

secunet

secunet(snort

A Nose for the Network



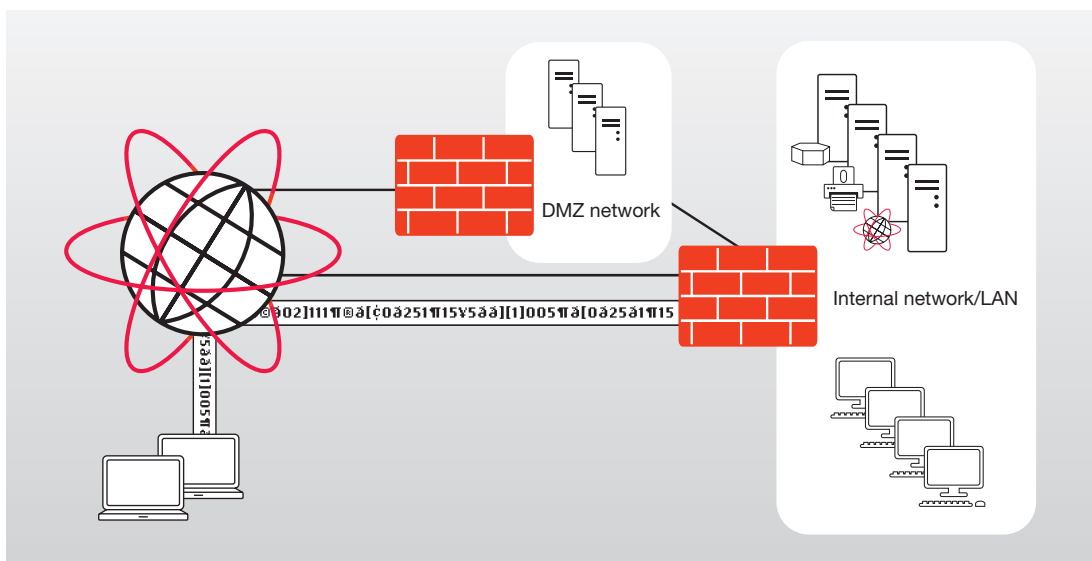
1	A popular target for attacks: the networks of companies and public authorities	3
2	Comprehensive protection for modern networks	4
3	secunet snort Intrusion Prevention System: examining and filtering data traffic	5
4	secunet snort Intrusion Detection System: examination of data traffic and alerts.	7
5	Product versions and IPS/IDS product features at a glance	9
6	Data Tables	10

1 A popular target for attacks: the networks of companies and public authorities

Global communication, mobile workstations, IT-supported business processes – this is standard in most of today’s organisations. For uninterrupted, seamless business operations, this means: integrity, confidentiality and availability of data are more critical for success than ever before. On the other hand, the number of network-based attacks continues to grow – the intensity of the attacks is rising, the intervals are decreasing, the threat has become a reality. Successful attacks reduce productivity and disclose company secrets. Consequently, they ultimately put the organisation as such at risk.

Firewalls and virus scanners are a good basis. But alone, they are no longer able to provide reliable protection for complex company networks against attacks from the web and from the company’s own network. Which additional measures and systems can successfully protect companies and organisations today?

Intrusion Detection Systems (IDS) are an indispensable addition to the IT security infrastructure; they provide an overview of all processes in the network and foil or analyse attacks wherever possible. One of the best known IDS applications is the open source tool snort, which has established itself as the de facto standard on the market.



Example of a typical network

2 Comprehensive protection for modern networks: **secunet**(snort)

secunet offers you a proven trustworthy and scalable solution for securing networks: secunet snort. Flexible and reliable attack detection is a must especially for complex IT infrastructures and those with special security requirements. With secunet snort, you considerably minimise the risk of attacks and sustainably improve the security of your organisation.

secunet snort provides you with a set of “ready-to-use” features and defaults, e.g. the auto-report function on attacks and rule violations. secunet snort also allows you to include individual configurations: your own settings and reports can be added to the system without any difficulty.

secunet snort flexibly adapts to your requirements

secunet snort is a modular system for a wide variety of applications. All possible application scenarios can be flexibly combined and linked. The use of several systems allows for the set-up of an extensive, uncomplicated and economical security solution. This makes secunet snort the perfect IT solution for mid-sized as well as large organisations.

secunet snort for maximum user-friendliness

With secunet snort, administration, configuration and analysis are carried out via a central, easy-to-use management system. Theoretically, the management system communicates with any number of sensors distributed in the network in any way whatsoever – which saves time and money.

You can use secunet snort either as an Intrusion Prevention System or as an Intrusion Detection System:

secunet snort Intrusion Prevention System

The secunet snort Intrusion Prevention System (secunet snort IPS) was specially developed for monitoring internal network gateways. It is usually installed inline at the level layer 2 in bridging mode. This guarantees simple and transparent installation upstream of the internal systems – without time-consuming and cost-intensive modifications. If the system detects attacks and threats to the systems under its protection, these attacks and threats are blocked automatically and filtered out of the data flow.

secunet snort Intrusion Detection System

Availability and performance cannot be compromised for attack detection. In sniffing mode, the secunet snort Intrusion Detection System (secunet snort IDS) is transparent and listens in on the network and reads all the data. It compares the content of the packets against characteristic patterns of well-known attacks. If the system detects an attack, an alarm can be triggered and the network packets can be logged for subsequent analysis or for the purpose of securing evidence.

3 secunet(snort) Intrusion Prevention System: examining and filtering data traffic

Firewall systems alone without an integrated Intrusion Prevention System no longer meet current requirements: today's worms, Trojans, hackers, etc. are too diverse. The secunet snort Intrusion Prevention System has an integrated firewall and analyses all packets in real-time – thus enabling targeted detection of attacks. Only data traffic which is actually desired and which complies with the rules is permitted to proceed without hindrance. The Intrusion Prevention Engine is the core of IPS. As the control entity, positioned downstream of the firewall, it determines whether packets are allowed to proceed or are blocked. The secunet snort Intrusion Prevention Engine has more than 7,000 rules and signatures for the detection of attacks. Attack packets are blocked directly at the gateway before they can penetrate the network.



Overview of the most important features and information on secunet snort IPS:

■ Intrusion Prevention in inline mode

The Intrusion Prevention System from secunet is usually used inline at the level of layer 2 in bridging mode. The firewall and Prevention Engine are active, with secunet snort IPS sitting right in the middle of the communication, yet practically transparent in bridging mode. This way, secunet snort IPS can even be used flexibly upstream of WLAN hotspots, server farms or individual servers – without any changes to the network configuration. DHCP, Bootp, NT domain logins or other broadcast communication continue to be fully functional.

■ Stateful Inspection Firewall as a secure control station

The secunet snort IPS Multi Inspection Firewall is the first control station in the network for all data traffic. It monitors all packets between the internal network and external networks in real-time. Only data traffic which is actually desired proceeds without hindrance. The rules of the firewall are simple to configure without requiring a lot of effort – and they are ready for use in next to no time.

■ Event correlation reduces the risk of false alarms

Using a special event correlation function, secunet snort IPS checks detected attacks to determine whether they could actually be executed on the targeted system. This way, attacks categorised as low-probability can be filtered out and false alarms are avoided. It is possible to easily add your own system attributes.

■ Anomaly detection as an additional warning function

Attacks generally have a tangible effect on the data traffic: a sudden rise in the volume of data or complete disruption of an Internet service may be indications of an attack. By means of anomaly detection, secunet snort IPS indicates and reports deviations from the defined rule. The system automatically learns what volume of data is considered “normal”. Alternatively, this data can be set manually by the administrator. It is possible to define anomalies for networks, individual machines and even individual ports on machines.

■ Optimum monitoring, forensic analysis and auto-reporting

secunet snort IPS allows clear and detailed forensic analysis of all attacks on the network. **All** disruptions are displayed in the data output and directly assigned various categories (High, Medium, Low, Info). secunet snort IPS represents attacks grouped by attack target and attacker, thus providing an optimum overview of the system under attack. It is possible to quickly and flexibly export all data typically required for an analysis. The most critical attacks and violations of the rules are summarised in clear, freely configurable reports by means of the auto-report function. This helps the administrator to differentiate between important and unimportant information, ensuring additional security that requires little administrative effort.

■ Easy generation of individual signatures

With secunet snort IDS, it is possible to generate signatures quickly and easily via the management interface. The rules can also be defined in combination, e. g. by source or destination address, port, packet type or content and frequency of occurrence within a specified period of time. This allows for the specification of individual combinations which trigger the alarm.



Function principle of secunet snort as IPS

4 secunet(snort) Intrusion Detection System: examination of data traffic and alerts

No other technology enables real-time monitoring and attack detection of communication in entire network segments – it was for this very reason that we designed secunet snort. In sniffing mode, secunet snort IDS transparently listens in on the network and reads all data traffic – without any negative impact on system availability or performance. It compares the content of the packets against characteristic patterns of well-known attacks. By means of intelligent correlation of detected attacks and available system attributes, the system determines in real-time which attacks are actually relevant and dangerous to the network. If the system detects an attack, an alarm can be triggered and the network packets are logged for subsequent analysis or for the purpose of securing evidence.



Overview of the most important features and information on secunet snort IDS:

■ Secure monitoring, secure management

The standard version of secunet snort IDS is able to “sniff” several interfaces simultaneously – making it possible to monitor several network segments with just one system. The sniffing interfaces do not possess their own IP configurations and are therefore invulnerable to attacks. Management access can be limited to specific IP addresses. Communication between the browser and manager as well as between the manager and sensor is encrypted.

■ Event correlation reduces the risk of false alarms

Using a special event correlation function, secunet snort IDS checks detected attacks to determine whether they could actually be executed on the target system. This is determined by means of defined system attributes. The likelihood of an attack being dangerous increases with every match. This way, attacks categorised as low-probability can be filtered out and false alarms are avoided. It is easily possible to add your own system attributes.

■ Anomaly detection as an additional warning function

Attacks generally have a tangible affect on the data traffic: a sudden rise in the volume of data or the complete disruption of an Internet service may be indications of an attack. By means of anomaly detection, secunet snort IDS indicates and reports deviations from the defined rule. The system automatically learns what volume of data is considered “normal”. Alternatively, this data can be set manually by the administrator. It is possible to define anomalies for networks, individual machines and even individual ports on machines.

■ Easy generation of individual signatures

With secunet snort IDS, it is possible to generate signatures quickly and easily via the management interface. The rules can also be defined in combination, e. g. by source or destination address, port, packet type or content and frequency of occurrence within a specified period of time. This allows for the specification of individual combinations which trigger the alarm.

■ Central sensor manager operation

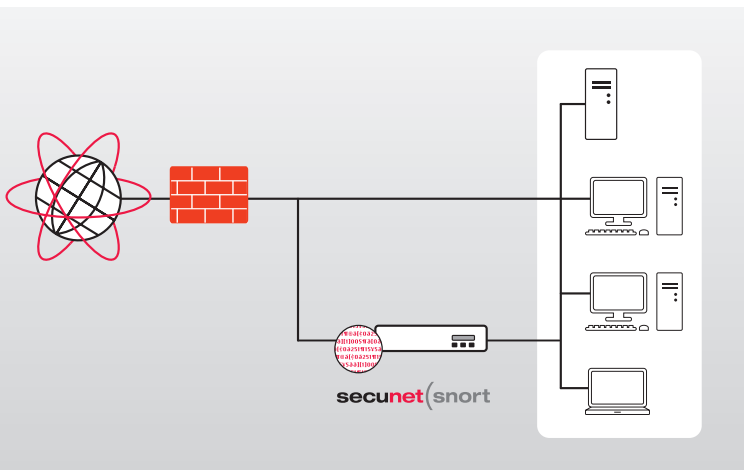
Any number of any secunet snort products can be operated as a distributed system. Individual sensors are distributed throughout the entire IT infrastructure and centrally configured, administrated and monitored by a manager. The sensors are able to communicate with the central manager via the Internet or Virtual Private Networks even if they are distributed.

■ Intrusion prevention in sniffing mode

If the Intrusion Prevention Engine is activated, secunet snort IDS can respond to attacks and prevent them by means of TCP resets or firewall hardening. In order to enable firewall hardening with systems from other manufacturers or with systems you have developed yourself, communication is via a special interface definition.

■ Optimum monitoring, forensic analysis and auto-reporting

secunet snort IDS allows clear and detailed forensic analysis of all attacks on the network. **All** disruptions are displayed in the data output and directly assigned various categories (High, Medium, Low, Info). secunet snort IDS represents attacks grouped by attack target and attacker, thus providing an optimum overview of the system under attack. It is possible to quickly and flexibly export all data typically required for an analysis. The most critical attacks and violations of the rules are summarised in clear, freely configurable reports by means of the auto-report function. This helps the administrator to differentiate between important and unimportant information, ensuring more security at low administrative cost.





Function principle of secunet snort as IDS



5 secunet (snort)

Product versions

secunet snort IPS appliances incl. 12 month software and pattern update

Type	Number of interfaces	User	Housing
IPS260	6x Gigabit	Unlimited	19", 2 RU 
IPS110	4x 10 / 100 Mbit	Unlimited	19", 1 RU 

secunet snort IDS appliances incl. 12 month software and pattern update

Type	Number of interfaces	User	Housing
IDS260	6x Gigabit	Unlimited	19", 2 RU 
IDS110	4x 10 / 100 Mbit	Unlimited	19", 1 RU 

IPS/IDS product features at a glance

Feature	IDS	IPS
Network-based	■	■
High availability	■	■
Integration layer 2 (inline mode)	—	■
Passive integration (sniffing mode)	■	—
TCP reset and firewall hardening	■	—
Event correlation	■	■
Anomaly detection	■	■
Sensor management	■	■
Forensic analysis	■	■
Auto-reporting	■	■
Traffic trace	■	■
Automatic software and pattern updates	■	■
Stateful inspection firewall	—	■
SNMP management	■	■
Integrated signatures	> 7000	> 7000

Data Tables

Performance Features	IDS 110	IDS 260	IPS 110	IPS 260
System Configuration				
10/100 Mbit Ethernet ports	4	—	4	—
10/100/1000 Ethernet ports	—	6	—	6
Processor speed	2,2 GHz	3,0 GHz	2,2 GHz	3,0 GHz
RAM	2 GB	4 GB	2 GB	4 GB
Hard drive capacity / Raid controller	250 GB S-ATA / -	147 GB (2x SAS) / 1	250 GB S-ATA / -	147 GB (2x SAS) / 1
Housing	19" 1 RU	19" 2 RU	19" 1 RU	19" 2 RU
System Performance				
Firewall throughput (Mbps)	—	—	1000	2800
Firewall and IDS throughput (Mbps)	—	—	210	560
IDS throughput (Mbps)	210	560	—	—
Simultaneous sessions	—	—	400000	1000000
Users	Unlimited	Unlimited	Unlimited	Unlimited
Integration				
Layer 2 (inline mode)	—	—	■	■
Passive (sniffing mode)	■	■	—	—
Dynamic Intrusion Detection and Intrusion Prevention				
IDS/IPS signatures	> 7000	> 7000	> 7000	> 7000
Individual signatures	■	■	■	■
Correlation with system attributes in real-time	■	■	■	■
Auto-prevention	■	■	■	■
Forensic analysis	■	■	■	■
Anomaly detection	■	■	■	■
Traffic trace	■	■	■	■
Port scans	■	■	■	■
DoS	■	■	■	■
Buffer overflow	■	■	■	■
Packet fragmentation attack	■	■	■	■
UDP attack	■	■	■	■
Application anomaly attack	■	■	■	■

Performance Features	IDS 110	IDS 260	IPS 110	IPS 260
System Management				
Sensor management	■	■	■	■
Number of sensors	Unlimited	Unlimited	Unlimited	Unlimited
Monitoring via SNMP	■	■	■	■
High availability	■	■	■	■
Logging				
Internal hard drive	■	■	■	■
Log to remote syslog server	■	■	■	■
Log to SNMP server	■	■	■	■
E-mail notification in case of attack	■	■	■	■
Win popups	■	■	■	■
Prelude Integration	■	■	■	■
Traffic Management				
Application protocol analysis	■	■	■	■
RFC compliance audit	■	■	■	■
Threshold analysis	■	■	■	■
Stateful pattern matching	■	■	■	■
Administration				
Auto-reporting	■	■	■	■
Automatic real-time updates	■	■	■	■
Console interface	■	■	■	■
Web GUI (HTTPS)	■	■	■	■
Firewall Modes and Features				
Stateful inspection firewall	—	—	■	■
NAT, PAT	—	—	■	■
Technical Data				
Dimensions:	19" 1 RU	19" 2 RU	19" 1 RU	19" 2 RU
Height (mm)	43	89	43	89
Width (mm)	426	426	426	426
Length (mm)	356	650	356	650
Weight (kg)	8	27	8	27
Power Supply				
Input voltage (VAC)	100 - 240	100 - 240	100 - 240	100 - 240
Frequency (Hz)	50 - 60	50 - 60	50 - 60	50 - 60
Current input (A)	5	10	5	10
Power consumption (max. W)	260	500 (2x)	260	500 (2x)

About secunet

secunet is one of the leading German providers of sophisticated IT security. In close dialogue with its customers – companies, public authorities and international organisations – secunet develops high-performance products and advanced IT security solutions. In doing so, secunet not only secures IT infrastructures for its customers, but also achieves intelligent process optimisation and generates sustainable added value.

More than 270 experts at secunet focus on issues such as cryptography (SINA), e-government, business security and automotive security with the objective to always remain a step ahead of the competition in terms of quality and technology. In its customer relationships, secunet strives to build long-term partnerships. This is impressively proven with the company's ongoing security partnership with the Federal Republic of Germany, which began in 2004.

secunet

secunet Security Networks AG

Kronprinzenstraße 30

45128 Essen, Germany

Phone: +49-201-54 54-0

Fax: +49-201-54 54-1000

E-mail: info@secunet.comwww.secunet.com