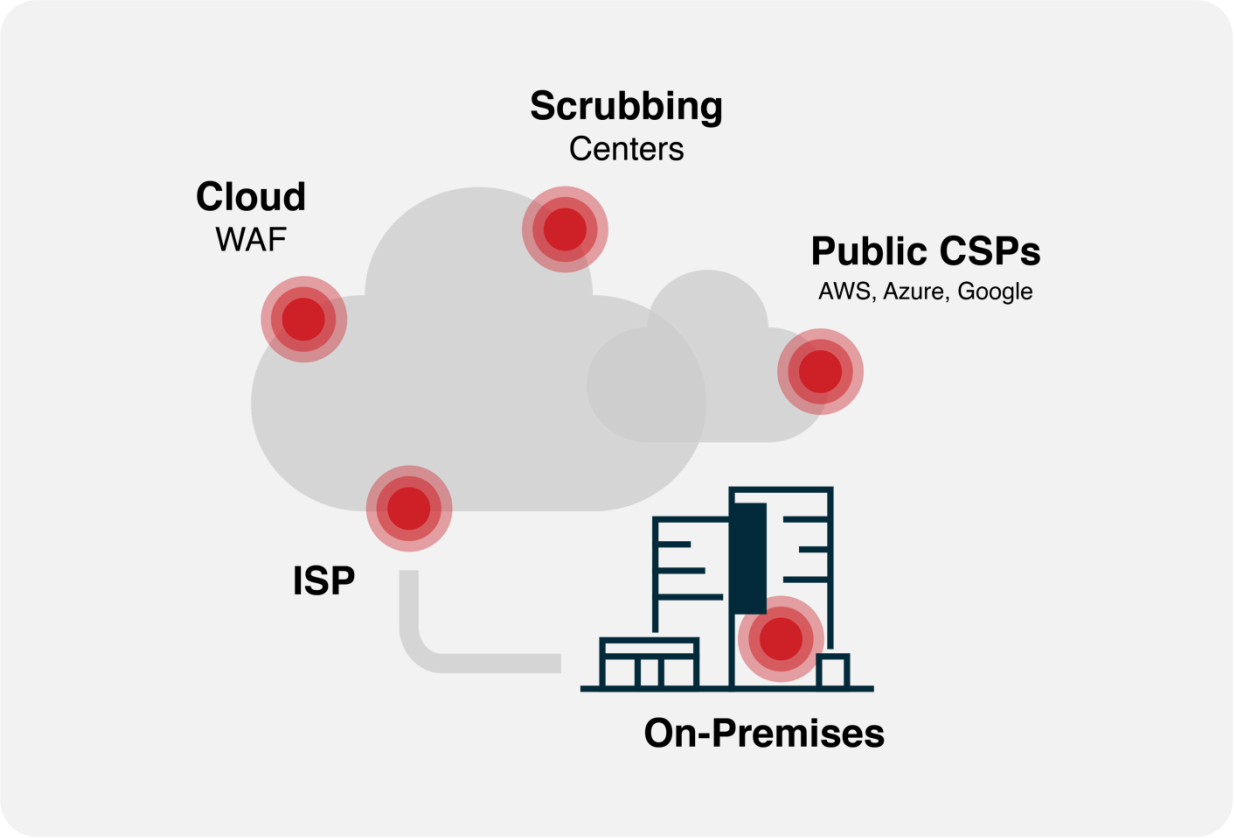
Understanding DDoS Protection Options

A DDoS attack is one of the more complex threats businesses face today. Given the intricacy of IT infrastructures and the sophistication of potential attackers, the optimal mitigation model would focus on a broad set of possible attack vectors.

Before examining specific DDoS security vendors, it is vital first to understand the topology, advantages and disadvantages of different protection options and the type of DDoS attacks they can block.

Essentially, there are five different locations for DDoS threat mitigation tools to be deployed:

- On-premises
- ISPs
- Cloud WAFs
- Scrubbing centers
- Public CSPs (cloud service providers)



On-Premises

On-premises DDoS protection consists of a dedicated hardware appliance or an on-premises web application firewall (WAF) installed in the data center. These allow you to protect your organization against layer 3 and 4 network attacks (using a dedicated DDoS solution) and against application-level attacks (using the on-premises WAF). Protection gear is installed at the network perimeter, between the internet router and network firewall.

The key drawback of on-premises protection is its inability to block DDoS attacks larger than the internet pipe effectively. This means that if the network pipe is saturated due to the attack volume, then the protection will simply not help. Another drawback is the lack of scalability needed to block large-scale network and application-level attacks, as WAFs were primarily designed for security against network intrusion and data theft.

Overall, on-premises DDoS protection has become less popular in recent years, with most organizations transitioning to cloud-based solutions.

ISPs

Many internet service providers (ISPs) provide DDoS protection for businesses. The attractiveness of this option is clear – a straightforward setup and hassle-free maintenance.

Yet, there is a price. First, this option only covers network layer vulnerabilities and does not protect against application-level attacks. Another important drawback is that small and medium ISPs cannot stop large volumetric attacks. However, very large ISPs, such as AT&T in the US, are an exception since they do have the bandwidth to absorb volumetric attacks.

In addition, DDoS security is not an ISP's core business, which means that its staff typically lacks the necessary expertise to respond efficiently. This can be a devastating discovery to suddenly make in the midst of an attack.

Cloud WAFs

With the migration of applications from private data centers to the cloud, cloud-based DDoS protection solutions have gained popularity over on-premises alternatives.

Cloud-based DDoS protection is based on companies offering CDN and cloud WAF solutions, including a DDoS mitigation layer. Traffic is diverted using DNS to the cloud provider, which can easily handle large volumetric attacks. Because the original server is not the one responding to requests, it's much harder for any DDoS attack to reach the targeted server.

Cloud WAFs also protect against application attacks, both static and dynamic. The one attack vector that cannot be blocked by cloud WAFs is **direct-to-origin** attacks.

Cloud WAF DDoS protection is easy to deploy and maintain. However, you have to provide your organization's private keys to the web provider. In some cases, such as for governmental entities, this requirement may be an insurmountable issue.

Scrubbing Centers

A DDoS scrubbing center holds DDoS mitigation equipment to handle large network attacks. Most vendors offer a solution consisting of multiple scrubbing centers, typically distributed globally. During an attack, traffic is diverted to the closest center and analyzed. Malicious traffic is removed, and legitimate traffic is passed on to the company's network.

You can use scrubbing center protection in two ways: direct traffic to a center on demand when an attack occurs or route traffic through scrubbing centers at all times.

A scrubbing center can stop any type of network attack, both web and non-web (FTP, SMTP, etc.) and direct-to-origin attacks. However, it cannot provide protection against application-layer threats.

Implementing a scrubbing center solution is more complicated than cloud WAF protection due to the need for BGP traffic diversion and GRE tunneling. You also have to own an **autonomous system** and network classes, but, on the other hand, private keys are not necessary. Another issue that should be considered is traffic latency, which can arise depending on the number, size and location of the scrubbing centers.

Public CSPs

Public cloud service providers (CSPs), such as AWS, Microsoft Azure and Google Cloud, typically provide DDoS protection as an 'out-of-the-box' part of their hosting packages.

The CSP takes responsibility for network protection and, as a customer, you get the inherent scalability of cloud data services. On the other hand, CSPs tend to charge separately for application-level DDoS mitigation.

Essentially, the CSP provides a built-in cloud WAF solution in which the configuration and ongoing management are your responsibility. CSP-based protection is less mature and sophisticated than what cloud WAF vendors have to offer as a point solution. However, the convenience of having all DDoS protection under a single roof is also of significant value to many organizations.

Which Attacks Will Be Blocked?

The choice you make regarding DDoS mitigation options is very much dependent on your priorities, technology, network size and expectations. Therefore, one key consideration is what types of attacks can be thwarted by which solution.

	On premises L3/4	On premises (WAF)	ISPs	Cloud WAFs	Scrubbing Centers	Public CSPs
Network attacks (web)	✓	✗	✓	✓	✓	✓
Network attacks (non web)	✓	✗	✓	✗	✓	✓
Very large network attacks	✗	✗	✗	✓	✓	✓
Direct to origin attacks	~~✓~~	~~✓~~	✓	✗	✓	✓
Application-level attack	✗	✓	✗	✓	✗	✓

Armed with an understanding of the options for protection from DDoS attacks, the next step is deciding what you actually need – and then finding the vendor who will provide it.