SysEleven

SysEleven DDoS Guard

We have developed the SysEleven DDoS Guard to provide you with an effective protection against DDoS attacks while also having transparent pricing. High performance components and the know-how of our cloud and network teams provide you with all-round protection.

Our Peering-Partner:

DE-CIX amsix swissix SWISS INTERNET EXCHANGE

and many more

Your advantages with the SysEleven network:

- More than 500G edge capacity
- The best peering — connected to DE-CIX, AMS-IX, BCIX, NL-ix, and SwissIX
- Direct connections to Amazon, Google, Facebook, Apple, Netflix, Twitch, and many more
- Direct connection to Deutsche Telekom
- Operations certified under ISO 27001 native and ISO 27001 under BSI's IT baseline protection

You choose your connection:

- with VLAN on IXP platforms
- with Cross Connect/PNI
- with GRE Tunnel
- in combination with transit services
- Always-On und OnDemand pro IP
- self-onboarding through BGP communities

SysEleven Carrier Services made with ♥ in Berlin

All features at a glance:

- automatic engineering for DDoS traffic
- FlowSpec mitigation/traffic washing
- selective blackholing (drop traffic outside of Europe)
- manual mitigation for previously unknown attack vectors (inline TCP dumps possible at all times)
- L3/L4 anomaly detection and mitigation
  - through Src IP/TCP/UDP sessions/connections
  - through TCP Syn proxy
  - ICMP/SCTP sweeping
- upstream filtering up to L4
- geofiltering upon request
- reporting and alarms
- access to mitigation portal

All of your automated filter protections at a glance:

DNS Floods

A DNS flood attack interrupts the DNS resolution. This causes the performance of your website, API, or application to no longer be sufficient or interrupts availability.

UDP Floods

Attackers use the functions of an open DNS or NTP resolver to overload a target server or network by increasing server requests to where the load is significantly higher than the original requirements.

HTTP Floods

An HTTP flood attack generates vast numbers of HTTP, GET or POST requests from various sources. They target the application layer and degrade the service or even cause it to go offline.

Other types of filter protection

SY flood, SYN-ACK flood, ACK/push flood, fragmented ACK, RST/FIN flood, synonymous IP, fake sessions, session attacks, misused or out of protocol attacks, peplay verb attacks, faulty application protocol attacks, UDP fragmentation attacks, VoIP flood, media data attacks, ICMP floods, fragmentation flood, ping flood, and many more

The SysEleven DDoS Guard can be combined with other SysEleven products like F5 load balancing and web application firewalling.

Get in touch with us at carriersales@syseleven.de