indevis
security in a connected world

Your benefits

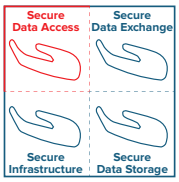
- Complementary DDoS protection for *indevis Datacenter and Virtualization Services* or *indevis Web App Secure*
- Multilayered protection system with alarm functionality
- Protection against volumetric attacks, transport protocol anomalies, attacks on Internet protocols and on services and applications
- Optional graphical user interface (WebUI) with realtime monitoring and reporting options
- No investment in hardware, future yearly software service level agreements, consulting or training courses
- indevis provides a helpdesk, providing relief to your own IT department

cloud services
MADE IN GERMANY

DO YOU WANT
TO KNOW MORE?

Your personal contact person will be happy to advise you and discover together with you what concept bestfits your needs.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de



INDEVIS DDoS PROTECT

COMPLEMENTARY DDoS PROTECTION FOR INDEVIS DATACENTER SERVICES

DDoS attacks can have the effect that a corporate website is not available and that important files and programs cannot be accessed. Serious economic damage can be the consequence for your company. Attacks of this kind can be repelled with DDoS protection enabling you to protect your company against downtime, loss of revenue and damage to your corporate image.

Distributed denial-of-service (DDoS) attacks have the intention of overloading a network infrastructure with large volumes of data. Hackers initiate DDoS attacks through bot networks on websites or web-based applications by sending large volumes of incomplete or false requests or protocol elements. The IT infrastructure becomes overloaded as a result and genuine requests can no longer be handled since the bandwidth is insufficient. The functionality of services is impaired in this way and the services are only available with restrictions to users and companies, or may not even be accessible at all. With *indevis DDoS Protect* you can protect yourself against service interruptions caused by DDoS attacks.

DDoS PROTECT: YOUR ADDITIVE PROTECTION SYSTEM

indevis DDoS Protect can be exclusively deployed complementary to the *indevis Datacenter & Virtualization Services* or *indevis Web App Secure*. You use *indevis DDoS Protect* to protect your company against volumetric attacks, transport protocol anomalies, attackson protocols such as TCP, http or https/TLS and on services and applications like DNS, SIP etc. Your data traffic is permanently monitored so that the DDoS protection system can independently detect attacks on IP addresses, IP address ranges (CIDR) and also on an Autonomous System (AS).

KEY FEATURES OF INDEVIS DDoS PROTECT

- Blocking of conspicuous users by means of defined threshold values
- Filter technology: behavioral monitoring of specific IP addresses, entire IP address ranges (CIDR) or Autonomous Systems (AS)
- Protocol verification by checking users and protocol standards
- Bogon filter: examination of the validity of IP addresses used
- Investigation of IP reputation using a global database
- Protection against flooding attacks
- Option for individual limitation of the data rate
- Geo-blocking: Option to block requests from specific regions and for restricting traffic according to geographical origin
- Whitelisting/blacklisting
- Layers 3, 4 & 7 DDoS protection

DDoS PROTECTION FOR LAYERS 3, 4 AND 7

The system can already detect anomalies in the transmission network by means of tracking and an alarm function, thereby enabling the appropriate defense mechanisms to take effect.

PROTECTION AT PROTOCOL LAYERS 3 AND 4 OF THE OSI LAYER MODEL

- The system can detect attacks by identifying anomalies (supported by tracking and alarm functions) if particular communication patterns for individual hosts outside normal network behavior are present.
- These communication patterns comprise the following: TCP-SYN, TCP-RST, TCP null, ICMP, IP null, IP-fragmented, DNS, UDP and IP private address traffic, including data traffic to and from IPv6 hosts.
- The following protocol anomalies/attacks can be detected: invalid packets and protocol violations, zombie detection (bot networks / zombie detection),TCP SYN authentication and HTTP authentication, DNS authentication, DNS malformed, HTTP malformed, SIP malformed, TCP connection reset (traffic detection only), baseline enforcement

LAYER 7 DDOS PROTECTION – REACTIVE PROTECTION
Application-specific protection at application level

- The system is capable of discarding dedicated HTTP packets with HTTP headers in accordance with configurable specifications.
- The system has the ability to block HTTP traffic on the basis of specific signatures with potentially malicious HTTP activities. The signature feeds are supplied from an IP reputation database with global access to metadata.
- The system can detect and discard faulty HTTP packets.
- The system can provide a number of selectable response options to faulty HTTP packets at different risk levels.
- Independently of the load, the system can detect and discard faulty HTTP packets if they do not comply to the standard, have invalid parameters or differ significantly from the typical behavior of clients.
- The system enables configurable threshold values (number of HTTP operations per second, per destination server) to be configured, based on which hosts can be blocked.
- The system enables configurable threshold values (number of HTTP operations per URL, per second, per destination server) to be configured, based on which hosts can be blocked.
- The system can use regular expressions to specify restrictions and filters for HTTP rate limiting, HTTP object detection and HTTP header recognition.
- The system can discard corrupt DNS requests.
- The system can terminate DNS floods from spoofed addresses.
- The system can block attackers sending DNS requests above a configured limit.
- The system can block faulty SSL/TLS requests.
- The system can block corrupt SIP packets.
- The system can block attackers sending SIP packets above a configured limit.

OPTIONAL: CLIENT USER INTERFACE (WEB UI) FOR REALTIME MONITORING AND REPORTING

The system has a graphical user interface that is opened in a standard browser; it can be provided as an optional add-on for a fee to view the status of configurable realtime data of the access point online.

Would you like to get to know *indevis DDoS Protect*? We would be happy to present our service to you in a demo session and explain the benefits of our additive DDoS protection system.

About indevis GmbH

Since 1999 indevis GmbH, ISO 27001 certified, has been providing IT security, datacenter and network solutions, accompanied by professional consulting, management and support services. In doing so, indevis fully meets the demands and requirements set out by the economic sector and public authorities and higher education institutions.

As one of Germany's leading managed security service providers, indevis is the partner for IT security and network technology for companies of all sizes and in any sector – after all, IT security is not a given, but rather has to be strategically planned.

indevis offices are located in two cities in Germany: Munich and Hamburg. Additional staff members work at a number of other locations distributed throughout Germany.

TÜV SÜD ISO 27001

indevis
security in a connected world

indevis GmbH

Irschenhauser Straße 10
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de