

# SECUREPOINT™

## INTRUSION DETECTION SYSTEM

# 2

## Identify attacks on your networks in real-time with Securepoint nuzzler server!

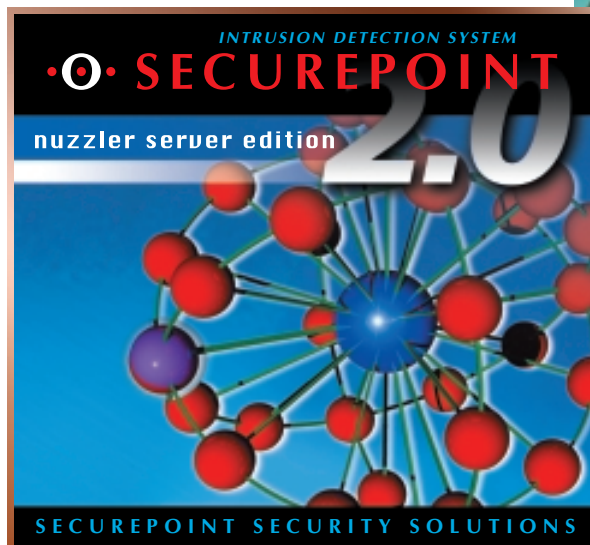
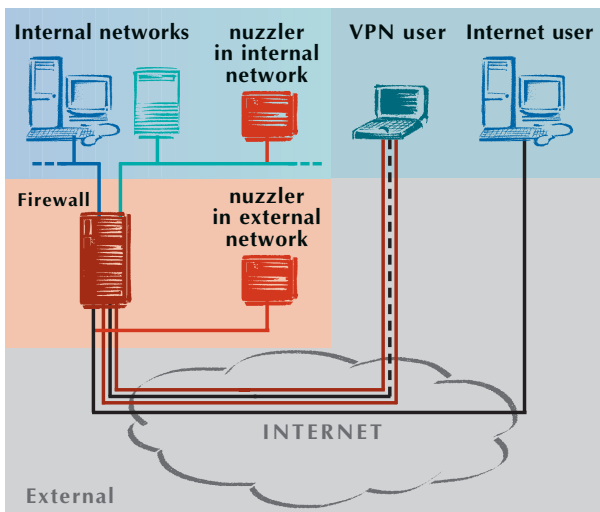
The network-based Securepoint Intrusion Detection System **nuzzler server edition** carries out a real-time inspection of the entire data traffic in your networks. The nuzzler IDS can be placed in different network segments. The nuzzler sensor is listening to the flow of data within the segments, without impeding network performance. nuzzler informs of an attack and can be connected with a **Securepoint Firewall & VPN Server** to give a high-end security system to you.

### Easy installation and graphical configuration

nuzzler is installed and activated in 3 minutes on a Windows™ 2000 and XP computer (A Linux version is available soon). It links the tried-and-tested nuzzler engine to an easy-to-use graphical user interface. The configuration is very easy. You have to specify your network address and start nuzzler. That's all.

### Reporting, informing and protecting

All network data is analysed and continuously searched for attacks. After identifying an attack, the attack data is recorded automatically, and the network admin will be informed. If a **Securepoint Firewall & VPN Server** exists, it can be auto-updated and a connection block with a temporary firewall rule can be done.



### Around 1.600 known attacks and automatic pattern update via the Internet

The database of attack signatures available is one of the most comprehensive and most detailed around. nuzzler covering around 1.600 known network attacks. All attacks are sorted in categories. On request, nuzzler automatically downloads the currently available attack signatures, scan engine and other software updates.

### Easy creation of individual attack signatures

New rules can be created in 3 steps with the nuzzler rule editor. You can put your own rules to individual categories. Combinations of rules can also be determined using the rule editor, for example by source or destination address, by port, packet type, packet size and content (keywords, text or hexadecimal) and by frequency or occurrence with a pre-defined time span. You can thus set alarms, terminations and create other kinds of reaction at specific connections, in accordance with your own requirements.

### Highest performance and better management

The high-speed, optimised scan engine generation 2 of nuzzler scans in real-time your network traffic without impeding the network performance. You can place different nuzzler servers in your network and administrate them over one nuzzler client.



# SECUREPOINT™

## INTRUSION DETECTION SYSTEM

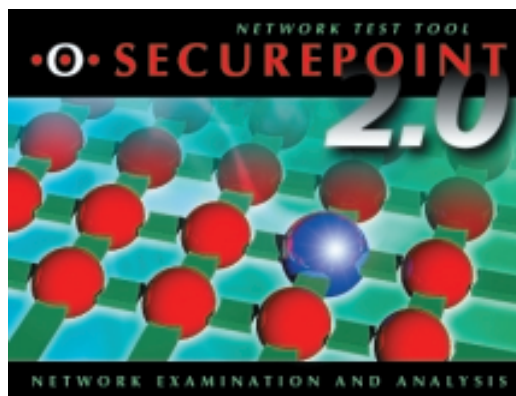


### nuzzler server edition features

Securepoint Intrusion Detection System: nuzzler server edition	
●	<b>Securepoint Client/Server architecture:</b>
●	Connect over one nuzzler client different nuzzler server
●	Connect Securepoint firewall with nuzzler server
●	<b>nuzzler IDS Engine generation 2:</b>
●	Performing scans on small to big networks
●	Scan of over 1.000 packages per second (PII 600MHz)
●	Thread safe
●	Compatible with Microsoft 2000 and XP
●	Compatible with Linux (coming soon)
●	<b>Easy-To-Use graphical user interface</b>
●	<b>Advanced output of found violations against rules:</b>
●	Auto DNS names
●	<b>Advanced rule editor:</b>
●	Over 1.500 different rules, from Exploit to Trojans signatures
●	Create new rules in 3 steps
●	Sorted in categories
●	Auto update via Internet
●	<b>Advanced alerts:</b>
●	Email message on rule
●	Window message on rule
●	<b>User database:</b>
●	Create, modify and delete users
●	<b>Securepoint Firewall &amp; VPN server plugin:</b>
●	Connect direct to a Securepoint firewall (V3.X)
●	Auto inform Securepoint firewall of a security problem
●	Blocking of a connection with temporary firewall rules
●	<b>Other features:</b>
●	Protect nuzzler IDS from third persons
●	Load, save and print reports
●	<b>Network Test Tool</b>
●	Analyzing network traffic content
●	Port scanner, sniffer and reporting of network activity

### Additional: Securepoint Network Test Tool, Version 2.0

The Securepoint Network Test Tool allows to analyse the traffic and content of your network. The tool works under WindowsNT, 2000, XP und ME.



Securepoint Network Test Tool features:

- Windows Protocol tables (TCP/IP/ARP):
- Easy and fast summary of all protocols. The TCP/IP/ARP table shows your internal window connections through your network.
- Network reporting:  
The report shows the located computers in the specified network. It reports the IP address and names of the computers
- Service programs to analyse:
  - Integrated port scanner
  - Traceroute and
  - a special analyse program of the local and network computer
- Network monitor:  
Shows the actual activity of the network interface and the traffic Sniffer: The sniffer gives you the possibility to monitor the traffic of the network. You will get every data package which is received at the selected network card. Either it is for your computer or not, results and reports are saveable.

### nuzzler server edition requirements



Minimum nuzzler requirements:

- Windows™ 2000 or XP
- CPU >= Intel Pentium II with 600 MHz
- RAM >= 128 MByte RAM
- CDROM CD-ROM,
- Disc space >= 16 MByte
- Network 1 network interface

nuzzler is available as hardware appliance and single software package for Microsoft Windows™ 2000 / XP. A Linux version will be available soon.



**Securepoint GmbH, Deutschland**

Salzstrasse 1  
21335 Lüneburg Germany  
Tel.: ++49 (0) 41 31 / 24 01-0, Fax: 24 01-50  
<http://www.securepoint.de>, [info@securepoint.de](mailto:info@securepoint.de)

**Securepoint, Österreich**

Franz-Pichler Str. 46  
3100 St. Pölten Austria  
Fax: ++43 (0) 27 42 76 000  
<http://www.securepoint.at>, [info@securepoint.at](mailto:info@securepoint.at)