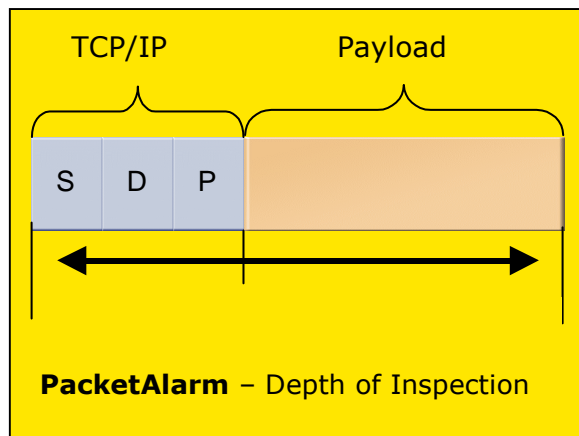


## PacketAlarm IDS & IPS Security Systems Seven reasons for their insertion

### 1. Why are the PacketAlarm IDS & IPS Products so important!

Cross-linking and global communication are company standards today, which without business life would not be the same. The extreme increase of system attacks has shown, that even with the prevention of firewalls and virus scanners, networks are still showing vulnerabilities. „Sobig“, „Sasser“, „Nimda“ and „CodeRed“, just to mention some of the current representatives of several hundred known network based attacks, have become synonyms for enterprise threats.

Within many organizations dominates still the erring assumption, that firewalls and Virus scanner alone are offering comprehensive protection. This opinion is so not correct. Firewalls are just processing data's at the TCP/IP protocol, such as Source, Destination and Port (SDP), but not the payload! In opposite thereto a virus scanner is only processing data's which are already on the local hard disk! Therefore this systems can in opposite to IDS/IPS-systems, which are processing both, the SDP- and the payload data's, not protect against network-based attacks.



and Virus scanner alone are offering comprehensive protection. This opinion is so not correct. Firewalls are just processing data's at the TCP/IP protocol, such as Source, Destination and Port (SDP), but not the payload! In opposite thereto a virus scanner is only processing data's which are already on the local hard disk! Therefore this systems can in opposite to IDS/IPS-systems, which are processing both, the SDP- and the payload data's, not protect against network-based attacks.

The costs which are associated with such attacks, respectively with to the system- and data recovery, can easily reach existential dimensions for every company. At a majority of systems even could not be recognised, that they are already attacked by worms and Trojans and could be attacked and conquered successfully again and again . In many organisations an instrument for a

continuously detection, inspection, traceability and prevention of attacks is missing. Thereby systems stay furthermore insecure and the security status of the systems or networks cannot be improved. PacketAlarm secures you comprehensive against such network attacks!



**The PacketAlarm product family offers IDS-, IPS-systems with a centralized administration, out of the box**

## 2. About which legal regulations, where IT-security is concerned, a company should pay attention?

Important out of today's point of view, is not just and only the protection of the IT-infrastructure, before a loss of availability, integrity and confidentiality, but also as well the legal alterations out of the near past.

The on the market not always, from many companies known, KonTraG (law for control and transparency in companies) is obliges companies, amongst others to the implementation of a risk-management. Will the company inflict a loss, by a lack of IT-Security, so can the management respectively the board of directors be made personally responsible by the act.

Affected there from are incorporations and companies, which are going to fulfil two of the following criterias within two sequenced years:

Total Assets	> 3,44 Mio. €
Turnover	> 6,87 Mio. €
Number of employees	> 50

As the before mentioned figures have shown, is this act not only applicable for larger medium-business and enterprises, as we hear it often from clients!

A further important subject are the bank ratings according to Basel II, which verifies the credit standing of organisations. Here flows the IT-security into the risk benchmark of an organisation. The relevance of an IDS/IPS implementation in addition to the common firewall and virus scanner is getting thereof very obvious. Because organisations with insufficient IT-security will get a poor rating, and therefore poor credit conditions.

The organisations do need better information's about the status of their IT-infrastructure, for a better risk management. Are there vulnerabilities in the network? Are networks or segments there out of, assailable? Are there actual



The PacketAlarm product family offers IDS-, IPS-systems with a centralized administration, out of the box

attacks to the network already happen, and how does they look like? How can we defend ourselves and how can we eliminate vulnerabilities of the network? All of these questions a PacketAlarm IDS/IPS-system is able to answer! With its defined actions it is able to contribute with a substantial and continuous amendment of the IT-security!

## 3. How is an IDS/IPS-system going to be defined and which components mark out the PacketAlarm products?

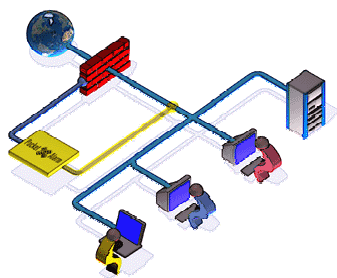
At the market there are currently offered Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and hybrid firewalls, which combine IDS/IPS with a firewall. In the following chart you will get the product features at a glance.

<b>PacketAlarm Product Features:</b>	<b>IPS</b>	<b>IDS</b>
	<b>Network based</b>	✓
<b>HA-Availability</b>	✓	✓
<b>Integration Layer 2 (Bridging Mode)</b>	✓	
<b>Integration Layer 3 (Routing Mode)</b>	✓	
<b>Passive Integration (Sniffing Mode)</b>		✓
<b>TCP-Reset and Firewall-Hardening</b>		✓
<b>Auto-Prevention</b>	✓	
<b>Event-Correlation</b>	✓	✓
<b>Anomalie Detection</b>	✓	✓
<b>Vulnerability Scanner</b>	✓	✓
<b>Sensor Management</b>	✓	✓
<b>Forensic Analysis</b>	✓	✓
<b>Auto-Reporting</b>	✓	✓
<b>Traffic-Trace</b>	✓	✓
<b>Automat. Software and Pattern Update</b>	✓	✓
<b>Integrated Signatures</b>	<b>&gt;6.200</b>	<b>&gt;6.200</b>
<b>Stateful Inspection Firewall</b>	✓	

#### 4. Integration options of PacketAlarm IDS/IPS and the Event-Correlation for the prevention of „false positives“?

##### PacketAlarm Intrusion Detection (IDS) – inspect and alarm

IT-Infrastructures with high security requirements do need an attack detection for entire network segments, or complete networks without interference of their availability and performance. Therefore PacketAlarm IDS is integrateable at central positions, such as core-switches or TAP-Devices. Invisible within the sniffing mode PacketAlarm IDS is listening at the network, reads all overflowing data's and is analyses them for may happen network attacks (i.e. DOS-Attacks, Exploits, Worms, unauthorized access). On the strength of its operation location at central switches the entire data traffic of a network segment will be analysed. The monitoring of the entire data traffic is therefore important, because attacks will not only come from external. According to statistics approx. 60-80% of the attacks to an enterprise network are coming out of the internal IT-scenery.

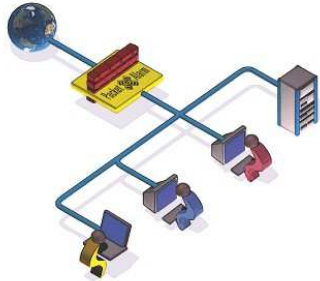


IDS System in sniffing mode for the inspection of the internal data traffic at a core-switch

Only the IDS-technology offers the possibility for the monitoring of the internal data traffic. A further benefit of the IDS-technology is, that in opposite to the IPS-technology, that with IDS it comes to no losses of performance and the availability of the network could not be reduced, because of the „Sniffing“ of the data stream. The passive Sniffing-Interfaces owns thereby no IP-Stack respectively IP-Address (Stealth-Mode) and is therefore not vulnerable.

## **PacketAlarm Intrusion Prevention (IPS) – inspect and eliminate**

PacketAlarm IPS detects detailed in real-time all data packets and only the actually desired data traffic flows freely along. The essential components of a PacketAlarm IPS-System are identical with those of PacketAlarm IDS. Identical because, only what's detected before as unwanted can be eliminated via an IPS. As two stage security concept represents an IPS often an entity with a „Stateful Inspection Firewall“. With both parts the data packets itself, and their content will be approved. Heart of the IPS is the Intrusion Prevention Engine, as down streamed active organ of the integrated firewall, which is finally responsible for the „pass“ or „drop“ of the data packets. Identified attack packets can thus dropped direct at the Gateway and do therefore not reach the target system.



**IPS System in inline mode**

In opposite to passive in Sniffing Mode operating IDS-Systems, are Intrusion Prevention Systems inline, that means installed within the data stream. A special feature of the PacketAlarm IPS Systems is the alternative possibility of the product integration as well on Layer 2, in „Bridging Mode“! Thereby is IPS able to be easily and quasi invisible integrated without any changes of the network configuration into existing topologies, without thereby e.g. to change anything at the Gateway. The PacketAlarm IPS-Systems are all available as High-Availability solutions (HA).

With all benefits the IDS- and IPS-Technology offers to the user, a critical point is up to the detection and minimization of so called „False Positives“ and „False Alarms“. False Positives are from the IDS/IPS reported attacks, which are in reality no attacks, because the data packets just look like coincidentally as a known attack. False Alarms are from the system alarmed attacks, for machines which we have not integrated in the network and which would not work in reality. Is the target system for example a Linux Apache Web server, a pure attack to an Windows IIS is not able to work thereof. A minimisation of false positives and false alarms happens in normal case by a continuous adjustment of the signatures for the protected network. The difficult field of the IDS/IPS-Technology is getting visible here. On one hand the minimisation, prevention of false alarms and on the other hand the fact, that persons and know-how should be available in organisations, which decide case to case how alarm messages will be handled. The PacketAlarm Event-Correlation with System-Attributes and found Vulnerabilities, offers therefore as single system an optimal solution to the market!

## **PacketAlarm Event-Correlation**

PacketAlarm uses a special function known as Event Correlation to check whether each specific attack that is identified could be carried out on the target system.

This decision is based on defined system- and service attributes (e.g. x86, Linux, Apache, Sendmail) and vulnerabilities detected by the Vulnerability Scanner.

**Found Attacks**  
**+ Vulnerability Scanner**  
**Results**  
**+ System-Attributes**  
  
**= Decision**

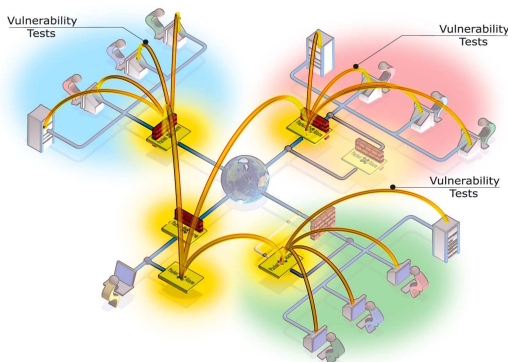
PacketAlarm correlates in real time both information's with the monitored attack as base of its decision. Each correlation increases thereby the probability, that it is a dangerous and achievable attack. The Event-Correlation with all PacketAlarm products determines in real time the expectations and reduces thereby the administration effort remarkable. Only relevant events will be marked for the administrator.

All PacketAlarm products have presently more than 6.200 attack signatures logged in all systems!

## **5. The PacketAlarm features, Vulnerability Scanner, Auto-Prevention and Anomaly-Detection!**

### **Vulnerability Scanner**

All PacketAlarm products dispose of a Vulnerability-Scanner, which automatically is reporting about in its scan area integrated machines and their vulnerabilities. Network attacks are using known vulnerabilities of operating systems for their attacks. Are those vulnerabilities known, remedy in form of patches und updates can be created. Therewith the attack is inefficient! The PacketAlarm



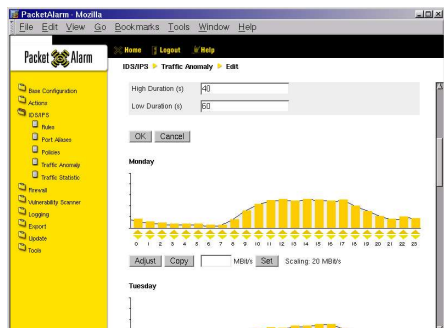
Vulnerability Scanner is automatically or manually able to analyse all in a network integrated machines for their vulnerabilities. For their remedy, reports are generated, which contain solution suggestions, up to given links for patches and updates. The found Vulnerabilities are, up to their final deletion, subject to the already described Event-Correlation.

### **Auto-Prevention**

An important aspect for the practical feasibility of an IPS is the so called Auto-Prevention functions. It reflects the basic function of the already discussed Event-Correlation, plus an automatically conversion of a recommended action, via a predefined policy. Of what avail is the best IPS-system for an user, when it does not contain predefined decisions for various attacks. Without Auto-Prevention, the administrator has to decide about his reaction for each signature manually and case by case. This effort is in practice barely to overcome. The PacketAlarm products offer this automatism! Is the Auto-Prevention function activated, the system is acting according to the preset activity- or policy-steps of our expert system. All of the more than 6.200 signatures are therein with its kind of defence predefined and new incoming pattern-updates will automatically be added to these directories. Important in this interrelation is, that reactions to attacks also still can be manually defined variational to the predefined policy-steps.

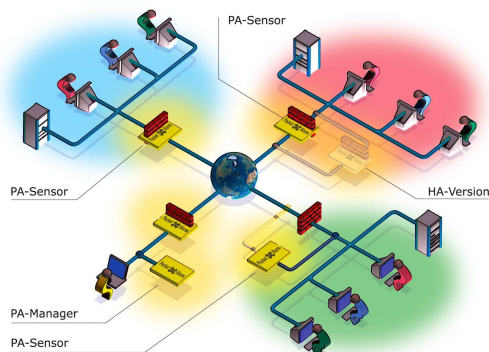
## Anomaly-Detection

Attacks and the effects of attacks often cause irregularities in data traffic. A sudden increase of the data amount or a drastically decrease of the data traffic, always points to exceptional events. An undershoot average volume of traffic, could be an advice for a totally shutdown service. A far transgressed average data traffic gives, is also an advice for an attack. The PacketAlarm Anomaly-Detection learns now, what data volume is considered as "normal", and this can also be configured by administrators. It can notify the percentage over- or undercutting from the defined „normal" data appearance. PacketAlarm can notify these variations for net's, machines and single ports.



## 6. The PacketAlarm features: Sensor Management, Forensic Analysis and Traffic-Trace!

The PacketAlarm Sensor-Manager feature allows to install any number of PacketAlarm systems as sensor for the monitoring of network segments or complete networks. These singular distributed sensors inside the net



infrastructure will than be configured, administrated and monitored via one centralised manager. The central management offers also the possibility of correlating the events over multiple sensors away. PacketAlarm offers furthermore the possibility to monitor installed IDS, IPS systems also centralised.

## Forensic Analysis

All PacketAlarm products support a detailed forensic analysis, of attacks on the network. A user-friendly query and display option lists the incidents occurring in a freely definable period into various categories. The risk of the event is shown (High, Medium, Low, Info) inclusive the entire attack packet, as well as their success feasibility and accordingly their relevance (via Correlation). PacketAlarm disposes in addition about the so-called Auto-Report function, which are combining the most important attacks and breach of the rules in one eMail-report, cyclical and automatically.

## Traffic-Trace

PacketAlarm products dispose by standard about Traffic-Trace functions. Beyond these functions conceals the possibility, to store not just and only the data

packet with the attack signature, but also any lot of afterwards following packets. With PacketAlarm on default adjusted are 30 more data packets. This applies as well for outgoing, as for incoming data's!

These functions are important for companies, which are committed by law to store the data traffic. At present does this belong to Swiss Banks, but it gives ambitions on the part of the EU for such an edict. It is just a matter of time until other European organisations will be faced with it.

## **7. The PacketAlarm Software- and Pattern updates**

### **Software- and Pattern updates and Services**

The more than 6.200 in PacketAlarm integrated signatures are constantly updated and supplemented with the newest. This happens with PacketAlarm, online and automatically each hour! By purchase of a PacketAlarm product the first 12 months of software- and pattern updates are included!

Additional information is available from: [www.packetalarm.com](http://www.packetalarm.com)