The bridge to possible

6 Key DDoS Protection SLA Metrics

The bridge to possible

The service-level agreement (SLA) is a crucial component of your organization's distributed-denial-of-service (DDoS) protection and your overall security preparedness. It is the contractual guarantee that outlines the level of DDoS protection your provider will deliver as well as their obligations to provide remedies in the event those guarantees are not met.

Many vendors make extensive claims about mitigation capabilities, but when it comes to contractual commitments, these claims often aren't backed up by written SLAs. It is fair to say that DDoS protection is only as good as its SLA.

Use these six questions to evaluate the SLAs that provide the backbone of your organization's DDoS protection. Each metric has a specific technical benchmark and defined business purpose. The absence of one or more of these KPIs can put your organization at serious risk in the event of a DDoS attack.

1. Time to Detect

The first step in stopping a DDoS attack is recognizing that an attack is taking place. Many vendors make misleading claims about mitigation time because they are unclear about when the time to detect begins. The sooner an attack can be identified the sooner that attack can be mitigated. With a **Time-to-Detect** SLA, your DDoS mitigation vendor commits to how quickly they will detect an attack. If your contract does not include an SLA for time to detect, a DDoS attack may be well under way before it is detected.

2. Time to Alert

When a security event happens, you need to be the first to know about it. The **Time-to-Alert** SLA is crucial for ensuring that you're notified immediately if your organization is attacked. Failure to include this metric means that your DDoS provider will not commit to notify you immediately if an attack takes place. This creates considerable exposure and puts the burden on you to ensure that your organization is alerted quickly if an attack takes place.

3. Time to Divert

For on-demand DDoS protection deployments, the time it takes the system to initiate a diversion is crucial to ensuring quick mitigation. Any delay in diversion can result in needless—and expensive—downtime. The **Time-to-Divert** SLA commits to how fast a mitigation provider will initiate diversion once an attack has been detected. Not having this metric in your SLA likely means that the DDoS mitigation provider lacks the technology or processes to ensure fast diversion, leaving you exposed for longer periods.

4. Time to Mitigation

Once an attack has been detected and diverted by/to your DDoS mitigation provider, you need to know how quickly your DDoS provider can mitigate the attack The **Time-to-Mitigate** metric measures the speed with which different types of attacks will be mitigated, based on attack characteristics. While most providers provide this commitment, there are still many that do not. This is a key metric, and unwillingness to commit to mitigation time should cast serious doubt on their ability to stop attacks.

5. Consistency of Mitigation

Another key consideration is the quality of mitigation. This is where it's important to read the fine print because "mitigation" can be defined differently by different providers, and definitions matter! The **Consistency-of-Mitigation** metric provides a baseline to calculate the effectiveness of mitigation and how much attack is allowed to go unmitigated. Customers should look for a mitigation threshold that allows less than 5% of attack traffic to be unmitigated. Failure to include a consistency-of-mitigation commitment in an SLA effectively renders time-to-mitigate commitments meaningless because vendors can consider almost anything to be "mitigation" and claim that they are meeting their SLA commitments.

6. Service Reliability

Finally, when under attack, you need assurances that your mitigation service will be there to ensure that your organization is protected and available. The Service Availability metric defines uptime requirements for service and the maximum amount of downtime per year. A high-quality service will commit to at least 99.999% uptime, which means only about 5 minutes of allowed downtime throughout the year. If an SLA does not include a service availability commitment, that should make you question whether your DDoS provider can guarantee service availability when you come under attack.

Secure DDoS Protection solutions are sold by Cisco through their global OEM partnership with Radware.

These six performance indicators are crucial to guarantee the effectiveness of your DDoS protection and the resilience and availability of your organization. These metrics should be outlined in clear, straightforward terms in your SLA document.

If you don't see them, ask your DDoS provider what their commitment is to these SLAs and how they guarantee that they will meet them.

Industry-leading SLAs

Cisco® Secure DDoS Protection solutions are sold through Cisco's global OEM partnership with Radware. Secure DDoS Protection offers the industry's most extensive and granular service-level commitments, ensuring the highest quality of DDoS protection. Secure DDoS Protection's SLA provides individual commitments to time-to-detect, time-to-alert, time-to-divert, time-to-mitigate, consistency-of-mitigation, and service availability.

Need more information?

Visit www.cisco.com/go/secure-ddos today!