LINK11

WEB APPLICATION FIREWALL

A STRONG PARTNER

COMPANY

Link11 - longstanding security experience

Link11 is a European IT security provider, headquartered in Frankfurt, Germany with operations in Europe, the US and Asia. Established in 2005, Link11 has been pioneering DDoS protection since the early days of attacks. Its **Cloud Security Platform** is focused on security-related services like **a Content Delivery Network (CDN), DDoS protection, Web Application Firewall (WAF), secure DNS hosting** and more.

The company's DDoS protection, a part of Link11's Cloud Security Platform, is entirely built using proprietary, patent-pending technology. **This state-of-the-art DDoS protection service for web applications and IT infrastructures uses Artificial Intelligence (AI)** and enables Link11 to protect mission-critical web applications, APIs and IT infrastructures against all types of DDoS attacks. This allows customers to focus on their core business.

With more than 11 years of experience in internet security and a clear security focus, Link11 has developed one of the most sophisticated DDoS protection services available. **Link11 protects some of Europe's largest media, financial, e-commerce and online organizations.** The company has won numerous awards and continues to innovate to ensure that Link11's IT security services are always one step ahead of the game.

Link11's global network is built to ensure resilience, performance and maximum availability for its customers' IT infrastructure. In recent years, Link11 has strengthened its network to offer the best possible protection, and the firm plans to further expand into Asia and the Middle East in the near future.

Link11's Strategic Points of Presence

London
Amsterdam
Helsinki
Frankfurt
Berlin
Prague
Paris
New York
Lisbon
Los Angeles
Miami
Vienna
Nuremberg
Zurich
Barcelona
Singapore

Why Web Application Firewalling?

Security incidents happen on a daily basis and we constantly read about new data breaches in the news. **The threat landscape evolves faster than ever before and web application attacks become more and more complex and persistent.**

Besides that, web application or web API owners face the challenge to distinguish non-productive traffic from bots, crawlers and spammers. At the same time, **changing business needs make it necessary for companies to adapt web applications and APIs.** New features need to be produced quickly and usage patterns change with every single release.

Web Application Firewalls protect against unauthorized data exposure. They can proactively protect websites and APIs against fraud or data theft. Businesses from all sectors that rely on storing private user data securely benefit from a Web Application Firewall. Even well accepted security standards like PCI DSS suggest to deploy a Web Application Firewall.

Every enterprise is a potential target for data theft and needs to protect their mission critical web applications, services and APIs.

LINK11 WEB APPLICATION FIREWALL

Link11's cloud-based Web Application Firewall (WAF) service is an add-on to the Link11 Web DDoS Protection. It protects applications and APIs against all common web application threats, including the Open Web Application Security Project's Top10 (OWASP Top10). Mission critical applications can get complete protection against all common web application threats and attacks with a single solution.

BENEFITS

- Protects critical web applications, APIs and services
- One-click deployment on top of Link11 Web DDoS Protection
- Global coverage using Link11 Cloud Security Platform
- Single point of contact for 24/7 support and emergencies
- Real-time access to Link11 WebGUI
- Attack reports
- State-of-the-art encryption (SSL/TLS)
- Specific front-end SSL/TLS settings
- Specific back-end SSL/TLS settings (reencryption)
- OWASP Top10 coverage out-of-the-box
- DoS/DDoS protection

Self-Learning DDoS Protection Based on AI

Link11's patent-pending DDoS proxy offers protection against non-volumetric and volumetric attacks. Protection is ensured from layer 3 to layer 7. Single-vector and multi-vector attacks get detected and mitigated. Sophisticated algorithms based on Artificial Intelligence ensure that even zero-day attacks are detected. Web application threats are detected and blocked. OWASP Top10 coverage out-of-the box.

State-of-the-Art Reporting and Monitoring

The Link11 WebGUI enables customers to monitor and configure all services via one common interface. It offers a consolidated view across all security modules from layer 3 to layer 7 and across all protected applications.

24/7 Single Point of Contact

The Link11 Security Operation Center (LSOC) acts as a single point of contact at any time. Network and security experts are available whenever needed, around the clock. This ensures that no handover to any other group or vendor is required.

Lowest Possible Time to Mitigate

Link11's patent-pending DDoS detection and mitigation mechanisms detect abnormal activities and mitigate even unknown and future attack types and vectors automatically in real-time. This is how we ensure a market-leading time to mitigate.

WE PROTECT YOUR BUSINESS

A cloud-based scrubbing service is a must-have today. DDoS attacks can easily take your internet facing applications offline in seconds. But enterprises need to take care of more than just DDoS – web applications and APIs also need protection against additional web application threats. A WAF is essential to ensure 360° application security. The Link11 WAF complements the Link11 Web DDoS Protection to cover today's most common web application security threats, known as the OWASP Top10. The solution is based on the OWASP ModSecurity Core Rule Set (CRS) to guarantee the best possible coverage. The rules are manageable and well documented.
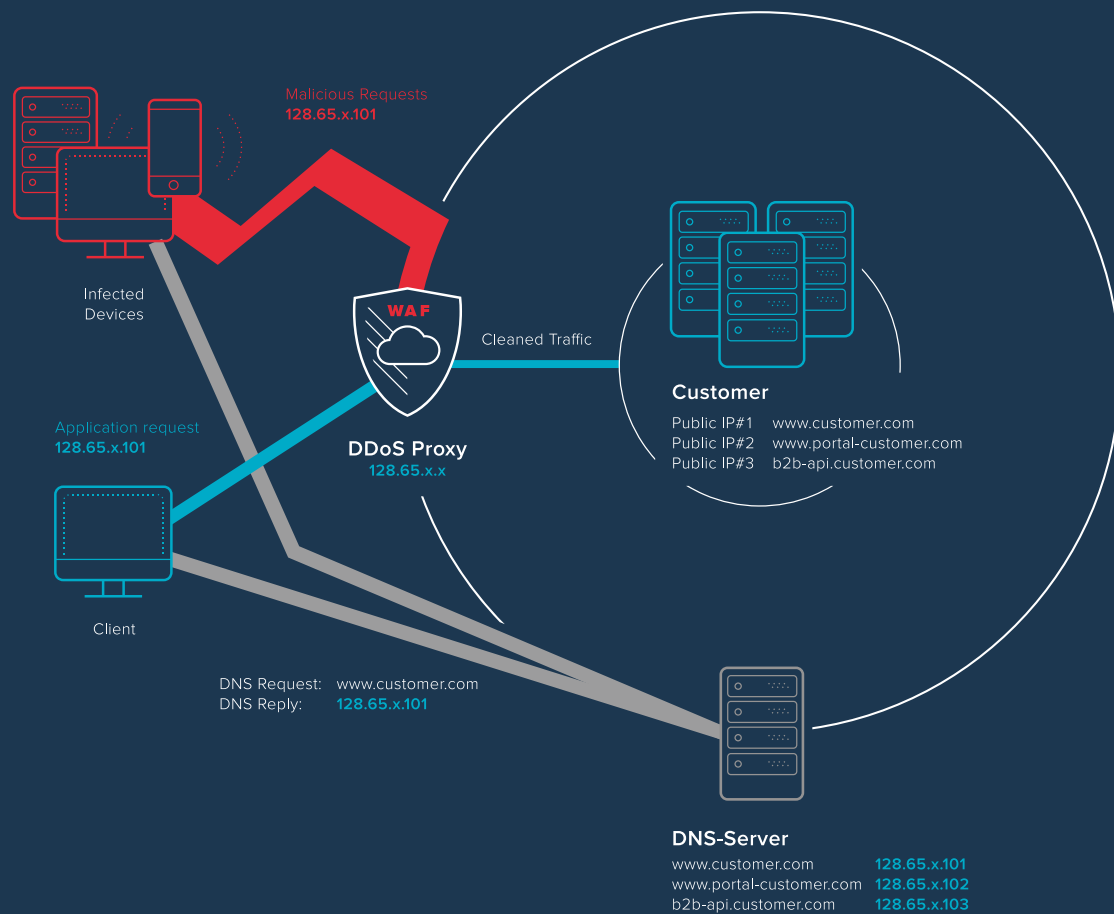
THE RULE SET PROVIDES PROTECTION AGAINST COMMON WEB ATTACKS AND HACKS LIKE:

- SQL Injections
- Cross-Site Scripting
- Local File Inclusion
- Remote File Inclusion
- Remote Code Execution
- Metadata/Error Leakages

- Scanner Detection
- Session Fixation
- Shellshock
- HTTProxy
- GeoIP Country Blocking

Together with Web Application Firewalling, Link11 Web DDoS Protection provides full coverage against attacks and threats at all layers. Protection of SSL/TLS encrypted services is also possible. Due to the solution's always-on deployment, customers get immediate protection against any type of DoS, DDoS attack or application threat that strikes their services.

Traffic is cleaned in Link11's Cloud Security Platform, and the cleaned traffic is sent back to the customer via the public internet. The protection services act as a proxy between clients/attacks and the customer. SSL/TLS Termination is possible and includes the ability to reencrypt traffic back towards the origin server. Implementation is fast and simple.

Link11 Web DDoS Protection with Web Application Firewall

Malicious Requests
128.65.x.101

Infected
Devices

Application request
128.65.x.101

DDoS Proxy
128.65.x.x

WAF

Cleaned Traffic

Client

Customer

Public IP#1   www.customer.com
Public IP#2   www.portal-customer.com
Public IP#3   b2b-api.customer.com

DNS Request: www.customer.com
DNS Reply: **128.65.x.101**

DNS-Server
www.customer.com   **128.65.x.101**
www.portal-customer.com   **128.65.x.102**
b2b-api.customer.com   **128.65.x.103**

CONTACT OUR EXPERTS

Do not lose the race! The attack landscape is changing rapidly, and attackers find new ways to take down their targets on a daily basis. Ransom DDoS has become more and more popular – who knows who will be hit next?

DDoS protection is a mandatory pillar of any security strategy. Get in touch with the experts from Link11 to gain access to the world's leading DDoS protection for web applications, services and APIs.

link11.com   +49 (0) 69 264 929 777   sales@link11.com