Backbone DDoS Protection

Reactive protection against volume attacks for Internet access & bandwidth directly in the Telekom backbone

Avoid DDoS attacks before they paralyze your organization.

DDoS attacks have reached a new level of escalation. As threats continue to increase in frequency, duration and sophistication, no single company is able to cope with high-volume DDoS attacks alone.

Today, organizations need external support to mitigate DDoS attacks in front of their own network. We mitigate DDoS attacks directly in our own backbone. There is no external rerouting to a third-party network. This is what makes the Telekom Backbone Product so unique for our customers.

To help stem the flow of attacks, we have launched our stateof-the-art IP Transit Security platform, available for Telekom IP Transit customers. It protects against volume dependent DoS and DDoS attacks, or spikes in traffic due to flash crowds (e. g. Black Friday Sale).

Key Attributes:

- A team of experts available 24/7, to ensure the safe delivery of our customers' content
- Traffic is exclusively handled in Tekeom's network! No third-party network is involved.
- Flexible and combinable four pillar defense against DDoS attacks (Mitigation Device, Filtering, Rate Limiting, Blackholing)
- Fixed monthly rate, no hidden charges
- Highest security and reliability standards due to continual analysis of IP flows
- Available for multihomed customers

Telekom has a 4-Pillar Mitigation Strategy:

- **Mitigation Device (Scrubbing):** Filtering and rejection of abnormal IP packets by a mitigation service. Redirection of individual addresses or the customer's entire IP address range using a mitigation device. This also includes the activation of automatic filtering.
- **Filtering:** Our filtering system separates malicious traffic from ordinary traffic by implementing edge router filter lists. These filter lists are manually configured on routers and deactivated after an attack has been stopped.
- **Rate limits:** Restriction of bandwidth (bandwidth throttling) for a dedicated service. In the event of an attack, the availability of the attacked service is limited, and only parts of the IP packets are routed to the target address.
- **Blackholing:** The entire data traffic to an IP address or to an IP address range is rejected. The IP address or IP address range is no longer available on the internet. This method of mitigation is only used as a last resort.

Benefits:

- More than 60 Tbps global interconnection capacity
- We partner with Arbor Netscout, the No. 1 DDoS Defense provider worldwide
- All major networks connected to Telekom's backbone
- Easy implementation – no configuration for the customer and no hardware deployment needed
- No latency caused by re-routing during an attack
- No GRE tunnels required
- Full BGP hijacking prevention
- No hardware deployment required
- No special prefix/route registrations needed, no prefix splitting

T · · Systems · Let's power higher performance

Solution Package for Backbone DDoS Protection

When to use?	▪ Mitigate DDoS attacks directly in the Telekom backbone
What is included?	▪ Reactive DDoS protection ▪ Protection against volume attacks
Which support is provided?	▪ Operating time: Monday – Sunday, 24 x 7 hrs. ▪ Reaction time: 30 minutes
How much does it cost?	▪ Onetime: 2.500€ ▪ Monthly: from 2.500€ (< 1 Gbits) ▪ 36 months fixed contract Product available only for Telekom IP transit customers. To all prices applicable VAT will be added.

Fit your DDoS protection to your specific needs through additional modules (prices on request)

Cloud Web DDoS Protection:
Out of the Cloud for local or hosted webservices

- Automatic protection
- Against complex and volume attacks

Border Gateway Protocol Cloud DDoS Protection:
Out of the Cloud for the Internet access

- Against complex and volume attacks
- Protection from DDoS attacks via several providers
- For the Internet access and bandwith

On Premise DDoS Protection:
On customer premise for the local infrastructure

- Automatic protection against complex attacks
- Combined with Backbone DDoS Protection: Automatic mitigation of volume attacks via **cloud signaling**
- For systems and applications

What is Cloud Signaling: Advanced services for highest and most convenient protection

With cloud signaling, we offer our customers an add-on service for combining on-premises DDoS protection with the DDoS Defense Backbone Protection.

To be able to use Cloud Signaling, a contract concerning on-premises DDoS Protection and Backbone DDoS Protection must be in place or concluded at the same time.

Contact
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Publisher
T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany