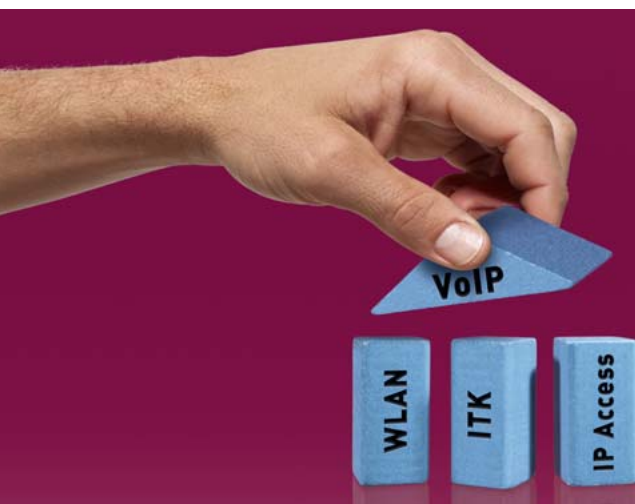




## funkwerk PacketAlarm IPS-/IDS-Systeme

**First Class Security.  
Intrusion Detection und  
Intrusion Prevention.**

**Packet  Alarm**  
SECURITY EMBEDDED



# Flexibel und zukunftsicher.

## Funkwerk Enterprise Communications: Allrounder für professionelle Sprach-Daten-Lösungen

Das Leistungsportfolio der Funkwerk Enterprise Communications umfasst professionelle Wireless LAN-Lösungen, Lösungen für IP-basierten Netzwerkzugang und IP-Netz-Absicherung sowie Systeme für VPN-Netze, Voice over IP und Voice over VPN. Hinzu kommen hochintegrierte modulare Telekommunikationslösungen auf ISDN/DSL-Basis sowie Personensicherungssysteme für Industrie und Dienstleistung auf GSM-, DECT- und Analogfunk-Basis.

Das umfangreiche Produktportfolio ermöglicht es Unternehmen unterschiedlicher Größe, Standorte via VPN miteinander zu vernetzen, mobile Mitarbeiter an die Firmenzentrale anzubinden sowie flexible, zuverlässige und schnelle Telekommunikations- oder Wireless LAN-Infrastrukturen mit umfassenden Leistungsmerkmalen aufzubauen.

Dabei steht das Thema Sicherheit im Vordergrund. Hierzu stellt das Unternehmen modernste Sicherheits- und Verschlüsselungstechnologien sowie IPS-, IDS- und UTM-Systeme für den Schutz Ihrer Unternehmensdaten bereit.

## Firmennetze: ein beliebtes Ziel für Angriffe

Mittlerweile sind beinahe alle geschäftlichen und industriellen Prozesse EDV-gestützt. Dies stellt höchste Ansprüche an die permanente Verfügbarkeit der IT-Infrastruktur. Unabhängig davon, ob es sich z. B. um E-Mail-Kommunikation oder ERP-Systeme handelt: Ein störungsfreier Betrieb ist ein wichtiger Erfolgsfaktor.

Die stetig steigende Zunahme von Angriffen durch Würmer, Viren, Trojanische Pferde, DoS-Attacken, Hackerangriffe, E-Mail-Spam oder anderen potenziellen Angreifern auf Unternehmensnetze stellt eine immer konkretere Gefahr für den geschäftlichen Arbeitsbetrieb dar. Erfolgreiche Angriffe verursachen mittlerweile Millionenschäden, mindern die Produktivität, verletzen Betriebsgeheimnisse und gefährden so letztlich die Substanz des Unternehmens.

Immer raffiniertere und intelligentere Schädlinge bedrohen auch Ihr Netzwerk. Wer nichts unternimmt, handelt fahrlässig. Die Anzahl und die Art der Angriffe auf Firmennetze sind in den vergangenen Jahren stetig zahlreicher und komplexer geworden. Die Zeiten, in denen eine Firewall und ein Virens Scanner als ausreichende Sicherheitslösung galten, sind endgültig vorbei. Es wird täglich wichtiger, sich gegen diese Gefahren zu schützen und Schaden durch Datendiebstahl oder -vernichtung vom Unternehmen abzuwenden.

Die IP-Sicherheitssysteme der Funkwerk IP-Appliances GmbH bieten hochwertige und anpassungsfähige Lösungen zur Sicherung ganzer Netzwerke, welche die genannten Risiken deutlich minimieren und somit nachhaltig die Sicherheit im Unternehmen verbessern. Nicht zuletzt aufgrund ihrer geringen Anschaffungs- und Betriebskosten garantieren sie darüber hinaus einen schnellen ROI (Return on Investment).

Die Systeme gliedern sich in zwei Produktgruppen:

### Funkwerk PacketAlarm IPS: Intrusion Prevention Systeme

Funkwerk PacketAlarm IPS wurde speziell für die Überwachung interner Netzwerkübergänge entwickelt und kann sowohl im Routing Modus auf Layer 3 als auch im Bridging Modus auf Layer 2 installiert werden. Durch die Möglichkeit der Integration auf Layer 2 kann das Produkt ohne langwierige und kostenintensive Umstellungen einfach und transparent vor internen Systemen installiert werden.

Werden Angriffe und Bedrohungen auf die zu schützenden Systeme erkannt, so werden diese automatisch geblockt und aus dem Datenstrom herausgefiltert.

### Funkwerk PacketAlarm IDS: Intrusion Detection Systeme

Gerade sensitive Infrastrukturen mit hohen Sicherheitsanforderungen benötigen eine Angriffserkennung, ohne dabei die Verfügbarkeit und die Performance zu beeinträchtigen.

Unsichtbar im Sniffing Modus lauscht das Funkwerk PacketAlarm IDS am Netzwerk und liest alle vorbei fließenden Daten mit. Alle Attacken werden aufgezeichnet und können alarmiert werden. Wird das Prevention System aktiviert, werden Angriffe mittels TCP Reset oder einem Firewall-Hardening verhindert.

Um auch ein Firewall-Hardening mit den Systemen anderer Hersteller oder mit selbst entwickelten Systemen zu ermöglichen, wird über eine spezielle Schnittstellendefinition, der Open Funkwerk PacketAlarm Architecture (OPA), kommuniziert. Funkwerk PacketAlarm IDS erkennt auch Angriffe in internen Netzwerksegmenten und ist der Spezialist für High Performance-Angriffserkennung. Durch die Sensor-/Manager-Architektur können alle Sensoren einfach und kostengünstig zentral administriert werden.

## Funkwerk PacketAlarm IPS-Systeme: High Performance Intrusion Prevention

Reine Firewall-Systeme ohne ein integriertes Intrusion Prevention System sind heute nicht mehr denkbar – zu vielfältig und „clever“ sind heute Würmer, Trojaner, Hacker & Co., um Bedrohungen nur mit einer rein auf IP und Portadressen basierten Entscheidung zu eliminieren. Doch ob ein einfaches Intrusion Prevention Add-on auf einer Firewall ausreicht, um die heutigen Gefahren abzuwehren, darf bezweifelt werden.

Funkwerk PacketAlarm IPS verfolgt hier eine ganz andere Strategie. Nicht das simple Reduzieren von Kommunikationsmöglichkeiten, sondern die detaillierte Untersuchung jedes einzelnen Paketes und die damit verbundene Möglichkeit, Angriffe gezielt zu erkennen, stehen im Vordergrund. Das Herzstück bildet die Intrusion Prevention Engine, die auf der Technik des bewährten Intrusion Detection Systems des Funkwerk PacketAlarm IDS beruht. Natürlich wird auf eine Multi Inspection Firewall nicht verzichtet – ganz im Gegenteil. Egal, ob es sich um die Event-Korrelation, den Schwachstellen-Scanner, die Anomalie-Erkennung oder die Auto-Prevention handelt, es wird immer die neueste Sicherheitstechnologie eingesetzt und stetig weiterentwickelt.

### Intrusion Prevention im Routing und Bridging Modus

Das Intrusion Prevention System des Funkwerk PacketAlarm IPS kann inline sowohl im Routing Modus auf Layer 3 als auch im Bridging Modus auf Layer 2 betrieben werden. Obwohl das Funkwerk PacketAlarm IPS im Bridging Modus „unsichtbar“ zwischen der Kommunikation sitzt, sind die Firewall und die Prevention Engine aktiv. So kann das Funkwerk PacketAlarm IPS auch vor WLAN Hotspots, Serverfarmen oder einzelnen Servern eingesetzt werden – an der Netzwerkconfiguration muss nichts geändert werden. DHCP, BootP, NT-Domain-Anmeldungen oder andere Broadcast-Kommunikationen funktionieren weiterhin, ohne dass ein Administrator eingreifen muss.

Die Funkwerk PacketAlarm IPS Appliance verfügt über eine, die Funkwerk PacketAlarm IPS Software über beliebig viele demilitarisierte Zonen – so genannte DMZs –, und dies im Routing und im Bridging Modus. So können gezielt Systeme mit sensiblen Daten oder Anwendungen abgegrenzt und geschützt werden.

### Multi Inspection Firewall

Die erste „Kontrollstation“ für den gesamten Datenverkehr ist die Funkwerk PacketAlarm IPS Multi Inspection Firewall. Sie überwacht in Echtzeit alle Datenpakete zwischen dem zu schützenden Netzwerk und den externen Netzen. Nur der tatsächlich erwünschte Datenverkehr fließt ungehindert weiter. Einfach und ohne großen Aufwand lassen sich die Regeln der Firewall konfigurieren und erlauben einen Einsatz innerhalb kürzester Zeit.

### Intrusion Prevention

Die Funkwerk PacketAlarm Intrusion Prevention Engine verfügt über mehr als 6000 Regeln und Signaturen (Stand: Januar 2007) zur Erkennung von Angriffen. Das System greift aktiv in den Datenverkehr ein und blockt Angriffe, bevor sie in das Netzwerk eindringen können.

### Auto-Prevention Funktion

Mit einer speziellen Auto Prevention-Funktion wird die Konfiguration vereinfacht und ein schnelles Anpassen der Regeln oder Regelgruppen an die unterschiedlichen Sicherheitsbedürfnisse der zu schützenden Systeme ermöglicht. Nur die Funkwerk PacketAlarm-Produkte verfügen über die Auto Prevention-Funktion und sind daher mit dem automatischen Regel-Update schneller gegen Angriffe geschützt als andere Systeme.

*Alle Funkwerk PacketAlarm-Produkte lassen sich in einem verteilten System beliebig kombinieren. Das Administrieren, Konfigurieren und Analysieren erfolgt über einen zentralen Manager.*

### Vulnerability Scanner

Mit dem leistungsstarken Funkwerk PacketAlarm Vulnerability Scanner werden die zu schützenden Systeme zielgerichtet auf Schwachstellen untersucht. Kontinuierlich fährt das Funkwerk PacketAlarm IPS-System Tests und listet die dabei gefundenen Vulnerabilities übersichtlich auf. Neben der gut strukturierten Darstellung werden umfassende Informationen zu den gefundenen Schwachstellen gegeben und zudem Empfehlungen ausgesprochen, wie diese beseitigt werden können.



## Event-Korrelation

Durch eine spezielle Funktion, die Event-Korrelation, überprüft das Funkwerk PacketAlarm IPS bei jedem entdeckten Angriff, ob er auf dem Zielsystem durchgeführt werden könnte. Dies wird anhand von definierten Systemattributen oder mit Hilfe der vom Vulnerability Scanner gefundenen Schwachstellen entschieden. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um einen gefährlichen Angriff handelt.

Bei der Ausgabe können die Angriffe mit niedriger Wahrscheinlichkeitsstufe herausgefiltert und so Fehlalarme vermieden werden. Natürlich kann der Administrator auch eigene Systemattribute erstellen, eigene Korrelationen zwischen Regeln und Attributen oder Schwachstellen bilden und bestimmen, um wie viel sich die Wahrscheinlichkeit der Gefährdung dadurch erhöht oder verringert.

*Funkwerk PacketAlarm IPS bietet die Möglichkeit, einfach und schnell eigene Intrusion Prevention Signaturen über einen komfortablen Regel-Editor zu erstellen.*

## Anomalie-Erkennung

Angriffe oder Auswirkungen von Angriffen verursachen oft Abweichungen im Datenverkehr. Ein plötzliches Ansteigen der Datenmenge oder das völlige Lahmlegen eines Internetdienstes können auf einen Angriff hinweisen. Mit der Anomalie-Erkennung zeigt das Funkwerk PacketAlarm IPS Abweichungen von definierten „normalen“ Datenmengen an und meldet diese. Welche Datenmenge „normal“ ist, kann das Funkwerk PacketAlarm System lernen und vom Administrator anpassen lassen. Anomalien können für Netze, einzelne Maschinen und sogar einzelne Ports auf Maschinen definiert werden. Gemeldet wird, wenn über eine definierte Zeitdauer eine bestimmte prozentuale Über- oder Unterschreitung eines üblichen Wertes festgestellt wird.

## Einfache Erstellung von individuellen Signaturen

Das Funkwerk PacketAlarm IPS bietet die Möglichkeit, einfach und schnell eigene Signaturen über die Management-Oberfläche zu erstellen. Die Regeln können über den Regel-Editor auch in Kombination, z. B. nach Source- oder Destination-Adresse, Ports, Pakettyp, Paketgröße oder Inhalt (z. B. Schlüsselwörter, Text oder Hexadezimal) und Häufigkeit des Auftretens innerhalb einer definierten Zeitspanne, erstellt werden. Damit können nach individuellen Wünschen bestimmte Verbindungen alarmiert oder terminiert werden, oder es kann auf andere Weise auf sie reagiert werden.

## Optimales Monitoring, forensische Analyse und Auto Reporting

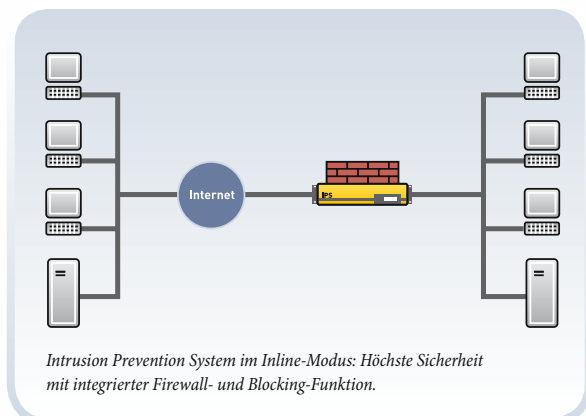
Das Funkwerk PacketAlarm IPS ermöglicht eine detaillierte forensische Analyse über die Angriffe auf das Netzwerk. Eine einfach zu bedienende Abfrage- und Anzeigeeoption listet innerhalb eines frei definierbaren Zeitraums die Vorfälle nach unterschiedlichen Kategorien auf. In der Anzeige wird die Gefährlichkeit der Events ausgewiesen (High, Medium, Low, Info). Dargestellt werden alle Angriffe, standardmäßig sogar inklusive des gesamten Angriffspakets. Funkwerk PacketAlarm IPS stellt Angriffe gebündelt nach Angriffsziel und Angreifer dar und verschafft so einen optimalen Überblick über attackierte Systeme.

Alle Daten, die für die Analyse benötigt werden, lassen sich problemlos exportieren. Über eine spezielle Auto Report-Funktion werden automatisch die wichtigsten Angriffe und Regelverstöße in einem übersichtlichen E-Mail-Report zusammengefasst. Es kann frei konfiguriert werden, ob die Reports täglich, wöchentlich oder monatlich versendet werden. Auch die Ausgabediagramme und -tabellen können nach individuellen Wünschen zusammengestellt werden. So haben Management, IT-Leiter und Administrator die Möglichkeit, sich genau die Daten anzeigen zu lassen, die für sie am wichtigsten sind.

## Open Funkwerk PacketAlarm Architecture (OPA)

Wird die Intrusion Prevention Engine aktiviert, kann das Funkwerk PacketAlarm IPS auf Angriffe reagieren und sie verhindern. Um auch ein Firewall Hardening mit Systemen anderer Hersteller oder mit selbst entwickelten Systemen zu ermöglichen, wird über eine spezielle Schnittstellen-Definition, die Open PacketAlarm Architecture (OPA), kommuniziert.

*Durch das automatische Software- und Pattern-Update sind die Funkwerk PacketAlarm Systeme immer auf dem neuesten Stand.*



## Funkwerk PacketAlarm IDS: High Performance Intrusion Detection

Netzwerkbasierete Intrusion Detection ist ein unverzichtbares Instrument innerhalb einer unternehmensweiten Security-Lösung. Keine andere Technologie ermöglicht die Echtzeit-Überwachung und Angriffserkennung der Kommunikationen in kompletten Netzwerksegmenten. So können Intrusion Detection-Systeme z. B. an Core Switches oder mittels TAP-Devices an zentralen Stellen implementiert werden und überprüfen damit die gesamte interne Kommunikation.

Laut aktuellen Studien kommen rund 60-80% aller Angriffe aus dem internen Netzwerk. Diese bleiben jedoch für Gateway-Sicherheitsprodukte unerkannt. Da die Intrusion Detection-Technologie zudem passiv im Sniffing Modus eingesetzt wird, ist der Datenstrom nicht beeinflusst und höchste Verfügbarkeit dadurch garantiert.

Das Funkwerk PacketAlarm IDS wurde speziell für die Überwachung von ganzen Netzwerksegmenten konzipiert. Durch die bewährte Scan- und Detection-Technologie sowie die Sensor-/Manager-Architektur liefert das Funkwerk PacketAlarm IDS ein Höchstmaß an Performance und Skalierbarkeit. Mit dem integrierten Schwachstellen-Scanner werden die zu schützenden Systeme permanent nach vorhandenen Schwachstellen untersucht.

Mittels der intelligenten Korrelation zwischen gefundenen Angriffen und vorhandenen Schwachstellen wird in Echtzeit ermittelt, welche Angriffe tatsächlich relevant und gefährlich für das Netzwerk sind. Alle Angriffsdaten und Systemchwachstellen werden in übersichtlichen Reports ausgegeben. Damit hilft das Funkwerk PacketAlarm IDS dem Administrator, wichtige Informationen von unwichtigen zu trennen, und schafft damit mehr Sicherheit bei geringen Administrationskosten.

*Die Funkwerk PacketAlarm Systeme verfügen über eine integrierte SNMP-Schnittstelle, mit der man statistische Daten von den Funkwerk PacketAlarm IDS-Systemen abrufen kann, um sich z. B. über CPU-Auslastung und Festplattenkapazität zu informieren.*

### Sichere Überwachung, sicheres Management

Das Funkwerk PacketAlarm IDS kann standardmäßig mit mehreren Interfaces zugleich sniffen und bietet dadurch die Möglichkeit, mehrere Netzwerksegmente mit einem System zu überwachen. Die Sniffing Interfaces besitzen keine eigene IP-Adresse (Stealth-Modus). Dadurch ist das Funkwerk PacketAlarm IDS selbst nicht angreifbar. Das Management Interface kann einfach in einem z. B. durch eine Firewall geschützten Segment platziert werden. Zusätzlich kann über die Funkwerk PacketAlarm Managementkonsole der Management-Zugriff auf bestimmte IP-Adressen beschränkt werden. Die Kommunikation zwischen Browser und Manager ist mittels Verschlüsselung geschützt.

### Intrusion Prevention im Sniffing Modus

Wird die Intrusion Prevention Engine aktiviert, kann das Funkwerk PacketAlarm IDS auf Angriffe reagieren und sie mittels TCP Reset oder einem Firewall Hardening verhindern. Um auch ein Firewall Hardening mit Systemen anderer Hersteller oder mit selbst entwickelten Systemen zu ermöglichen, wird über eine spezielle Schnittstellen-Definition, die Open PacketAlarm Architecture (OPA), kommuniziert.

### Vulnerability Scanner

Mit dem leistungsstarken Funkwerk PacketAlarm Vulnerability Scanner werden die zu schützenden Systeme zielgerichtet auf Schwachstellen untersucht. Kontinuierlich fährt das Funkwerk PacketAlarm IDS-System Tests und listet die dabei gefundenen Vulnerabilities übersichtlich auf. Neben der gut strukturierten Darstellung werden umfassende Informationen zu den gefundenen Schwachstellen gegeben und zudem Empfehlungen ausgesprochen, wie diese beseitigt werden können.



## Event-Korrelation

Durch eine spezielle Funktion – die Event-Korrelation – überprüft das Funkwerk PacketAlarm IDS bei jedem entdeckten Angriff, ob er auf dem Zielsystem durchgeführt werden könnte. Dies wird anhand von definierten Systemattributen oder mit Hilfe der vom Vulnerability Scanner gefundenen Schwachstellen entschieden. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um einen gefährlichen Angriff handelt.

Bei der Ausgabe können die Angriffe mit niedriger Wahrscheinlichkeitsstufe herausgefiltert und so Fehlalarme vermieden werden. Natürlich kann der Administrator auch eigene Systemattribute erstellen, eigene Korrelationen zwischen Regeln und Attributen oder Schwachstellen bilden und bestimmen, um wie viel sich die Wahrscheinlichkeit der Gefährdung dadurch erhöht oder verringert.

## Anomalie-Erkennung

Angriffe oder Auswirkungen von Angriffen verursachen oft Abweichungen im Datenverkehr. Ein plötzliches Ansteigen der Datenmenge oder das völlige Lahmlegen eines Internetdienstes können auf einen Angriff hinweisen. Mit der Anomalie-Erkennung zeigt das Funkwerk PacketAlarm IDS Abweichungen von definierten „normalen“ Datenmengen an und meldet diese. Welche Datenmenge „normal“ ist, kann PacketAlarm lernen und vom Administrator anpassen lassen. Anomalien können für Netze, einzelne Maschinen und sogar einzelne Ports auf Maschinen definiert werden. Gemeldet wird, wenn über eine definierte Zeitdauer eine bestimmte prozentuale Über- oder Unterschreitung eines üblichen Wertes festgestellt wird.

## Einfache Erstellung von individuellen Signaturen

Das Funkwerk PacketAlarm IDS bietet die Möglichkeit, einfach und schnell eigene Signaturen über die Managementoberfläche zu erstellen. Die Regeln können über den Regel-Editor auch in Kombination, z. B. nach Source- oder Destination-Adresse, Ports, Pakettyp, Paketgröße oder Inhalt (z. B. Schlüsselwörter, Text oder Hexadezimal) und Häufigkeit des Auftretens innerhalb einer definierten Zeitspanne, erstellt werden. Damit können nach individuellen Wünschen bestimmte Verbindungen alarmiert oder terminiert werden, oder es kann auf andere Weise auf sie reagiert werden.

## Optimales Monitoring, forensische Analyse und Auto Reporting

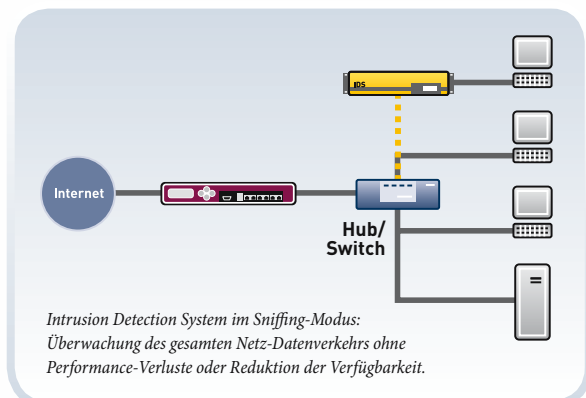
Das Funkwerk PacketAlarm IDS ermöglicht eine detaillierte forensische Analyse über die Angriffe auf das Netzwerk. Eine einfach zu bedienende Abfrage- und Anzeigeeption listet innerhalb eines frei definierbaren Zeitraums die Vorfälle nach unterschiedlichen Kategorien auf. In der Anzeige wird die Gefährlichkeit der Events ausgewiesen (High, Medium, Low, Info). Dargestellt werden alle Angriffe, standardmäßig sogar inklusive des gesamten Angriffspakets. Das Funkwerk PacketAlarm IDS stellt Angriffe gebündelt nach Angriffsziel und Angreifer dar und verschafft so einen optimalen Überblick über attackierte Systeme.

Alle Daten, die für die Analyse benötigt werden, lassen sich problemlos exportieren. Über eine spezielle Auto Report-Funktion werden automatisch die wichtigsten Angriffe und Regelverstöße in einem übersichtlichen E-Mail-Report zusammengefasst. Es kann frei konfiguriert werden, ob die Reports täglich, wöchentlich oder monatlich versendet werden. Auch die Ausgabediagramme und -tabellen können nach individuellen Wünschen zusammengestellt werden. So haben Management, IT-Leiter und Administrator die Möglichkeit, sich genau die Daten anzeigen zu lassen, die für sie am wichtigsten sind.

## Open Funkwerk PacketAlarm Architecture (OPA)

Wird die Intrusion Prevention Engine aktiviert, kann das Funkwerk PacketAlarm IDS auf Angriffe reagieren und sie verhindern. Um auch ein Firewall Hardening mit Systemen anderer Hersteller oder mit selbst entwickelten Systemen zu ermöglichen, wird über eine spezielle Schnittstellen Definition, die Open PacketAlarm Architecture (OPA), kommuniziert.

*Durch das automatische Software- und Pattern-Update sind die Funkwerk PacketAlarm-Systeme immer auf dem neuesten Stand.*



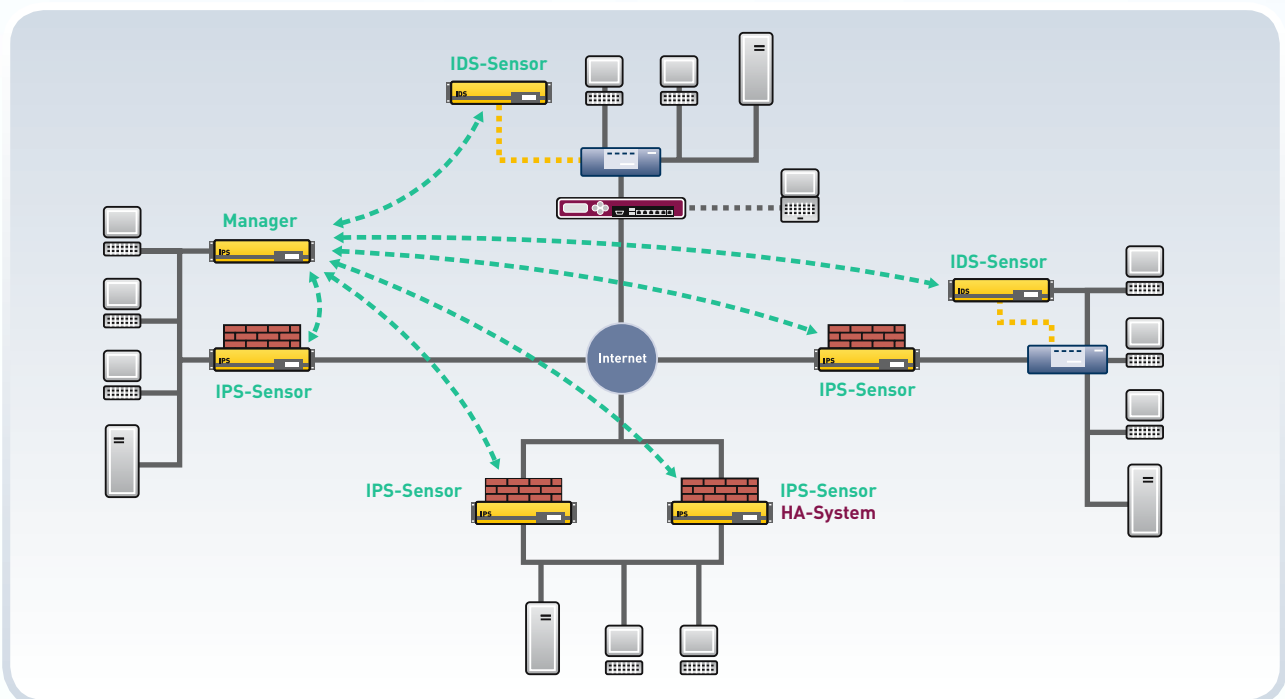
# Die Funkwerk PacketAlarm IPS-/IDS-Produktmerkmale im Überblick

Funkwerk PacketAlarm	IPS	IDS
Netzwerk-basierend	✓	✓
HA-Verfügbarkeit	✓	✓
Integration Layer 2 (Bridging)	✓	
Integration Layer 3 (Routing)	✓	
Passive Integration (Sniffing)		✓
TCP-Reset/Firewall Hardening		✓
Auto Prevention	✓	
Event-Korrelation	✓	✓
Vulnerability Scanner	✓	✓
Sensor-Management	✓	✓
Forensische Analyse	✓	✓
Auto Reporting	✓	✓
Traffic Trace	✓	✓
Automatisches Update	✓	✓
Integrierte Signaturen*	6000*	6000*
Multi Inspection Firewall	✓	

\*) Stand: Januar 2007



## Zentrales Management der Funkwerk PacketAlarm IDS-/IPS-Systeme durch Sensor-Manager-Betrieb

Alle Funkwerk PacketAlarm-Produkte lassen sich auch in beliebiger Anzahl als verteiltes System betreiben. Einzelne Sensoren werden dazu über die gesamte Infrastruktur verteilt und mit einem Manager zentral konfiguriert, administriert und überwacht. Die Sensoren können nicht nur lokal, sondern auch via Internet oder VPNs in Zweigniederlassungen mit einem zentralen Manager kommunizieren.




**Funkwerk PacketAlarm IPS Appliances**

inkl. 12 Monate Software und Pattern Update

Typ	Beschreibung	User		Appliance
IPS250	3x Gigabit	unlimited	19", 2 HE	
IPS100	3x 10/100 Mbit	unlimited	19", 1 HE	

**Funkwerk PacketAlarm IPS Software\***

inkl. 12 Monate Software und Pattern Update

Typ	Beschreibung	User		Software
IPS250	unterstützt Gigabit-Interfaces	unlimited		
IPS100	unterstützt 10/100 Mbit	unlimited		


**Funkwerk PacketAlarm IDS Appliances**

inkl. 12 Monate Software und Pattern Update

Typ	Beschreibung	User		Appliance
IDS250	3x Gigabit	unlimited	19", 2 HE	
IDS100	3x 10/100 Mbit	unlimited	19", 1 HE	

**Funkwerk PacketAlarm IDS Software\***

inkl. 12 Monate Software und Pattern Update

Typ	Beschreibung	User		Software
IDS250	unterstützt Gigabit-Interfaces	unlimited		
IDS100	unterstützt 10/100 Mbit	unlimited		

\*) Bitte beachten Sie unsere aktuellen Hardware-Anforderungen für die Funkwerk PacketAlarm Software unter [www.funkwerk-ip-appliances.de](http://www.funkwerk-ip-appliances.de)

**FAZIT:**

Die funkwerk PacketAlarm IPS-/IDS-Produktfamilie bietet mit ihrem Funktionsumfang für Netzwerke aller Größen eine technisch ausgereifte und preislich attraktive Lösung.

Durch ihre Flexibilität sowie ihre einfache Installation und Administration werden auch hohe Anforderungen an eine skalierbare IP-Sicherheitslösung erfüllt. Der Einsatz mehrerer Systeme erlaubt den unkomplizierten und wirtschaftlichen Aufbau eines umfassenden Sicherheitskonzeptes.

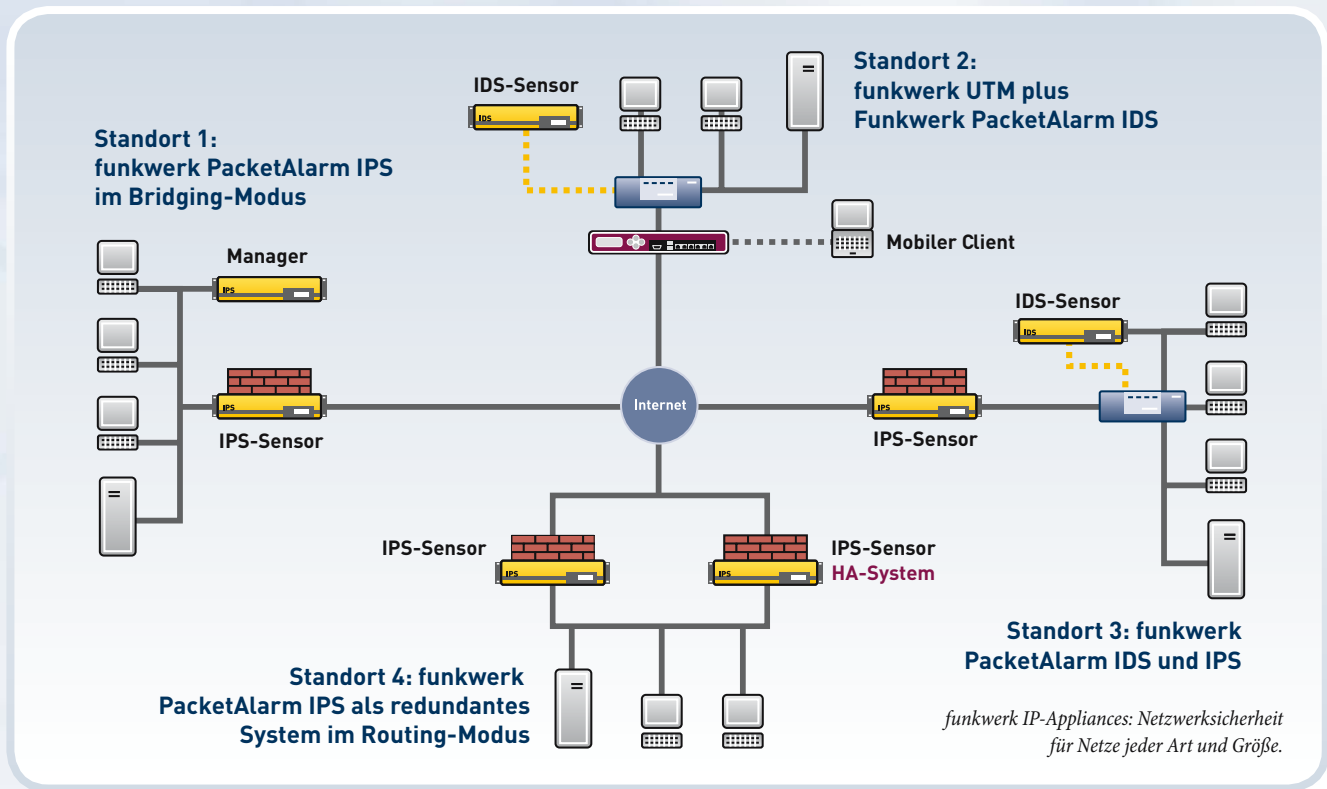
Die einzigartige funkwerk PacketAlarm Management-Technologie ermöglicht eine einfache zentrale Administration – unabhängig davon, ob nur eines oder mehrere Systeme eingesetzt werden.

funkwerk PacketAlarm IPS-/IDS-Systeme garantieren Investitionssicherheit und technologischen Vorsprung in puncto Angriffserkennung und Angriffsvermeidung.

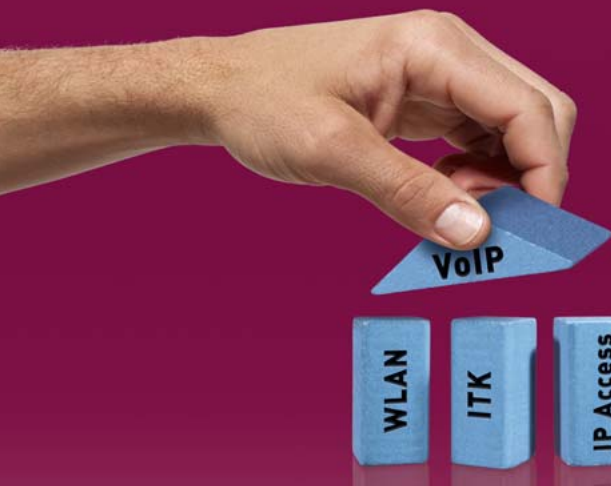
## LEISTUNGSMERKMALE FUNKWERK PACKETALARM IPS / IDS APPLIANCE- UND SOFTWARE-SYSTEME

Leistungsmerkmale	Funkwerk PacketAlarm IDS100	Funkwerk PacketAlarm IDS250	Funkwerk PacketAlarm IPS100	Funkwerk PacketAlarm IPS250
<b>Systemkonfiguration</b>				
10/100 Mbit-Ethernet ports	3	–	3	–
10/100/1000 Mbit-Ethernet ports	–	3	–	3
Prozessorgeschwindigkeit	2,8 GHz	2x 2,6 GHz	2,8 GHz	2x 2,6 GHz
RAM	512 MB	2 GB	512 MB	2 GB
Festplattenkapazität	80 GB	40 GB, SCSI	80 GB	40 GB, SCSI
Gehäuseform	19", 1 HE	19", 2HE	19", 1 HE	19", 2HE
<b>Systemleistung</b>				
Firewall-Durchsatz (Mbps)	–	–	1000	2800
Firewall- und IDS-Durchsatz (Mbps)	–	–	210	560
IDS-Durchsatz (Mbps)	210	560	–	–
Gleichzeitige Sessions	–	–	400.000	1.000.000
Benutzer	unlimitiert	unlimitiert	unlimitiert	unlimitiert
<b>Integration</b>				
Layer 2 (Bridging-Modus)	–	–	•	•
Layer 3 (Routing-Modus)	–	–	•	•
Passiv (Sniffing-Modus)	•	•	–	–
<b>Dynamische Intrusion Detection und Intrusion Prevention</b>				
IDS-/IPS-Signaturen	> 6.000*	> 6.000*	> 6.000*	> 6.000*
individuelle Signaturen	•	•	•	•
Vulnerability-Scanner	•	•	•	•
Korrelation mit System-Attributen in Echtzeit	•	•	•	•
Korrelation mit Vulnerability-Scanner in Echtzeit	•	•	•	•
Auto-Prevention	•	•	•	•
Forensische Analyse	•	•	•	•
Anomalie-Erkennung	•	•	•	•
Traffic-Trace	•	•	•	•
Port Scans	•	•	•	•
DoS	•	•	•	•
Buffer Overflow	•	•	•	•
Packet Fragmentation-Angriff	•	•	•	•
UDP-Angriff	•	•	•	•
Application Anomaly-Angriff	•	•	•	•
<b>System-Management</b>				
Sensor-Management	•	•	•	•
Anzahl Sensoren	Unlimited	Unlimited	Unlimited	Unlimited
Monitoring via SNMP	•	•	•	•
High Availability	•	•	•	•
<b>Logging</b>				
Interne Festplatte	•	•	•	•
Log an entfernten Syslog-Server	•	•	•	•
Log an SNMP-Server	•	•	•	•
E-Mail-Benachrichtigung von Angriffen	•	•	•	•
Win-Popups	•	•	•	•

\*) Stand: Januar 2007



Leistungsmerkmale	Funkwerk PacketAlarm IDS100	Funkwerk PacketAlarm IDS250	Funkwerk PacketAlarm IPS100	Funkwerk PacketAlarm IPS250
<b>Traffic-Management</b>				
Application Protocol-Analyse	•	•	•	•
RFC-Compliance-Prüfung	•	•	•	•
Threshold Analysis	•	•	•	•
Stateful Pattern Matching	•	•	•	•
<b>Administration</b>				
Auto-Reporting	•	•	•	•
Automatisches Echtzeit-Update	•	•	•	•
Konsolen-Interface	•	•	•	•
Web-GUI (HTTPS)	•	•	•	•
<b>Firewall-Modi und -Features</b>				
Stateful Inspection Firewall	–	–	•	•
NAT, PAT	–	–	•	•
<b>Technische Daten</b>				
Abmessungen	19", 1HE	19", 2HE	19", 1HE	19", 2HE
Höhe (mm)	46	88	46	88
Breite(mm)	435	560	435	560
Länge (mm)	360	450	360	450
Gewicht (kg)	7,3	15,0	7,3	15,0
<b>Stromversorgung</b>				
Eingangsspannung (VAC)	100 – 240	100 – 240	100 – 240	100 – 240
Frequenz (Hz)	50 – 60	47 - 63	50 – 60	47 – 63
Stromaufnahme (A)	5	8	5	8
Leistungsaufnahme (W max.)	200	435	200	435



**Flexibel und  
zukunftssicher.**

Funkwerk IP-Appliances GmbH  
Mönchhaldenstraße 28  
D-70191 Stuttgart

Telefon: +49 - 711 - 900 300-0  
Telefax: +49 - 711 - 900 300-90

E-Mail: [info@funkwerk-ip-appliances.com](mailto:info@funkwerk-ip-appliances.com)  
[www.funkwerk-ip-appliances.de](http://www.funkwerk-ip-appliances.de)