Network traffic monitoring and analysis software.

Andrisoft WANGuard Platform™ WANGuard Sensor 3.0

OVERVIEW

WANGuard Sensor is the WANGuard Platform and WANGuard Platform Lite component designed to do both incoming and outgoing traffic monitoring and accounting, as well as traffic anomalies detection (feature unavailable in the Lite version).
At it's core, WANGuard Sensor has a highly scalable traffic correlation engine capable of continuously monitoring hundred of thousands of IP addresses. Complex statistical algorithms integrate traffic data to build an accurate and detailed picture of real-time and historical traffic flows across the network.

SUPPORTED TRAFFIC CAPTURING METHODS

WANGuard Sensor was designed to monitor the largest enterprises with hundreds of thousands of endpoints to the smallest branch office with tens of endpoints. The supported traffic capturing methods work with most switches, routers, firewalls and other network devices. The supported methods are:

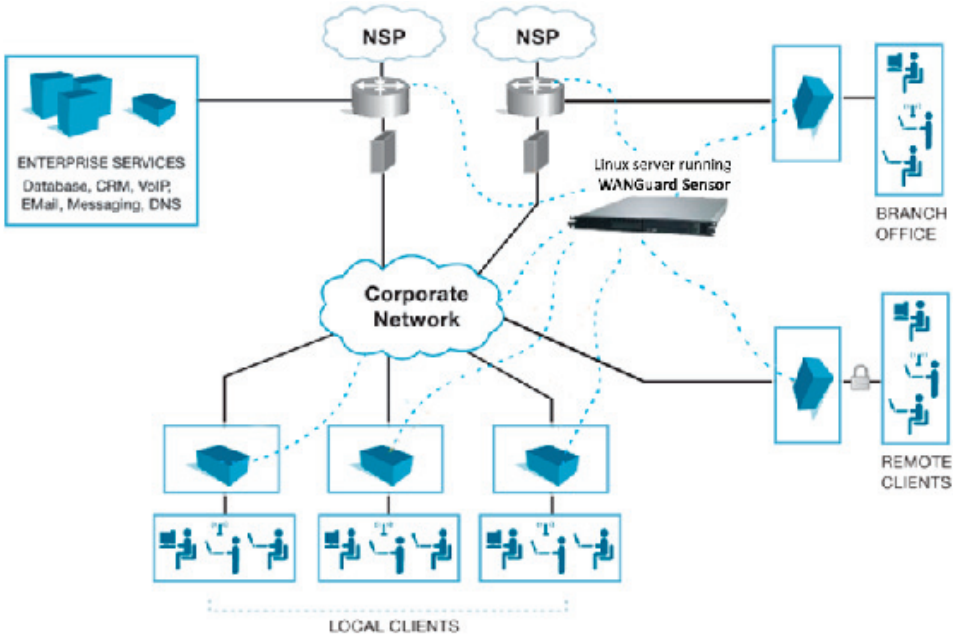
Port Mirroring (Switched Port Analyzer - SPAN, Roving Analysis Port), Network TAP - The analysis of network packets sent by a monitoring port of a switch, router or network TAP. The WANGuard Sensor type that handles network packets is called *WANGuard Sniff*.
NetFlow® Monitoring - The analysis of pre-aggregated data flows sent by NetFlow® or NetStream® enabled routers and Layer 3 switches*. The WANGuard Sensor type that handles NetFlow® and NetStream® data is called *WANGuard Flow*.
In-line Deployment - The analysis of incoming and outgoing network packets that pass through a network card of an in-line deployed Linux server. From a software perspective this method is virtually identical with the Port Mirroring method, so *WANGuard Sniff* is used in this scenario too.

FEATURES

- Any number of instances can be deployed across the network and all collected data will be centralized and available through a single web interface that you can quickly access from any location
- You can access various real-time parameters (top talkers, number of IP addresses, top protocols, protocols distribution etc.) about the data flowing through router interfaces and switch ports
- Provides on-demand MRTG-style traffic graphs for every IP address or subnet in your network, for any time frame. Traffic graphs accuracy can be defined between 5 seconds and 5 minutes
- WANGuard Sensor is completely scalable and can monitor and generate graphs for hundreds of thousands of IP addresses
- Detects traffic anomalies and provides per endpoint flexible threat management tools and an easy to use API for configuring the reaction to traffic anomalies:
  - activate WANGuard Filter for DoS, DDoS and DrDoS mitigation or additional threat information
  - alert the NOC staff by email using user-defined email templates
  - send custom syslog messages to remote log servers
  - send BGP announcements for blackholing targeted endpoints
  - execute custom scripts that extend the built-in capabilities such as:
    - configure ACLs or execute PIX "shun" commands to drop traffic towards targeted endpoints
    - send SNMP TRAP messages to SNMP monitoring stations
    - display the routers that are being transited by the anomalous traffic
- Includes a very flexible billing system for bandwidth based billing
- Easy and non-disruptive installation on common server hardware
- The most cost-effective traffic monitoring and analysis solution on the market

Requirements

Single WANGuard Sensor Deployment Example



	WANGuard Sensor	
	WANGuard Sniff	**WANGuard Flow**
Traffic Capturing Technology	Port Mirroring, Network TAP, In-line Deployment	NetFlow® or NetStream® v.5 enabled network devices*
Maximum Traffic Capacity	10 GigE > 150,000 endpoints	10 Gbps < 100,000 endpoints
Traffic Parameters Accuracy	Highest (5 seconds averages)	High
Traffic Anomalies Detection Time	< 5 seconds	< flow export time + 5 seconds
Traffic Validation Options	IP Subnets, MAC addresses, VLANs	IP Subnets, Interfaces, AS Number

Minimum System Requirements for analyzing 1 Gigabit Network Interface

Architecture	x86 (32 or 64 bit)	x86 (32 or 64 bit)
CPU	1 x Pentium IV 2.0 GHz	1 x Pentium IV 1.6 GHz
RAM	500 MBytes	3 GBytes
Network Cards	1 x Gigabit Ethernet (with NAPI Support) 1 x Fast Ethernet	1 x Fast Ethernet
Operating System	Red Hat Enterprise 5, CentOS 4, CentOS 5, Open-SuSE 10, SUSE Linux Enterprise 10, Debian Linux 4, Ubuntu Linux Server 8	Red Hat Enterprise 5, CentOS 4, CentOS 5, OpenSuSE 10, SUSE Linux Enterprise 10, Debian Linux 4, Ubuntu Linux Server 8
Installed Packages	tcpdump, WANGuard-Sensor 3.0, WANGuard-Controller 3.0	WANGuard-Sensor 3.0, WANGuard-Controller 3.0
Disk Space	5 GB (including OS)	5 GB (including OS)

Andrisoft SRL
Str. Lunei L30 Ap. 11
300109 Timisoara
Romania

office@andrisoft.com

Andrisoft is a network security company that offers IT organizations network monitoring and protection software and solutions.
Andrisoft WANGuard Platform is built on a scalable and performant architecture and offers unparalleled granularity, accuracy and precise, non-intrusive mitigation.