WanSight 6.1 User Guide

- Console
- Sensors (Packet Sensor, Flow Sensor, SNMP Sensor, Sensor Cluster)

Copyright ©2016 Andrisoft SRL
All rights reserved.
Revision 3.27

Copyright & Trademark Notices

This edition applies to version 6.x of the licensed program WanSight and to all subsequent releases and modifications until otherwise indicated in new editions.

Notices

References in this publication to ANDRISOFT S.R.L. products, programs or services do not imply that ANDRISOFT S.R.L. intends to make these available in all countries in which ANDRISOFT S.R.L. operates. Evaluation and verification of operation in conjunction with other products, except those expressly designated by ANDRISOFT S.R.L., are the user's responsibility. ANDRISOFT S.R.L. may have patents or pending patent applications covering subject matter in this document. Supplying this document does not give you any license to these patents. You can send license inquiries, in writing, to the ANDRISOFT S.R.L. sales department, sales@andrisoft.com.

Copyright Acknowledgment

© 2015, ANDRISOFT S.R.L. All rights reserved.

All rights reserved. This document is copyrighted and all rights are reserved by ANDRISOFT S.R.L. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage and retrieval system without permission in writing from ANDRISOFT S.R.L.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. ANDRISOFT S.R.L. will not be responsible for any loss, costs or damages incurred due to the use of this documentation.

WanGuard and WanSight are SOFTWARE PRODUCTS of ANDRISOFT S.R.L. WanGuard and WanSight are trademarks of ANDRISOFT S.R.L. Other company, product or service names may be trademarks or service marks of others.

ANDRISOFT S.R.L.

Website: https://www.andrisoft.com
Sales: sales@andrisoft.com
Technical Support: support@andrisoft.com

© 2015, ANDRISOFT S.R.L. All rights reserved.

Table of Contents

IP Traffic Monitoring and IP Accounting with WanSight

Andrisoft WanSight is enterprise-grade software that delivers to NOC and IT teams the functionality needed for effectively monitoring networks through a single integrated package. Andrisoft WanGuard extends WanSight with advanced DDoS detection and DDoS mitigation capabilities. To switch to WanGuard you purchase a WanGuard license.

WanSight Key Features & Benefits

- ✔ FULL NETWORK VISIBILITY – Supports all major IP traffic monitoring technologies: packet sniffing, NetFlow version 5,7 and 9; sFlow version 4 and 5; IPFIX and SNMP.
- ✔ ADVANCED WEB CONSOLE – Consolidated management and reporting through a single, interactive and highly-configurable HTML5 web portal with customizable dashboards, user roles, remote authentication, etc.
- ✔ PACKET SNIFFER – A distributed packet sniffer that saves packet dumps from different network entry points. View packet details in a Wireshark-like web interface.
- ✔ FLOW COLLECTOR – A fully featured NetFlow, sFlow, and IPFIX Analyzer and Collector that saves flows in a compressed format for long term storage. Flows can easily be searched, filtered, sorted, and exported.
- ✔ COMPLEX ANALYTICS – Generates complex reports with aggregated data for hosts, departments, interfaces, applications, ports, protocols, countries, autonomous systems, and more.
- ✔ REAL-TIME REPORTING – Bandwidth graphs are animated and have a short-term accuracy of just 5 seconds.
- ✔ HISTORICAL REPORTING – You can view reports from the last 5 seconds to the last 10 years by selecting any custom time period. Bandwidth histograms contain 95th-percentile values for burstable billing.
- ✔ SCHEDULED REPORTING – Any report can be generated automatically and emailed to interested parties at preconfigured intervals of time.
- ✔ FAST & SCALABLE – The software was designed to run on commodity hardware. Its components can be distributed on server clusters.

  All statistical data is stored in an internal SQL database that can be easily queried and referenced.

WanSight Software Components

WanSight Sensor provides in-depth traffic analysis, traffic accounting and bandwidth monitoring. The collected information enables you to generate complex traffic reports, graphs and tops; instantly pin down the cause of network incidents; understand patterns in application performance and make the right capacity-planning decisions.

WanGuard Console is a multi-tenant web graphical user interface that functions as the administrative core of the software. It offers single-point management and reporting by consolidating data received from the WanGuard Sensors that are deployed within the network.

For brevity, WanSight Sensor is referred to as Sensor, and WanSight Console as Console.

Choosing a Method of Traffic Monitoring

This chapter describes the traffic monitoring technologies supported by WanSight Sensor.

There are four WanGuard Sensor “flavors” that differ only in the way they obtain traffic information:

- **Packet Sensor** analyzes packets. It can be used on appliances that are either deployed in-line (servers, firewalls, routers, bridges) or connected to a mirrored port or TAP.

  In switched networks, only the packets for a specific device reach the device's network card. If the server running the Packet Sensor is not deployed in-line, in the main data-path, then a network TAP or a switch / router that offers a “monitoring port” or “mirroring port” must be used. In this case, the network device sends copies of data packets traveling through selected ports or VLANs to the monitoring port. Packet Sensor inspects every packet it receives and conducts packet-based traffic analysis.

- **Flow Sensor** analyzes flows. It is used for monitoring NetFlow® (jFlow, NetStream, cflowd), sFlow® and IPFIX data.

  Many routers and switches can collect IP traffic statistics and periodically send them as flow records to a Flow Sensor. Because the flow protocol already performs pre-aggregation of traffic data, the flow data sent to the Flow Sensor is much smaller than the monitored traffic. This makes the Flow Sensor a good option for monitoring remote or high-traffic networks. The main downside of flow-based traffic analysis is that pre-aggregating traffic data adds a delay of at least 30 seconds to collecting real-time traffic statistics.

- **SNMP Sensor** monitors the bandwidth usage of routers and switches on a port-by-port basis.

  When this technology is used, an SNMP Sensor queries the device (e.g. router, switch and server) for the traffic counters of each port with quite small data packets. These are triggering reply packets from the device. Compared to other bandwidth monitoring technologies, the SNMP option is very basic and offers no IP-specific information. SNMP creates the least CPU and network load.

- **Sensor Cluster** aggregates pre-existing Sensor traffic data into a single, unified IP graphing domain.

  It sums-up traffic data collected by Packet Sensors, Flow Sensors and SNMP Sensors.

For redundancy, high availability and to be able to view packet traces and flow dumps, use Flow Sensor(s) and Packet Sensor(s) simultaneously.

Comparison between Packet Sniffing, Flow Monitoring and SNMP Polling

Use the Packet Sensor when the speed of detecting attacks is critical or when there is a need for capturing raw packets for forensics. Because it inspects every packet entering the network, it needs to run on servers with powerful CPUs and fast network adapters.

Flow Sensor analyzes pre-aggregated traffic information sent by routers/switches, so it can monitor multiple 10 Gbit or 40 Gbit interfaces, even when it is running on a low-performance server.

Major Flow Sensor disadvantages:

- ✗ it exhibits reduced speed in processing real-time data because all flow exporters aggregate traffic data over time, with delays of more than 30 seconds
- ✗ enabling the flow exporting feature often results in increased CPU usage on the network device
- ✗ it needs to run on servers with lots of RAM

It is recommended to use the SNMP Sensor only for devices unable to export flows or mirror packets, or when comparing flow and SNMP derived statistics in order to ensure the flow data accuracy.

The table below lists the main differences between the Sensor types:

	Packet Sensor	Flow Sensor	SNMP Sensor
Traffic Monitoring Technology	- Sniffing packets passing an in-line appliance - Port mirroring (SPAN, Roving Analysis Port) - Network TAP	- NetFlow version 5, 7 and 9 (jFlow, NetStream, cflowd) - sFlow version 4 and 5 - IPFIX	- SNMP version 1 - SNMP version 2c - SNMP version 3
Maximum Traffic Capacity per Sensor*	10 GigE	multiples of 40 Gbps	multiples of 40 Gbps
DDoS Detection Time**	≤ 5 seconds	≥ flow export time (≥ 30 seconds) + 5 seconds	≥ 5 seconds, no details on attacked destinations
IP Graphing Accuracy	≥ 5 seconds	≥ 20 seconds	N/A
Traffic Validation Options	IP classes, MAC addresses, VLANs, BPF	IP classes, Interfaces, AS Numbers, Ingress/Egress	Interfaces
Packet Tracer	Yes	No	No
Flow Collector	No	Yes	No

* The software is not limited by the number of connections between IPs.
** WanGuard Sensor is able to detect which destination is under attack. The attackers and attack patterns are detected only by WanGuard Filter.

WanSight Installation

Installing WanSight does not generate negative side effects on the network's performance. Full installation and configuration may take less than an hour.

WanSight can be installed exclusively on Linux platforms. To install and configure the software you will need basic Linux operation skills and at least medium computer networking skills. Contact <support@andrisoft.com> if you encounter software installation issues or if you have questions about the system requirements listed below.

System Requirements

WanSight 6.1 can be installed on the following 64-bit Linux distributions: Red Hat Enterprise Linux 6 or 7 (commercial), CentOS 6 or 7 (free, Red Hat-based), Debian Linux 6 “Squeeze” or 7 “Wheezy” or 8 “Jessie” (free, community-supported), Ubuntu 12 or 14 (free, Debian-based), OpenSuSE 13 (free, Novel-based). The most tested and stable distribution that can be used with WanSight is CentOS 7.

WanSight was designed to be completely scalable, so it can be installed either on a single server with adequate hardware resources, or on multiple servers distributed across the network. You can use Virtual Machines to try the software, but the use of dedicated servers for production is mandatory.

A few arguments against using Virtual Machines with WanSight after the trial period:

- Having fast and uninterrupted access to the hard disk is a critical requirement.
- The resources must be provisioned in a predictable and timely manner.
- Many Virtual Machines do not have a stable clock source.

Importance of HW resources	CPU Speed (> GHz/core)	CPU Cores (> cores)	RAM Size (> GB)	HDD Size (> GB)	HDD/SSD Speed (> Mbytes/s)	Network Adapter (Vendor, Model)
Console	*High*	*High*	*High*	*Very High*	*Very High*	*Very Low*
Packet Sensor	*Very High*	*High*	*Low*	*Low*	*Low*	*Very High*
Flow Sensor	*Low*	*Low*	*Very High*	*Medium*	*High*	*Very Low*
SNMP Sensor	*Very Low*	*Low*	*Very Low*	*Very Low*	*Very Low*	*Very Low*
Sensor Cluster	*Medium*	*Medium*	*Medium*	*Very Low*	*Very Low*	*Very Low*

Legend	*Very High Importance*	*High Importance*	*Medium Importance*	*Low Importance*	*Very Low Importance*

Console Hardware Requirements

Capacity	Minimum Hardware Requirements for 20 Components
Architecture	64bit x86

CPU	2.4 GHz dual-core Xeon
RAM	4 GB
NICs	1 x Fast Ethernet for management
HDDs	2 x 7200 RPM HDD, RAID 1, 80 GB (additional disk space may be needed for IP graphs)

The Console server stores the database and centralizes all operational logs, graphs and IP accounting data.

Its performance is determined by its settings, as well as the performance of the server and the performance of the applications it relies on: MySQL or MariaDB, Apache HTTPD and PHP.

To access the web interface provided by Console, use one of the following web browsers: Google Chrome, Firefox 3.5 or later, Safari 3.0 or later, Internet Explorer 8 or later. JavaScript and cookies must be enabled. Java and Adobe Flash are not required. The contextual help provided by Console requires Adobe PDF Reader. For the best experience, use a 1280x1024 or higher resolution display.

Packet Sensor Hardware Requirements

Packet Sniffing Capacity	1 Gbit/s – 1,400,000 packets/s	10 Gbit/s – 14,000,000 packets/s
Architecture	64bit x86	64bit x86
CPU	2.0 GHz dual-core Xeon	3.2 GHz quad-core Xeon (e.g. Intel X5672)
RAM	2 GB	4 GB
NICs	1 x Gigabit Ethernet (with driver supported by PF_RING) 1 x Fast Ethernet for management	1 x 10 GbE adapter (Myricom or Intel 82599 chipset) 1 x Fast Ethernet for management
HDDs	2 x 5200 RPM HDD, RAID 1, 35 GB	2 x 5200 RPM HDD, RAID 1, 35 GB

Packet Sensor can be load-balanced on multiple CPU cores only with:

- Intel 82599 chipset network adapters, such as Intel X520, Intel X540, HP X560, Silicom PE310G4DBi9-T.
- Myricom network adapters with a Sniffer 10G license.

On any other network adapter supported by Linux, Packet Sensor runs single-threaded on a single CPU core, which may lead to packet loss when analyzing very high packet rates. Packet Sensor is compatible with the PF_RING high-speed packet capturing engine.

Through Sensor Cluster you can increase the packet sniffing capacity to 40 Gbit/s, 100 Gbit/s or more by using multiple servers that run Packet Sensors on 10 Gbit/s network adapters.

Flow Sensor Hardware Requirements

Capacity	Minimum Hardware Requirements for 5,000 flows/s
Architecture	64bit x86
CPU	2.0 GHz dual-core Xeon

RAM	8 GB
NICs	1 x Fast Ethernet for management
HDDs	2 x 7200 RPM HDD, RAID 1, 60 GB

Flow Sensor does not have a limit on the number of interfaces it can monitor or a limit of how many flows per second it can process. Each Flow Sensor can process the flows of a single flow exporter. A server with enough RAM can run tens of Flow Sensors. For Flow Sensor, the amount of the RAM is much more important than the CPU speed.

Flow Sensor stores all received flows on the local disk in a compressed binary format.

SNMP Sensor Hardware Requirements

Capacity	Minimum Hardware Requirements for 20 Devices
Architecture	64bit x86
CPU	1.6 GHz dual-core Xeon
RAM	1 GB
NICs	1 x Fast Ethernet for management
HDDs	2 x 5200 RPM HDD, RAID 1, 20 GB

SNMP Sensor does not have a limit on the number of interfaces it can monitor. Each SNMP Sensor can monitor a single device. A server can run an unlimited number of SNMP Sensors.

Sensor Cluster Hardware Requirements

The hardware requirements for Sensor Cluster are low because the analyzed traffic information is pre-aggregated by the associated Sensors (Flow Sensors, Packet Sensors or SNMP Sensors).

It is recommended to run Sensor Cluster on the Console server.

Software Installation

The download link is listed in the email containing the trial license key. The latest software installation instructions are listed on the Andrisoft website.

The trial license key activates all WanSight features for 30 days. You can install the trial license key on any number of servers. To switch to a full, registered version, apply a license key purchased from the online store.

Opening the Console for the First Time

WanSight Console provides a web interface and centralized system through which you will control and monitor all other components. If you correctly followed the installation instructions, from now on you will only need

to log into the Console to manage and monitor servers and software components.

To login into the Console, open http://<console_hostname>/wansight. If the page cannot be displayed, make sure the Apache web server is running and the firewall does not block incoming traffic on port 80. You can also access the Console securely using HTTPS if the Apache web server was configured with SSL/TLS support.

Licensing Procedure

If you have not yet licensed WanSight you will be asked to do so. Upload the *trial.key* file sent to you by email by clicking the key icon. The license key contains encrypted information about the licensed capabilities of the software. You can switch between WanGuard and WanSight by changing the license key.

Log into the Console using the default username/password combination: **admin/changeme**.

If the Console is installed on a public server, you should immediately change the default password of the "admin" account. To do so, click the **Admin** menu at the top-right corner of the browser window and select <**Change Password**>.

To understand how to navigate within Console, read the chapter beginning on page 12.

Quick Configuration Steps

- ➔ Estimate storage requirements, review decoders and IP graph settings – page 13
- ➔ Add your IP address ranges and important hosts to an IP Zone – page 17
- ➔ Add a Packet Sensor – page 19, Flow Sensor – page 23, or SNMP Sensor – page 27
- ➔ Watch the event log. Receive error notifications by email – page 32
- ➔ Generate reports and send them periodically by email – page 31
- ➔ Create your own dashboards and add widgets with useful information – page 50
- ➔ Create personalized Console accounts for your staff or customers – page 34

Basic Concepts of WanSight Console

Please read this chapter to understand the basic premises required to properly operate the software. The next chapters cover the configuration of the software, while the last 5 chapters cover the reporting features.

To understand the operation of the Console you should be aware of the structure of the web interface:

Side Region

The Side Region is used for navigation throughout the Console. It is located at the east and/or west edge of the browser's window, according to the user's preference. If it is not visible, it has been either collapsed or hidden by an administrator. Clicking the edge of regions expands or collapses them.

The Side Region contains 2 sections – Reports and Configuration – that can be collapsed or expanded by clicking the title bars or by pressing Ctrl+R. Both sections contain multiple panels that can also collapse or expand, with such state being maintained between sessions. Panels are refreshed every 5 to 10 seconds.

The Reports section title bar contains a “Quick Search” button. Keyboard shortcut: Ctrl+S.

Central Region

Each report, dashboard or tool you select in the Side Region opens a tab (page) in the Central Region. You may switch between (sub-) tabs with a mouse or with the keyboard shortcut (Alt+) Ctrl+→ and (Alt+)Ctrl+←. You can close all tabs except for the Landing Tab (initially set to the Configuration Wizard). To change the Landing Tab, edit your user profile in Configuration » General Settings » User Management.

South Region

The South Region provides a quick way to view live data: events (system logs), animated traffic graphs, and statistics from all software components. It is located at the bottom of the browser's window. By default, it is collapsed; to expand it, click the thin line near the bottom edge or press Ctrl+E.

Upper Menus

The Upper Menus are located on the top-right part of the Console window.

The Help menu contains a link to the User Guide, a few helper tools and the About window. Dependent on context, the User Guide will open at the chapter describing the last-opened window or tab. Contextual help works with Adobe PDF Reader.

The User menu provides a Log Out option and lets you quickly change the password and few user preferences.

Configuration » General Settings » Graphs & Storage

A very important initial step in configuring WanSight is to make sure that the server(s) the software runs on have enough resources to process and store IP graphs, flows and packet dumps. Storage-related settings can be tuned by editing Configuration » General Settings » Graphs & Storage.

In a later chapter, you will be able to configure the Sensors to generate traffic graphs, tops and accounting data for every IP that belongs to the monitored network. If you intend to use this feature, you may want to change the default IP storage settings, as changing these later will reset all existing IP graphs, tops and accounting data.

The **Sensor Top N** value (default: 20) specifies the maximum number of items stored for ordered sets of data, such as top Talkers, External IPs, ASNs, Countries, TCP/UDP ports, IP protocols, etc.

The Packet Sensors save packet dumps on the local disk in the path configured for **Packet Traces**. The Flow Sensors save flow data on the local disk in the path configured for **Flow Collectors**. When the Console is not installed on the Sensor server, export these paths towards the Console's file system using an NFS share (KB article link). If you do not, the Console will not be able to display data saved on remote servers.

All graph files are stored by the Console server, in the **Graphs Disk Path**. Graph files are optimized for storing time series data and do not grow over time. All IP graph options described below have a direct impact on the storage space required on the Console server.

The **Graph IP Sweeps** option prevents creating IP graph files for IPv4 and/or IPv6 addresses that receive traffic without sending any traffic in return. Do not set to “Off” when monitoring unidirectional links or asymmetric traffic.

The size of each IP graph file is listed on the bottom of the window in the *Disk space required for each IP graph file* field. When Sensor Clusters are not used, the maximum number of IP graph files that could be generated can be calculated with the formula: ((number of Packet Sensors) + (number of Flow Sensor interfaces)) x (number of IPs contained in subnets with IP Graphing set to “Yes” in the IP Zone).

There are 2 mutually exclusive methods for creating and updating IP graph files, so select the appropriate one for your setup:

- **Create & update IP graph files directly on disk** – This method optimizes the long-term storage of IP graph data by allowing up to 3 **Round Robin Archives**. The values within the Round Robin Archives determine the granularity of the graphs and the interval of time they are saved for. These entries specify for how long, and how accurately data should be stored. A smaller data average (5 seconds minimum) will generate a very accurate graph, but will require more disk space, while a bigger data average is less accurate and uses less disk space.

  On non-SSD drives, the disk seek time may be too high to update thousands of IP graph files every few minutes. If this is the case, configure the **RRDCache daemon** to increase the I/O performance of the Console server (KB article link). If the speed of updating IP graph files is not fast enough, consider the method below.

- **Update IP graph files in RAM or SSD** – This method is not optimal for long-term storage because it allows a single Round Robin Archive per IP graph file. The files are created and updated in **Graphs RAM Path**, and moved periodically onto a larger, albeit slower disk. Select this method when the previous method configured with RRDCached is not fast enough to sustain updating thousands of very high-

granularity IP graphs.

Decoders represent internal functions that differentiate and classify the underlying protocols of each packet and flow. Each enabled decoder increases the size of IP graph, top and accounting data, and causes a small performance penalty on Packet Sensor. It is recommended to enable only the decoders you are interested in.

You can define your own decoders in Configuration » General Settings » Custom Decoders. Default decoders:

Decoder	Description
TOTAL	Always enabled, matches all IP packets & flows.
TCP	Matches TCP traffic.
TCP+SYN	Matches TCP traffic with SYN flag set and ACK unset. Flow Sensor counts one packet per flow.
UDP	Matches UDP traffic.
ICMP	Matches ICMP traffic.
OTHER	Matches IP protocols that differ from TCP, UDP and ICMP.
BAD	Matches TCP or UDP port set to 0, or IP protocol set to 0.
FLOWS	Matches flow records and replaces packets/s with flows/s. Works only with Flow Sensor.
FLOW+SYN	Matches flow records with SYN flag set. Flow Sensor counts all packets per flow.
FRAGMENT	Matches fragmented IP packets. Works only with Packet Sensor.
TCP-NULL	Matches TCP traffic without TCP flags, indicative of reconnaissance sweeps.
TCP+RST	Matches TCP traffic with RST flag set.
TCP+ACK	Matches TCP traffic with SYN flag unset and ACK set.
TCP+SYNACK	Matches TCP traffic with SYN flag set and ACK flag set.
HTTP	Matches TCP traffic on source or destination port 80.
HTTPS	Matches TCP traffic on source or destination port 443.
MAIL	Matches TCP traffic on source or destination ports 25,110,143,465,585,587,993,995.
DNS	Matches UDP traffic on source or destination port 53.
SIP	Matches TCP or UDP traffic on source or destination port 5060.
IPSEC	Matches IP traffic on IP protocol 50 or 51.
WWW	Matches TCP traffic on source or destination ports 80, 443.
SSH	Matches TCP traffic on source or destination port 22.
NTP	Matches UDP traffic on source or destination port 123.
SNMP	Matches UDP traffic on source or destination ports 161, 163.
RDP	Matches TCP or UDP traffic on source or destination port 3389.
YOUTUBE	Matches IP traffic going or coming from Youtube AS 43515, 36561, or from Youtube subnets.
NETFLIX	Matches IP traffic going or coming from Netflix AS 55095, 40027, 2906, or from Netflix subnets.
HULU	Matches IP traffic going or coming from Hulu AS 23286, or from Hulu subnets.
FACEBOOK	Matches IP traffic going or coming from Facebook AS 54115, 32934, or from Facebook subnets.

Consolidation functions build consolidated values for Round Robin Archives. If you are interested in traffic spikes, check MAXIMUM. If you are interested in average values, check AVERAGE. For low traffic values, check MINIMUM.

Automate the deletion of old data and monitor the disk usage of IP graphs in Configuration » General

Settings » Data Retention.

Sensor and Applications Graph Troubleshooting

- ✔ Ensure that all Sensors run correctly by verifying the event log and by viewing live statistics from Reports » Components » Overview. The troubleshooting guide for Packet Sensor is located on page 22, for Flow Sensor on page 25 and for SNMP Sensor on page 29.
- ✔ If the Applications graph is empty but other Sensor graphs are not, and the Sensor is running for more than 5 minutes, open Configuration » General Settings » Graphs & Storage, click <**Save**> and select <**Yes**> when being asked to delete existing graph files.

IP/Subnet Graph Troubleshooting

- ✔ Ensure that all Sensors run correctly by verifying the event log and by viewing live statistics displayed in Reports » Components » Overview. The troubleshooting guide for Packet Sensor is located on page 22, for Flow Sensor on page 25 and for SNMP Sensor on page 29.
- ✔ Generating IP graph data has the biggest impact on the load of the Console server. Enable each feature (IP graphing, IP accounting) sequentially for each subnet, after making sure the Console server can handle it. The storage requirements for each subnet are listed in the IP Zone, and the current disk usage in Configuration » General Settings » Data Retention.
- ✔ The internal program used for saving IP graph data is /opt/andrisoft/bin/genrrds_ip. If it is overloading the Console server or the event log contains warnings such as “Updating IP graph data takes longer than 5 minutes”, use RRDCacheD, RAM/SSD updating method, faster disk drivers, enable IP graphing for fewer subnets, or deploy a Sensor Cluster configured to aggregate IP graph data.
- ✔ The internal program used for generating IP or subnet graphs is /opt/andrisoft/bin/gengraph_ip. The program is launched by Console users for each requested IP or subnet graph. If the Console server gets too loaded by gengraph_ip, execute “killall gengraph_ip” and configure RRDCacheD. When launched, the program does not stop until the graph is generated. The program can be slow when users request subnet graphs for subnets not specifically defined in the IP Zone. It is not possible to throttle the number of graphs requested by users.

AS and Country Graph Troubleshooting

- ✔ Ensure that all Sensors run correctly by verifying the event log and by viewing live statistics from Reports » Components » Overview. The troubleshooting guide for Packet Sensor is located on page 22, for Flow Sensor on page 25 and for SNMP Sensor on page 29.
- ✔ To enable AS and Country graphs, set the Top Generator parameter to either “Extended” for Flow Sensor, or “Full” for Packet Sensor.
- ✔ SNMP Sensor is not able to generate AS graphs or Country graphs.

Configuration » General Settings » Custom Decoders

Decoders represent internal functions that differentiate and classify the underlying protocols of each packet and flow. The predefined decoders are listed in the "Graphs & Storage" chapter on page 13. If you do not wish to define custom decoders, you may safely skip this chapter.

To manage user-defined decoders go to Configuration » General Settings » Custom Decoders. Each custom decoder contains the following information:

- **Decoder Name** – A short name to help you identify the decoder. The field is mandatory.
- **Graph Color** – The color used in graphs for the decoder. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
- **Decoder Description** – An optional short description of the decoder.
- **Packet Filtering Expression** – Enter a BPF filtering expression for packets if you intend to use a Packet Sensor and/or Packet Filter. Click the light bulb icon on the right to open a window that will show you the correct syntax. Examples:
  - To match TCP packets with the SYN flag set, enter *tcp[tcpflags] & tcp-syn!=0*
  - To match UDP packets with the destination port under 1024, enter *udp and dst portrange 1-1023*
- **Flow Filtering Expression** – Enter a filtering expression for flows if you intend to use a Flow Sensor and/or Flow Filter. Click the light bulb icon on the right to open a window that will show you the correct syntax. Examples:
  - To match TCP flows having only the SYN flag set, enter *flags S and not flags AFRPU*
  - To match flows with the MPLS label0 set to 2, enter *mpls label0=2*
- **Included Decoders** – Required if you plan to use the decoder for IP graphing. Select the decoders that include the matched traffic, or TOTAL if not sure.
- **Conflicting Decoders** – Required if you plan to use the decoder for IP graphing. Select the decoders that might match same traffic, but not always. Useful only for stacking multiple decoders inside IP graphs.

Configuration » Network » IP Zone

IP Zones are hierarchical, tree-like structures from which Sensor(s) learn the monitored network's boundaries and extract per-subnet settings.

You must add all your IP blocks the IP Zone(s) listed in Configuration » Network . You can add prefixes (IP blocks/subnets/ranges) using the Console web interface, or from the CLI by executing the command “php /opt/andrisoft/api/cli_api.php” on the Console server.

To define a new IP Zone, go to Configuration » Network » <+> » IP Zone. You need more than one IP Zone only when you need different per-subnet settings for different Sensors. If this is the case, it may be easier to open an existing IP Zone that already contains your IP address ranges, and duplicate it by pressing the < **Duplicate**> button. A new IP Zone will be created with the same name and the word “(copy)” attached, containing the same prefixes and IP groups as the original.

The IP Zone Configuration window is divided by two vertical sections. The buttons that manage prefixes are located in the upper part of the left-hand section. When a new prefix is added, the tree below automatically updates itself. The right-hand section contains panels with user-provided settings for the selected prefix.

To enter IP addresses or IP blocks, you must use the CIDR notation. To enter individual hosts in IP Zones you must use the /32 CIDR mask for IPv4, or /128 for IPv6. For more information about the CIDR notation, see Appendix 1 from page 56.

Every IP Zone contains at least the 0.0.0.0/0 network. Since the CIDR mask is /0, this “supernet” contains all IP addresses available for IPv4 and IPv6. For an easier configuration, every new prefix that you define will inherit by default the properties of the closest (having the biggest CIDR) IP class that includes it.

The **IP Settings** panel in the right-hand section provides the following options:

- **IP Group** – This editable combo box should contain a short description of the selected prefix, or the name of the customer that uses it. Setting the same IP group for multiple prefixes will allow you to generate aggregated traffic reports.
- **IP Graphing** – Set to “Yes” to allow the Sensor to generate graph data for every IP contained in the selected prefix. The **Graph IP Sweeps** option from Configuration » General Settings » Graphs & Storage can be used to prevent generating graph data for IPs that only receive traffic without sending any traffic in return.
- **IP Accounting** – Set to “Yes” to allow the Sensor to generate daily accounting data for each IP contained in the selected prefix.

The **Storage Requirements** column indicates the disk space needed to store the data generated by a single Packet Sensor or Flow Sensor interface. Enabling IP graphing and IP accounting for very large prefixes (e.g. 0.0.0.0/0) might generate (useless) data that can potentially overload the Console server.

The **Comments** panel allows you to write a comment for the selected prefix. It is not visible elsewhere.

Configuration » Servers

Any server running Sensor(s) must be listed under Configuration » Servers. The Console server is automatically added on installation.

To add a new server, click the <+> button from the title bar of the Configuration » Servers panel. To configure an existing server, go to Configuration » Servers and click its name.

The Server Configuration window contains the following fields:

- **Server Name** – A short name to help you identify the server.
- **Graph Color** – The color used in graphs for this server. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
- **Reports Visibility** – Whether the Reports » Servers panel should contain icons of the components the server runs.
- **Device Group** – Optional description used within Console to group servers by location, role, etc.
- **Server ID** – Read-only unique identifier of the server, used when exporting NFS shares.
- **IP Address** – The IP address of the server as defined during the WANsupervisor service installation. Can be public or private.
- **Linux Distro** – The Linux distribution installed on the server.
- **Hardware Key** – Read-only string used for licensing purposes. The hardware key field is updated by the WANsupervisor service on installation or when the hardware, IP or hostname changes.
- **Monitored Network Interfaces (optional)** – The WANsupervisor service can monitor packets/s, bits/s, errors and dropped frames for each interface that exists on the server. The data is available in Reports » Servers » [Server] » Server Graphs » Data Units = Server Interfaces. These stats are provided by the OS.
- **Comments** – Comments about the server can be saved here. These comments are not visible elsewhere.

Server Troubleshooting

- ✔ In order for the server to be operational, make sure it always runs the WANsupervisor service and that its clock is synchronized with NTP. You can verify the operational status of each server in Reports » Components » Overview » Servers.
- ✔ The WANsupervisor service breaks when the MySQL service running on the Console server is restarted or unavailable even for a short amount of time (e.g. networking issue). In this case, either restart WANsupervisor manually, or use automated tools such as systemd, monitd or similar.
- ✔ You can discover performance-related issues by monitoring Reports » Server » [Server] » Server Graphs and Reports » Server » [Server] » Server Events.

Configuration » Components » Packet Sensor

In switched networks, only the packets for a specific device reach the device's network card. If the server running the **Packet Sensor** is not deployed in-line (in the main data-path), a network TAP, or a switch/router that offers a “monitoring port” or “mirroring port” must be used. In this case, the network device sends copies of data packets traveling through selected ports or VLANs to the monitoring port. Packet Sensor inspects every packet it receives and conducts packet-based traffic analysis. The advantages and disadvantages of packet-based traffic monitoring are listed on page 6.

For instructions on how to configure switches or routers for port mirroring, consult their documentation.

To add a Packet Sensor, click the <+> button from the title bar of the Configuration » Components panel. To modify an existing Packet Sensor, go to Configuration » Components and click its name.

The Packet Sensor Configuration window contains the following fields:

- **Sensor Name** – A short name to help you identify the Packet Sensor.
- **Graph Color** – The color used in graphs for the Packet Sensor. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
- **Reports Visibility** – Whether the Packet Sensor should be listed inside the Reports » Components panel.
- **Device Group** – Optional description used within Console to group components by location, role, etc.
- **Sensor Server** – The server that runs the Packet Sensor. The configuration of servers is described on page 18.
- **Sniffing Interface** – The network interface listened by the Packet Sensor. If the server that runs the Packet Sensor is deployed in-line, then this field must contain the network interface that receives the traffic entering your network.
- **Capture Engine** – Select the best packet capturing engine for your setup:
  - *Embedded LibPcap* – Select to use the built-in LibPcap 1.6.2 library.
  - *System LibPcap* – Select to use the LibPcap library installed by the Linux distribution.
  - *Myricom Sniffer10G* – Select when using a Myricom network adapter with a Sniffer 10G license. Click the button on the right for driver-specific settings.
  - *PF_RING, RX+TX* – Select to use the PF_RING 6.2 library for RX and TX traffic.
  - PF_*RING, RX* – Select to use the PF_RING 6.2 library for RX traffic.
  - *PF_RING, TX* – Select to use the PF_RING 6.2 library for TX traffic.
- **CPU Affinity** – You can force the Packet Sensor to run exclusively on a given set of CPU cores.
- **Link Speed IN / OUT** – Enter the speed (bandwidth, capacity) of the monitored link. The values are used for percentage-based reports.
- **Sensor License** – The license used by the Packet Sensor. WanGuard provides all features; WanSight does not provide traffic anomaly detection and reaction.

- **Top Generator** – Allows generation of traffic tops:
  - *Basic* – Enables tops for Internal IPs, IP protocols, versions and TCP/UDP ports. It is the recommended value because it adds a very small performance penalty.
  - *Extended* – Enables all tops from *Basic* as well as tops for External IPs (IPs not included in the IP Zone). It adds performance penalty of over 20%, especially during spoofed attacks.
  - *Full* – Enables all tops from *Extended* as well as tops and graphs for autonomous systems. It adds a performance penalty of over 20%, especially during spoofed attacks.
- **IP Zone** – Packet Sensor needs an IP Zone from which to learn about your network's boundaries and to extract per-subnet settings. IP Zones are described in the "IP Zone" chapter on page 17.
- **IP Validation** – This option can be used to distinguish the direction of the packets or to ignore certain IPs:
  - *Off* – Packet Sensor analyzes all traffic and uses MAC Validation to distinguish the direction of traffic.
  - *On* – Packet Sensor analyzes the traffic that has the source and/or the destination IP in the selected IP Zone.
  - *Strict* – Packet Sensor analyzes the traffic that has either the source or the destination IP in the selected IP Zone.
  - *Exclusive* – Packet Sensor analyzes the traffic that has the destination IP in the selected IP zone, but not the source IP.
- **MAC Validation/Address** – This option can be used to distinguish the direction of the packets or to ignore unwanted OSI Layer 2 traffic:
  - *None* – Packet Sensor analyzes all traffic and uses IP Validation to distinguish the direction of traffic.
  - *Upstream MAC* – MAC validation is active and the MAC Address belongs to the upstream router.
  - *Downstream MAC* – MAC validation is active and the MAC Address belongs to the downstream router.

    The MAC Address must be written using the Linux convention – six groups of two hexadecimal values separated by colons (**:**).
- **BPF Expression** – You can filter the type of traffic the Packet Sensor receives using a tcpdump-style syntax.
- **Comments** – Comments about the Packet Sensor can be saved here. They are not visible elsewhere.

To start the Packet Sensor, click the gray square button next to its name in Configuration » Components. Ensure that the Packet Sensor starts properly by watching the event log (details on page 32).

If the Packet Sensor starts without errors, but you can't see any data collected by it in Reports » Components » Overview, follow the troubleshooting guide from page 22.

Packet Sensor Optimization Steps for Intel 82599

To distribute the packet-processing tasks of the Packet Sensor over multiple CPU cores when using an adapter with the Intel 82599 chipset (Intel X520, Intel X540, HP X560, etc.):

- ✔ Follow the documentation and optimization guides provided by the network adapter vendor.
- ✔ Install PF_RING 6.2 and switch to the ZC or PF_RING-aware ixgbe driver.
- ✔ See the number of RSS queues allocated by the ixgbe driver by executing dmesg, or by listing /var/log/messages or /var/log/syslog. By default, the number of RSS queues is equal to the number of CPU cores when hyper-threading is off, or double the number of CPU cores when hyper-threading is on. You can set the number of RSS queues manually, by loading ixgbe.ko with the RSS=<number> option.
- ✔ Define multiple Packet Sensors, each listening to ethX@queue_id or ethX@queue_range. All Packet Sensors defined to listen to a single interface use a single Sensor license.
- ✔ Add the Packet Sensors to a Sensor Cluster to have a unified reporting and anomaly detection domain.

On a quad-core CPU with multithreading, the ixgbe driver will allocate 8 RSS queues. In this case, if you define a Packet Sensor for ethX@0-3 and another one for ethX@4-7, the packet-processing task will be distributed over 2 CPU cores. PF_RING exposes up to 32 RSS queues.

Packet Sensor Optimization Steps for Myricom

To distribute the packet-processing tasks of the Packet Sensor over multiple CPU cores with a Myricom adapter:

- ✔ Follow the documentation provided by Myricom in order to install Sniffer10G v2 or v3 (recommended).
- ✔ Start the driver with `/opt/snf/sbin/myri_start_stop start`
- ✔ Check that the driver is loaded successfully with `lsmod | grep myri_snf`. Check for errors in syslog.
- ✔ Define multiple Packet Sensors, one for each CPU core if needed.
- ✔ For each Packet Sensor, set the Capture Engine parameter to “Myricom Sniffer10G”, and click the <Capture Engine Options> button on the right. Set the **Packet Sensor Rings** parameter to the number of Packet Sensors listening to the interface. Sniffer10G v3 users must set two unique **App IDs** for Packet Sensors and Packet Tracers listening to the same interface to ensure that the traffic is directed to both applications.
- ✔ Stop all Packet Sensors before changing the **Capture Engine** parameter.
- ✔ Add the Packet Sensors to a Sensor Cluster to have a unified reporting and anomaly detection domain.

Packet Sensor Troubleshooting

- ✔ Look for warnings or errors produced by the Packet Sensor in the event log (details on page 32).
- ✔ Ensure that you have correctly configured the Packet Sensor. Each configuration field is described in detail in this chapter.
- ✔ Make sure that the sniffing interface is up:

  ```
  ip link show <interface_usually_eth1_or_p1p2>
  ```
- ✔ Ensure that you have correctly configured the switch/TAP to send packets to the server on the configured interface.
- ✔ Verify whether the server is really receiving packets through the configured interface:

  ```
  tcpdump -i <interface_usually_eth1_or_p1p2> -n -c 100
  ```
- ✔ When **IP Validation** is not disabled, make sure that the selected IP Zone contains all your subnets.
- ✔ If the CPU usage of the Packet Sensor is too high, set the **Top Generator** parameter to “Basic”, install PF_RING (no ZC/DNA/LibZero required!), or use a network adapter that allows distributing Packet Sensors over multiple CPU cores.
- ✔ To troubleshoot Sensor graph or IP graph issues, follow the Graphs Troubleshooting guide from page 15.
- ✔ For PF_RING installation issues, contact ntop.org. To increase the maximum number of PF_RING programs from 64 to 256, increase the MAX_NUM_RING_SOCKETS defined in kernel/linux/pf_ring.h and recompile the pf_ring kernel module.
- ✔ Make sure you are running the latest version of the software.

Configuration » Components » Flow Sensor

Many routers and switches can collect IP traffic statistics and periodically export them as flow records to a **Flow Sensor**. Because the flow protocol already performs pre-aggregation of traffic data, the flow data sent to Flow Sensor is much smaller than the monitored traffic. This makes the Flow Sensor a good option for monitoring remote or high-traffic networks. The advantages and disadvantages of flow-based monitoring are listed on page 6.

For detailed instructions on how to enable NetFlow, sFlow or IPFIX on your network device, consult its documentation. Appendix 2 from page 57 contains some examples on how to configure NetFlow on few Cisco IOS, CatOS and Juniper devices.

To add a Flow Sensor, click the <+> button from the title bar of the Configuration » Components panel. To modify an existing Flow Sensor, go to Configuration » Components and click its name.

The Flow Sensor Configuration window contains the following fields:

- **Sensor Name** – A short name to help you identify the Flow Sensor.
- **Device Group** – Optional description used within Console to group components by location, role, etc.
- **Reports Visibility** – Whether the Flow Sensor should be listed inside the Reports » Components panel.
- **Sensor Server** – The server that runs the Flow Sensor. The configuration of servers is described on page 18.
- **Listener IP:Port** – The IP address of the network interface that receives flows and the destination port.
- **Repeater IP:Port** – An embedded packet repeater can send all incoming flows to another host or collector. Optional.
- **Flow Collector** – When enabled, all flow data is stored in a space-efficient binary format. Flow records can be queried in Reports » Tools » Flow Collectors.
- **Sensor License** – The license used by the Flow Sensor. WanGuard provides all features; WanSight does not provide traffic anomaly detection and reaction.
- **Flow Protocol** – The flow protocol used by the flow exporter: NetFlow, IPFIX or sFlow.
- **Flow Exporter IP** – The IP address of the flow exporter (router, switch, probe). Usually it is the loopback address of the router. For sFlow exporters, enter the IP that sends flow packets, not the Agent IP.
- **Sampling (1/N)** – Must contain the sampling rate configured on the flow exporter, or 1 when no sampling rate is configured. For NetFlow v9 and sFlow the value entered here is ignored because the sampling rate is automatically adjusted by the flow protocol. To force a particular sampling value, enter a negative value.
- **Flow Timeout (s)** – For flow exporters that maintain the start time of flows, such as Juniper MX, set the same flow-active/inactive-timeout value as the one defined in the flow exporter's configuration. The value must be entered in seconds (s).
- **Time Settings** – The time offset between the time zone (TZ) of the Flow Sensor server and the flow exporter. Running NTP on both devices to keep their clocks synchronized is a critical requirement for

Flow Sensor.

- **IP Zone** – Flow Sensor needs an IP Zone from which to learn the monitored network's boundaries and to extract per-subnet settings. For more information about IP Zones consult the “IP Zone” chapter on page 17.
- **Graphs Accuracy** – Low values increase the accuracy of Sensor graphs, at the expense of increasing the RAM usage. Setting this to under 20 seconds is not recommended.
- **IP Validation** – This option can be used to distinguish the direction of traffic or to ignore certain flows:
  - *Off* – Flow Sensor analyzes all flows and the traffic direction is established by interface.
  - *On* – Flow Sensor analyzes the flows that have the source and/or the destination IP in the selected IP Zone.
  - *Strict* – Flow Sensor analyzes only the flows that have either the source or the destination IP in the IP Zone.
  - *Exclusive* – Flow Sensor analyzes only the flows that have the destination IP in the IP zone, but not the source IP.
- **AS Validation** – Flows from BGP-enabled routers usually contain the source and destination AS (Autonomous System) number. In most configurations, if the AS number is set to 0, then the IP address belongs to your AS.

  If enabled, only flows having the AS number set to “0” (your AS) are processed. This is rarely-used option used for establishing traffic direction. AS validation has three options:
  - *Off* – Disables AS validation.
  - *On* – Only flows that have the source ASN and/or the destination ASN set to 0 are analyzed.
  - *Strict* – Only flows that have either the source ASN or the destination ASN set to 0 are analyzed.
- **SNMP Settings** – Configure the SNMP settings of the flow exporter to allow Console to extract interface information. When the SNMP settings are not configured, you must enter the SNMP index, speed, etc. manually for each interface.
- **Monitored Network Interfaces** – The list of interfaces that should be monitored. To avoid producing duplicate flow entries, add only upstream interfaces. Settings per interface:
  - *SNMP Index* – The interfaces are identifiable in flows only by their SNMP indexes. Enter the index manually, or configure the SNMP settings.
  - *Interface Name* – A short description used to identify the monitored interface. Descriptions longer than 10 characters clutter some reports.
  - *Graph Color* – The color used in graphs for the interface. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
  - *Traffic Direction* – The direction of traffic entering the interface, relative to your network:
    - “Auto” – Set to establish the direction of traffic by IP and/or AS Validation.
    - “Upstream” – Set for upstream interfaces, e.g. peering interfaces, interfaces connected to the Internet.
    - “Downstream” – Set for downstream interfaces, e.g. customer interfaces, interfaces connected to your network.

- "Null" – Traffic to Null interfaces is discarded by the router and should be ignored.

- *Top Generator* – Allows generating traffic tops:
  - "Basic" – Enables tops for Internal IPs, IP protocols, versions and TCP/UDP ports. It adds a very small performance penalty.
  - "Extended" (recommended) – Enables all tops from "Basic" as well as tops and graphs for autonomous systems and countries, but increases the CPU usage by a few percentage points. When the router does not export AS information (e.g. non-BGP router) Flow Sensor uses an internal GeoIP database to get ASNs. Live stats for autonomous systems and countries are not very accurate.
  - "Full" – Enables all tops from "Extended" as well as tops for external IPs (IPs not included in the IP Zone), but increases the RAM usage several times over, especially during spoofed attacks. Live stats for autonomous systems and countries are very accurate. Set the value to "Extended", unless you know what you are doing.
- *Link Speed In & Link Speed Out* – Enter the speed (bandwidth, capacity) of the interface. The values are used for percentage-based reports.

- **Comments** – Comments about the Flow Sensor can be saved here. These comments are not visible elsewhere.

To start the Flow Sensor, click the gray square button next to its name in Configuration » Components. Ensure that the Flow Sensor starts properly by watching the event log (details on page 32).

If the Flow Sensor starts without errors, but you can't see any data collected by it in Reports » Components » Overview after more than 5 minutes, follow the troubleshooting guide below.

Flow Sensor Troubleshooting

- ✔ Look for warnings or errors produced by the Flow Sensor in the event log (details on page 32).
- ✔ Check if you have correctly configured the Flow Sensor. Each configuration field is described in detail in the previous section.
- ✔ Ensure that the server is receiving flow packets on the configured **Listener IP:Port**:

```
tcpdump -i <interface_eth0_or_p1p1_etc> -n -c 100 host <flow_exporter_ip> and udp
and port <destination_port>
```

- ✔ Make sure that the local firewall permits the Flow Sensor to receive flow packets:

```
iptables -L -n -v && iptables -t raw -L -n -v
```

- ✔ Ensure that the clocks of both devices are synchronized with NTP. When the devices do not reside in the same time zone, adjust the **Time Settings** parameter from the Flow Sensor configuration accordingly.
- ✔ The Flow Sensor may crash during spoofed attacks for not having enough RAM, when a monitored interface has the *Top Generator* parameter set to "Full". It is highly recommended to set the **Top Generator** parameter to "Extended", not to "Full".
- ✔ If you define interfaces with the **Traffic Direction** parameter set to "Auto", make sure that the IP Zone you have selected for the Flow Sensor contains all your IP blocks.

- ✔ In order to provide fast and up-to-date traffic statistics, the Flow Sensor accepts only flows generated in the last 5 minutes. All flows aged with delay exceeding 5 minutes (300 seconds) are automatically discarded with the event log warning "*Wrong flow timeout settings! Received flow <starting/ending> <X> seconds ago*".

  When the warnings refer to the starting time, make sure that the clocks are synchronized, the flow exporter is properly configured, and the time-zone and the **Flow Timeout** parameter are properly set.

  When the warnings refer to the ending time, make sure that the clocks are synchronized, the time-zone is properly set and the flow exporter is properly configured.

  You can double-check whether the time of the Flow Sensor and the start/end time of flows really differ by more than 300 seconds. In Reports » Tools » Flow Collectors » Flow Records, select the Flow Sensor, set Output to Debug and generate a listing for the last 5 minutes:

  - The Date_flow_received column indicates the time when the Flow Sensor received the flow packet
  - The Date_first_seen column indicates the time when the flow started
  - The Date_last_seen column indicates the time when the flow ended

  Flow Sensor does not misinterpret the start/end time of flows. A few flow exporters are known to have bugs or limitations regarding flow aging. In this case, contact your vendor to make that the flow exporter is correctly configured and it is able to expire flows in under 5 minutes.

- ✔ Ensure that you have correctly configured the flow exporter to send flows to the server for each of the monitored interfaces. To list all interfaces that send flows, go to Reports » Tools » Flow Collectors » Flow Tops, select the Flow Sensor, set Output to Debug, set Top Type to Any Interface and generate the top for the last 10 minutes. The In/Out_If column shows the SNMP index of every interface that exports flows, whether or not it was configured as a monitored interface in the Flow Sensor configuration.

- ✔ If you see statistics for only one traffic direction (inbound or outbound), go to Reports » Tools » Flow Collectors » Flow Records, and generate a listing for the last 10 minutes. If all your IPs are listed in a single column, check the flow exporter's configuration and feature list. Not all devices can export flows in both directions (e.g. Brocade equipments generate only inbound sFlow) or with the same SNMP interface index.

- ✔ The traffic readings of the Flow Sensor may differ from the SNMP Sensor or from other SNMP-based monitoring tools. Flow Sensor counts In/Out traffic as traffic entering/exiting the IP Zone (when **IP Validation** is enabled), unlike SNMP tools that count In/Out traffic as traffic entering/exiting the interface. You can double-check the traffic readings of a Flow Sensor by configuring a SNMP Sensor that monitors the same flow exporter (page 27).

- ✔ If the Flow Sensor does not show the correct statistics after upgrading the router's firmware, the SNMP index of the interfaces may have changed. In this case, enter the new SNMP index for each monitored interface.

- ✔ To troubleshoot Sensor graph or IP graph issues, follow the Graphs Troubleshooting guide from page 15.

- ✔ Make sure you are running the latest version of the software.

Configuration » Components » SNMP Sensor

SNMP Sensor monitors the bandwidth usage of routers and switches on a port-by-port basis. SNMP Sensor queries devices (e.g. routers, switches and servers) for the traffic counters of each port with small data packets. These are triggering reply packets from the device. The advantages and disadvantages of monitoring traffic by SNMP are listed on page 6.

For detailed instructions on how to enable SNMP on your network device, consult its documentation.

To add a SNMP Sensor click the <+> button from the title bar of the Configuration » Components panel. To modify an existing SNMP Sensor, go to Configuration » Components and click its name.

The SNMP Sensor Configuration window contains the following fields:

- **Sensor Name** – A short name to help you identify the SNMP Sensor.
- **Device Group** – Optional description used within Console to group components by location, role, etc.
- **Reports Visibility** – Whether the SNMP Sensor should be listed inside the Reports » Components panel.
- **Sensor Server** – The server that runs the SNMP Sensor. It is recommended to run all SNMP Sensors on the Console server. The configuration of servers is described on page 18.
- **Polling Interval** – Polling is the process of sending the SNMP request periodically to the device to retrieve information. A low polling interval (of say 1 minute) gives you granular reports but may place an increased load on your server if you poll large amount of interfaces.
- **Sensor License** – The license used by the SNMP Sensor. WanGuard provides all features (although severely limited by the SNMP technology); WanSight does not provide traffic anomaly detection and reaction.
- **IP Zone** – When a WanGuard license is being used, the SNMP Sensor is able to check thresholds listed in the selected IP Zone with the following restrictions (SNMP does not provide any information about IPs or protocols):
  - Subnet must be “0.0.0.0/0”.
  - Domain must be “subnet”.
  - Value must be absolute, not percentage.
  - Decoder must be “TOTAL”.
- **Device IP:port** – Enter the IP address and SNMP port of the networking device. The standard SNMP port is 161.
- **Timeout (ms)** – The timeout value should be at least a little more than double the time it takes for a packet to travel the longest route between devices on your network. The default value is 1000 milliseconds (1 second).
- **Retries** – This value represents the number of times the SNMP Sensor will retry a failed SNMP request defined as any SNMP request that does not receive a response within the Timeout (ms) defined above. The default value is 2.

- **Discovery** – Activates or deactivates interface discovery:
  - *Monitor all interfaces* – Select to automatically add all interfaces to the SNMP Sensor. The interface names are based on the **Interface Name** setting available when pressing the <**OIDs and Tester**> button.
  - *Monitor defined interfaces* – Select to monitor only interfaces listed in the SNMP Sensor configuration.
- **Authentication Protocol** – Select the SNMP protocol used for authentication:
  - *SNMP v1* – The oldest version. Easy to set up – only requires a plaintext community. The biggest downsides are that it does not support 64 bit counters, only 32 bit counters, and that it has little security.
  - *SNMP v2c* – Version 2c is identical to version 1, except it adds support for 64 bit counters. This is very important when monitoring gigabit interfaces. Even a 1Gbps interface can wrap a 32 bit counter in 34 seconds, which means that a 32 bit counter being polled at one minute intervals is useless. Select this option instead of v1 in most cases.
  - *SNMP v3* – Adds security to the 64 bit counters. SNMP version 3 adds both encryption and authentication, which can be used together or separately. Setup is much more complex than just defining a community string.
- **Community String** – SNMP v1 and v2c credentials serve as a type of password that is authenticated by confirming a match between the string provided here and the SNMP Community String stored as a MIB object on an SNMP-enabled, managed device.
- **Security Level & Name** – SNMP v3-only. SNMP Sensor supports the following set of security levels as defined in the USM MIB (RFC 2574):
  - *noAuthnoPriv* – Communication without authentication and privacy.
  - *authNoPriv* – Communication with authentication and without privacy.
  - *authPriv* – Communication with authentication and privacy.
- **Authentication Protocol & Passphrase** – SNMP v3-only. The protocols used for Authentication are *MD5* and *SHA* (Secure Hash Algorithm).
- **Privacy Protocol & Passphrase** – SNMP v3-only. An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value *DES* (CBC-DES Symmetric Encryption) or *AES* (Advanced Encryption Standard).
- **Monitored Network Interfaces** – The interfaces that should be monitored. To avoid mirrored graphs, add only upstream interfaces. Settings per interface:
  - *SNMP Index* – The interfaces are identifiable by their unique indexes.
  - *Interface Name* – A short description used to identify the monitored interface. Descriptions longer than 10 characters clutter some reports. By default, the auto-filled interface name is retrieved from the ifAlias OID. To change the OID used for the interface name click the <**OIDs and Tester**> button.
  - *Graph Color* – The color used in graphs for the interface. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
  - *Traffic Direction* – The direction of the traffic entering the interface, from the user's perspective:
    - "Unset" – Traffic entering the interface is considered "downstream"; traffic exiting the interface

is considered “upstream”.

- “Upstream” – Set for upstream interfaces, e.g. peering interfaces, interfaces connected to the Internet.
- “Downstream” – Set for downstream interfaces, e.g. customer interfaces, interfaces connected to your network.
- “Null” – Traffic to Null interfaces is ignored.

  - *Link Speed In & Link Speed Out* – Enter the speed (bandwidth, capacity) of the interface. The values are used for percentage-based reports.

- **Comments** – Comments about the SNMP Sensor can be saved here. These comments are not visible elsewhere.

To start the SNMP Sensor, click the gray square button next to its name in Configuration » Components. Ensure that the SNMP Sensor starts properly by watching the event log (details on page 32).

If the SNMP Sensor starts without errors, but you can't see any data collected by it in Reports » Components » Overview after more than 5 minutes, follow the troubleshooting guide below.

SNMP Sensor Troubleshooting

- ✔ Look for warnings or errors produced by the SNMP Sensor in the event log (details on page 32).
- ✔ Ensure that you have correctly configured the SNMP Sensor. Each configuration field is described in detail in this chapter.
- ✔ Verify if the Console can reach the device by clicking the <**OIDs and Tests**> button from the SNMP Sensor Configuration window, then press <**Query Device**>.
- ✔ Permit the server to contact the SNMP device, by configuring its ACL.
- ✔ If Sensor graphs are very spiky, increase the Polling Interval value.
- ✔ Make sure you are running the latest version of the software.

Configuration » Components » Sensor Cluster

Sensor Cluster aggregates traffic data provided by Packet Sensors and Flow Sensors into a single IP graphing domain.

To add a Sensor Cluster, click the <+> button found on the title bar of the Configuration » Components panel. To configure an existing Sensor Cluster, go to Configuration » Components, and click its name.

The Sensor Cluster Configuration window contains the following fields:

- **Sensor Name** – A short name to help you identify the Sensor Cluster.
- **Graph Color** – The color used in graphs for the Sensor Cluster. The default color is a random one, which can be changed by entering a different HTML color code or by clicking the drop-down menu.
- **Reports Visibility** – Whether the Sensor Cluster should be listed inside the Reports » Components panel.
- **Device Group** – Optional description used within Console to group components by location, role, etc.
- **Sensor Server** – The server that runs the Sensor Cluster. It is recommended to run Sensor Clusters on the Console server. The configuration of servers is described on page 18.
- **Link Speed IN / OUT** – The summed-up speeds (bandwidth, capacity) of the aggregated interfaces. The values are used for percentage-based reports.
- **Associated Sensors** – Select which Packet Sensors and Flow Sensor interfaces must be aggregated by the Sensor Cluster.
- **IP Zone** – Sensor Cluster extracts from the selected IP Zone per-subnet settings about thresholds and/or IP graphing. For more information about IP Zones consult the “IP Zone” chapter on page 17.
- **IP Graphing** – Select “Aggregated” to enable IP graphing by the Sensor Cluster for the summed up traffic data, and disable IP graphing by the associated Sensors. Select “Not Aggregated” to enable IP graphing by each associated Sensor and to disable IP graphing by the Sensor Cluster.
- **Comments** – Comments about the Sensor Cluster can be saved here. These comments are not visible elsewhere.

To start the Sensor Cluster, click the gray square button next to its name in Configuration » Components.

Ensure that the Sensor Cluster starts properly by watching the event log (details on page 32) and by monitoring Reports » Components » Overview.

Configuration » Schedulers » Scheduled Reports

One of the greatest strengths of the Console is the ease in which it can generate complex Reports. Most reports created by clicking items from the Reports Region can be printed, exported as PDFs or sent by email.

If you want to receive periodic reports by email without having to log into Console, go to Configuration » Schedulers and click the <+> button from the title bar of the panel.

You can include more than one email address in the **Email To** field by separating addresses with a comma.

The emails are sent periodically according to the settings in the **Scheduler** tab.

To see how the email would look like without waiting for the preconfigured time, enter your email address, and then click the <**Save & Execute Now**> button. You should receive the email containing the report within a few seconds. If you do not, verify the settings from Configuration » General Settings » Outgoing Email.

All emails are formatted as HTML messages and include MIME attachments.

Configuration » Schedulers » Event Reporting

Events are short text messages that describe the change of an operational status. They are generated by WanSight components and logged by Console.

You can list events in Reports » Components » [Component Name] » [Component Type] Event sub-tab. To search, sort or filter event messages, click the small down arrow that appears when hovering over the Event column header. To see additional details about an event click the <+> button from the first column.

To see a recent list of **Latest Events**, click the small bottom edge of the window to raise the South Region, or press Ctrl+E. On one side the Latest Events tab displays the latest 60 events, while on the other side it displays a list of components that can generate events and the number of events generated in the last 24 hours by each component. The number's color indicates the maximum severity of the events: red means that there are ERRORS, blue is for INFO events, etc.

The event's **severity** indicates its importance:

- **MELTDOWN** – Meltdown events are generated in very serious situations, such as hardware failures.
- **CRITICAL** – Critical events are generated when significant software errors occur, such as a memory exhaustion situation.
- **ERROR** – Error events are usually caused by misconfigurations, communication errors between components, or bugs. Sensors auto-recover from errors by restarting themselves.
- **WARNING** – Warning events are generated when authentication errors occur, on I/O bottlenecks or when there are time synchronization issues.
- **INFO** – Informational events are generated when configurations are changed or when users log into Console.
- **DEBUG** – Debug events are generated to help troubleshooting coding errors.

As an administrator, you should keep events with high severities under surveillance! Configure Console to send important events periodically by email, Syslog or SNMP in Configuration » Schedulers » Event Reporting.

Configuration » General Settings » Outgoing Email

Console sends notification emails using the settings from Configuration » General Settings » Outgoing Email.

Email configuration options:

- **From Email** – The email address you would like to appear as the sender.
- **From Name** – The name as you would like it to appear on messages.
- **Mailer** – Console supports several mailing systems:
  - *PHP Mail* – Use the PHP mail() function. To use it, you may have to configure a Mail Transfer Agent (postfix, qmail, sendmail) on the Console server.
  - *SMTP* – Use the integrated SMTP support to send emails directly, without using a local Mail Transfer Agent.
  - *Sendmail* – Send mails using the sendmail command. To use it, you may have to configure a Mail Transfer Agent (postfix, qmail, sendmail) on the Console server.
- **SMTP Security** – Security options:
  - *None* – No encryption.
  - *SSL* – Enable SSL encryption.
  - *TLS* – Enable TLS encryption.
- **SMTP Host** – Specify the SMTP server(s). You can include backup SMTP server(s) separated by the ";" character.
- **SMTP Port** – TCP port to connect to, usually 25 (insecure) or 587 (secure, uses SSL/TLS).
- **SMTP Login/Password** – Credentials used for SMTP authentication. When the fields are empty, no authentication is performed.
- **Email Tester** – Send a test email to verify the settings.

Configuration » General Settings » User Management

To add, modify or delete Console user accounts click Configuration » General Settings » User Management.

Each Console user must be assigned to one role (access level):

- **Administrator** – Has full privileges. Can manage other user accounts. Is the only role allowed to access Configuration » General Settings » License Manager.
- **Operator** – Can change any configuration but is not allowed to modify user accounts.
- **Guest** – Has read-only access to Console, without access to any configuration. Can have a granular, permission-based access to specific reports, dashboards, Sensors, IP groups, tools, etc.

To add a Console account, press <**Add User**> and the select the desired role. You can modify an account by double-clicking it, or by selecting it and by pressing the <**Modify User**> button.

The **Active** checkbox enables or disables the selected account.

There are two **Authentication** options:

- Local Password – The user is authenticated with the password entered in the **Password** field. All passwords are stored encrypted.
- Remote Authentication – The user is authenticated by remote LDAP or RADIUS servers configured in Configuration » General Settings » User Management (details on page 35).

The **Full Name**, **Company**, **Position**, **Email, Phone** and **Comments** fields are optional. These details are not used anywhere else.

Landing Tab shows the tab that will open immediately after logging in. The list is dynamic and expands as you add Sensors, dashboards, IP groups etc. Set the Landing Tab to a relevant dashboard or report.

Minimum Severity shows the minimum severity level of events displayed in Console.

Reports Region lets you switch the position of the Reports Region (described on page 12) to east or west.

Configuration Region lets you switch the position of the Configuration Region (described on page 12) to east or west.

Console Theme lets you change the Console look after re-login. The most popular themes are the corporate “Gray” and the futuristic/industrial “Azenis”.

Configuration » General Settings » User Authentication

To configure remote authentication mechanisms and login window settings click Configuration » General Settings » User Authentication.

Persistent Sessions enable cookie-based authentication for Console users that select the *Remember* option in the login screen. Subsequent sessions will skip the login screen for the next 30 days or until the user logs off.

Authentication Mode enables or disables the authentication of Console users that are not defined in Configuration » General Settings » User Management, but defined in LDAP or Radius.

Console permits the use of external Radius and LDAP servers for end user authentication.

LDAP server settings:

- **Priority** – You can set the order in which Console connects to multiple authentication services. The authentication process stops after the first successful authentication.
- **Template User** – Remotely authenticated users without a Console account have the privileges of the Template User.
- **LDAP Host** – IP or hostname of the LDAP server. To connect to a LDAP server by SSL, set this parameter as *ldaps://<IP>/*.
- **Login Attribute** – Enter the LDAP attribute that contains the username. For Active Directory is may be *mailNickname* or *sAMAccountName*, for OpenLDAP or IBM Directory Server it may be *uid*.
- **LDAP Base DN** – Specify the location in the LDAP hierarchy where Console should begin searching for usernames for authorization requests. The base DN may be something equivalent to the organization, group, or domain name (AD) of external directory: *dc=domain,dc=com*.
- **Bind User DN/Password** – Distinguished name and password for a LDAP user permitted to search within the defined Base DN.
- **Search Filter** – May contain rules that restrict which users are authenticated using the current configuration. For example, the string "|(department=*NOC*)(department=ISP)" will only allow users from departments containing the string “NOC” or (|) from the “ISP” department to authenticate in Console.

RADIUS server settings:

- **Priority** – You can set the order in which Console connects to multiple authentication services. The authentication process stops after the first successful authentication.
- **Template User** – Remotely authenticated users without a Console account have the privileges of the Template User.
- **RADIUS Host** – IP or hostname of the Radius server.

- **RADIUS Port** – Port through which the Radius server is listening for authentication requests.
- **RADIUS Protocol** – Protocol used for authentication purposes:
  - **PAP** (Password Authentication Protocol) – provides a simple method for the peer to establish its identity using a 2-way handshake
  - **CHAP** (Challenge-Handshake Authentication Protocol) – authenticates a user or network host to an authentication entity
  - **MSCHAP** – is the Microsoft version of the Challenge-handshake authentication protocol, CHAP
  - **MSCHAP2** – is another version of Microsoft version of the Challenge-handshake authentication protocol, CHAP
- **RADIUS Secret** – Enter the credentials for connecting to the Radius server.

The contents of the **Login Window Notification** field is shown inside the Console login window.

The contents of the **Successful Window Notification** field is shown inside the Console window after logging in.

Reports » Tools

The **Reports » Tools** panel contains links to the **Flow Collectors** and **Packet Tracers** tabs.

Reports » Tools » Flow Collectors

The **Reports » Tools** panel contains a link to **Flow Collectors** if there is at least one Flow Sensor in use. The number of active Flow Collectors is displayed within the panel.

Here you can list, aggregate, filter and sort flow records, generate traffic tops and statistics.

The tab contains 2 sub-tabs, located at the left lower side of the window:

Flow Records

You can list and filter flow data. The options are:

- **Flow Sensors** – Select the interfaces you are interested in. Administrators can restrict the interfaces accessible by guest accounts.
- **Time Frame** – Select a predefined time frame, or select “Custom...” to enter a specific time interval, in order to list flows that started or ended inside the interval. Time-zone differences between the Console server and remote Flow Sensor servers are not automatically adjusted.
- **Flow Filtering Expression** – Here you can enter a filtering expression for flows. Click the light bulb icon on the right to open a window that will show you the correct syntax. Frequently- used flow filters can be saved there and reused at a later time.
- **Output** – You can select several output formats, or you can type your own format. Click the light bulb icon on the left to open a window that will show you the correct syntax.
- **Export** – If the output is not very large, it can be emailed or printed.

  If you need to list huge amounts of flow data, doing it solely from within the web browser may not be a good idea. In this case, select the “Dump” option to view the CLI command used for flow listing. You can execute that CLI command from the shell and forward the output to a file.
- **Aggregation** – By default, flows are not aggregated. By clicking on the appropriate checkboxes, you can select how to aggregate flows. You can aggregate entire subnets by selecting src(dst)IPv4(IPv6)/<subnet bits>.
- **Limit Flows** – List only the first N flows of the selected time slot.
- **Sorting –** When listing flows sent by different interfaces, you can sort them according to the start time of the flows. Otherwise, flows are listed in the sequence of the selected interfaces.

Flow Tops

You can generate tops from flow data. The options are:

- **Flow Sensors** – Select the interfaces you are interested in. Administrators can restrict the interfaces accessible by guest accounts.
- **Time Frame** – Select a predefined time frame, or select "Custom..." to enter a specific time interval, in order to count only flows that started or ended inside the interval. Time-zone differences between a the Console server and remote Flow Sensor servers are not automatically adjusted.
- **Flow Filtering Expression** – Here you can enter a filtering expression for flows. Click the light bulb icon on the right to open a window that will show you the correct syntax. Frequently-used flow filters can be saved there and reused at a later time.
- **Output** – You can select several output formats, or you can type your own format. Click the light bulb icon on the left to open a window that will show you the correct syntax.
- **Export** – If the output is not very large, it can be emailed or printed.

  If you need to list huge amounts of flow data, doing so solely from within the web browser may not be a good idea. In this case, select the "Dump" option to view the CLI command used to list the top. You can execute that CLI command from the shell and forward the output to a text file.
- **Top Type** – Select the top type from the drop-down menu.
- **Aggregation** – By default, flows are not aggregated. By clicking on the appropriate checkboxes, you can select how to aggregate flows. You can aggregate entire subnets by selecting src(dst)IPv4(IPv6)/<subnet bits>.
- **Limit** – Limit the output to only those records whose packets or bytes match the specified condition.
- **Top** – Limit the top listing to the first N records.

Reports » Tools » Packet Tracers

The **Reports » Tools** panel contains a link to **Packet Tracers** when there is at least one Packet Sensor in use. The number of active packet traces is displayed within the panel.

Here you can easily capture packets from various parts of your network using distributed Packet Sensors. You can view the contents of packets directly from Console using an integrated packet analyzer UI.

The tab contains 2 sub-tabs located at the lower left side of the window:

Active Packet Traces

Administrators, operators and guests with packet capturing privileges can generate packet dumps by clicking the <**Capture Packets**> button. The options are:

- **Description** – An optional short description to help you identify the packet trace.

- **Packet Sensor** – Select which Packet Sensors can capture the traffic you are interested in. Administrators can restrict which Packet Sensors are accessible by guest accounts.
- **BPF Expression** – Click the light bulb icon on the right to open a window that explains the Berkley Packet Filter (BPF) syntax. Frequently used BPF expressions can be saved there and reused at later time. Entering a BPF expression is mandatory. To capture all IP traffic enter “ip”.
- **Max. Running Time** – The maximum running time of the capturing thread (process).
- **Stop Capture Time** – When Max. Running Time is set to “Unlimited”, you can set the exact date when the capturing thread will stop.
- **Max. File Size (MB)** – The option is used for splitting packet dumps into multiple files of <number> Mbytes. Before writing a raw packet to a file, the Packet Sensor checks whether the file is currently larger than <number> and, if so, closes the current file and opens a new one.
- **Max. Packets** – The capture stops after receiving <number> packets.
- **Max. Files Number** – Setting this will limit the number of files created for the specified <number>, and begin overwriting files from the beginning, thus creating a “rotating” buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly.
- **Time Rotation (s)** – If specified, this rotates the file every <number> seconds.
- **Sampling Type & Value** – Select “None” when no packet sampling is required. Select “1 / Value” to save just one packet every <value> packets. Select “Value / 5s” to save maximum <value> packets every 5 seconds.
- **Filename Prefix** – The name of the capture file. If any file-rotation options are used, a number will be appended to the filename.
- **Snapshot (bytes/pkt)** – Snarf <number> bytes of data from each packet rather than the default of 65535 bytes. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit this <number> to the smallest number that will capture the protocol information you are interested in.
- **Comments** – This field may contain comments about the packet trace.

All active Packet Traces are listed as a table having the following format:

- **Description [BPF]** – The description and BPF expression of the trace.
- **Sampling** – The type of sampling being used.
- **From** – The date when the Packet Tracer started capturing packets.
- **Until** – The time or the conditions that will cause the Packet Tracer to stop capturing the traffic.
- **Status** – Indicates the status of the Packet Tracer. It is green if it's running, and red if it's not.
- **Packet Tracer** – The Packet Sensor or the Packet Filter used for capturing packets.
- **Files / Size** – The number of dump files generated and the size of the latest dump file.
- **Packets** – The number of packets captured.
- **Actions** – Click the first icon to view the latest dump file in an integrated packet analyzer tab. Click the second icon to download the latest dump file to your computer. If downloading does not work, but

viewing does, increase the values of the *max_execution_time* and *memory_limit* from php.ini. Click the third icon to stop capturing packets.

Packet Trace Archive

By default, packet traces are sorted by time in descending order. By clicking the down arrow of any column header, you can apply row filters, change sorting direction and toggle the visibility of columns.

The <+> sign from the first column expands each row for additional information about the trace and provides access to packet dump files. The columns are explained in the previous section.

Reports » Components

The **Reports » Components** panel contains links to the **Overview**, **Device Group** and **Sensor** tabs.

The Overview tab provides a real-time view on the status of all active WanSight components and servers. The Device Group tab provides a real-time view on the status of the Sensor(s) assigned to the selected device group. The Sensor tab provides data specific to the selected Sensor. Administrators can restrict which device groups and Sensors are accessible by guest accounts.

Reports » Components » Overview

The Overview tab shows self-refreshing tables that display real-time system parameters collected from all active WanSight components and servers:

Console

The table displays the following data:

Status	A green check mark indicates that Console is functioning properly. When a red “X” is displayed, enable the WANsupervisor service on the Console server.
Online Users	Number of active Console sessions.
Avg. DB Bits/s (In/Out)	Average number of bits/s sent and received since the start of the Console database.
Avg. DB Queries/s	Average number of queries per second since the start of the Console database.
DB Clients	Number of DB clients that are currently using the Console database.
DB Connections	Number of active connections to the Console database.
DB Size	Disk space used by the Console database.
Free DB Disk	Disk space available on the partition configured to store the Console database.
Free Graphs Disk	Disk space available on the partition configured to store IP graphs.
Time Zone	Time zone of the Console server.
Console Time	Time on the Console server.
Uptime	Uptime of the Console database.

Servers

The table displays the following data for each server that runs components of WanSight:

Status	A green check mark indicates that the server is connected to Console. When a red “X” is displayed, start the WANsupervisor service and make sure that the clocks are synchronized between the server and the Console server.
Server Name	Displays the name of the server and a colored square with the color defined in its configuration. Click to open a new tab with data specific to the server. Administrators and operators can right-click to open the Server Configuration window.
Load	Load average reported by the Linux kernel for the last 5 minutes.
Free RAM	Available RAM. Swap memory is not counted.
CPU% User	Percentage of CPU resources used by the user space processes. Can be >100% on multiple cores/CPUs (e.g. the maximum value for a quad-core system is 400%).
CPU% System	Percentage of CPU resources used by the kernel. Can be >100% on multiple cores/CPUs (e.g. the maximum value for a quad-core system is 400%).
CPU% IOwait	Percentage of CPU resources waiting for I/O operations. A high number indicates an I/O bottleneck.
CPU% Idle	Percentage of idle CPU resources. Can be >100% on multiple cores/CPUs (e.g. the maximum value for a quad-core system is 400%).
Free Flows Disk	Disk space available on the partition that is configured to store flows.
Free Dumps Disk	Disk space available on the partition that is configured to store packet dumps.
Contexts/IRQs/SoftIRQs	Number of context switches, hardware interrupts and software interrupts per second.
Uptime	Uptime of the operating system.

Sensor Clusters

The table is displayed while there is at least one active Sensor Cluster.

Status	A green check mark indicates that the Sensor Cluster is connected to Console. If you see a red “X” instead, make sure that the WANsupervisor service is running and look for errors in the event log (see page 32).
Sensor Name	Displays the name of the Sensor Cluster and a colored square with the color defined in its configuration. Click to open a new tab with data specific to the Sensor Cluster. Administrators and operators can right-click to open the Sensor Cluster configuration window.
Pkts/s (In / Out)	Inbound and outbound packets/second throughput.

Inbound Bits/s	Inbound bits/second throughput and the usage percent.
Outbound Bits/s	Outbound bits/second throughput and the usage percent.
Received Pkts/s	Number of packet/s reported by the associated Sensors.
IPs (Int.)	Number of IP addresses from to the IP Zone that send or receive traffic.
Dropped	Number of packets dropped by the Server Cluster.
CPU%	Percentage of CPUs used by the Sensor Cluster process.
RAM	Amount of memory used by the Sensor Cluster process.
Start Time	When the Sensor Cluster instance started.
Server	Which server runs the Sensor Cluster. Click to open a new tab with data specific to the server. Administrators and operators can right-click to open the Server Configuration window.

Packet Sensors

The table is displayed while there is at least one active Packet Sensor.

Status	A green check mark indicates that the Packet Sensor is connected to Console. If you see a red "X" instead, make sure that the WANsupervisor service is running and look for errors in the event log (see page 32).
Sensor Name	Displays the name of the Packet Sensor and a colored square with the color defined in its configuration. Click to open a new tab with data specific to the Packet Sensor. Administrators and operators can right-click to open the Packet Sensor Configuration window.
Pkts/s (In / Out)	Inbound and outbound packets/second throughput after IP or MAC validation.
Inbound Bits/s	Inbound bits/second throughput after IP or MAC validation and the usage percent.
Outbound Bits/s	Outbound bits/second throughput after IP or MAC validation and the usage percent.
Received Pkts/s	Rate of sniffed packets before IP or MAC validation.
IPs (Int / Ext)	Number of IP addresses that sent or received traffic. The Int(ernal)/Ext(ernal) IPs are the IPs inside/outside the IP Zone. The Top Generator parameter from the Sensor configuration enables or disables the monitoring of external IPs.
Dropped	Number of packets dropped by the packet capturing engine. A high number indicates a sniffing performance problem.
CPU%	Percentage of CPUs used by the Packet Sensor process.
RAM	Amount of memory used by the Packet Sensor process.
Start Time	When the Packet Sensor started.

Server	Which server runs the Packet Sensor. Click to open a new tab with data specific to the server. Administrators and operators can right-click to open the Server Configuration window.

Flow Sensors

The table is displayed while there is at least one active Flow Sensor.

Status	A green check mark indicates that the Flow Sensor is connected to Console. If you see a red "X" instead, make sure that the WANsupervisor service is running and look for errors in the event log (see page 32).
Sensor Name	Displays the name of the Flow Sensor. Click to open a new tab with data specific to the Flow Sensor. Administrators and operators can right-click to open the Flow Sensor Configuration window.
Interface	The interface name and a colored square with the configured graph color. If the interface names are missing for more than 5 minutes after the Flow Sensor has started, check the troubleshooting guide from page 25.
Pkts/s (In / Out)	Inbound and outbound packets/second throughput after IP or AS validation.
Inbound Bits/s	Inbound bits/second throughput after IP or AS validation and usage percent.
Outbound Bits/s	Outbound bits/second throughput after IP or AS validation and usage percent.
IPs (Int / Ext)	Number of IP addresses that send or receive traffic. The Int(ernal)/Ext(ernal) IPs are the IPs inside/outside the IP Zone. The Top Generator parameter from the Sensor configuration enables or disables the monitoring of external IPs.
Flows/s	Number of flows per second received by the Flow Sensor.
Flows Delay	Because traffic data must be aggregated first, flow devices export flows with a configured delay. Some devices export flows much later than the configured delay and this field contains the maximum flows delay detected by the Flow Sensor. Flow Sensor cannot run with flow delays of over 5 minutes.
Dropped	Number of unaccounted flows. A high number indicates a performance problem of the Flow Sensor or a network connectivity issue with the flow exporter.
CPU%	Percentage of CPU resources used by the Flow Sensor process.
RAM	Amount of RAM used by the Flow Sensor process.
Start Time	When the Flow Sensor started.
Server	Which server runs the Flow Sensor. Click it to open a new tab with data specific to the server. Administrators and operators can right-click to open the Server Configuration window.

SNMP Sensors

The table is displayed while there is at least one active SNMP Sensor.

Status	A green check mark indicates that the SNMP Sensor is connected to Console. If you see a red "X" instead, make sure that the WANsupervisor service is running and look for errors in the event log (see page 32).
Sensor Name	Displays the name of the SNMP Sensor and a colored square with the color defined in its configuration. Click to open a new tab with data specific to the SNMP Sensor. Administrators and operators can right-click to open the SNMP Sensor Configuration window.
Interface	Interface name and a colored square with the configured graph color.
Pkts/s (In / Out)	Inbound and outbound packets/second throughput.
Inbound Bits/s	Inbound bits/second throughput and usage percent.
Outbound Bits/s	Outbound bits/second throughput and usage percent.
Errors/s (In / Out)	For packet-oriented interfaces, it represents the number of inbound and outbound packets that contained errors, preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, it represents the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
Discards/s (In / Out)	Number of inbound and outbound packets which were chosen to be discarded even though no errors had been detected to prevent them from being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Oper. Status	Current operational state of the interface. The *Testing* state indicates that no operational packets can be passed. If Administrative Status is *Down* then Operational Status should be *Down*. If Administrative Status is changed to *Up* then Operational Status should change to *Up* if the interface is ready to transmit and receive network traffic; it should change to *Dormant* if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the *Down* state if and only if there is a fault that prevents it from going to the *Up* state; it should remain in the *NotPresent* state if the interface has missing (typically, hardware) components.
Admin. Status	Desired state of the interface. The *Testing* state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with the Administrative Status in the *Down* state. As a result of either explicit management action or per configuration information retained by the managed system, the Administrative Status is then changed to either the *Up* or *Testing* states (or remains in the *Down* state).
CPU%	Percentage of CPU resources used by the SNMP Sensor process.
RAM	Amount of RAM used by the SNMP Sensor process.
Start Time	When the SNMP Sensor started.
Server	Which server runs the SNMP Sensor. Click it to open a new tab with data specific to the server. Administrators and operators can right-click to open the Server Configuration window.

Reports » Components » Sensors

Click on a Sensor name anywhere in Console to open a tab that contains specific information. The tab includes a few sub-tabs, located at the lower side of the window. All sub-tabs share the following common toolbar fields:

- **Sensors** – Select the Sensors you are interested in, or select "All" to select all Sensors. Administrators can restrict which Sensors are accessible by guest accounts.
- **Time Frame** – Select a predefined time frame, or select "Custom..." to enter a specific time interval.

Sensor Dashboard

The Sensor dashboard allows you to group the most relevant data collected by Sensors. The Sensor dashboard configuration does not apply to a particular Sensor, so the changes you make will be visible for other Sensor dashboards as well. The operation of dashboards is described in the "Reports » Dashboards" chapter on page 50.

The configuration of Sensor widgets is described in the following paragraphs.

Sensor Graphs

This sub-tab allows you to view a variety of Sensor-related histograms for the selected Sensor(s):

- **Data Units** – Select one or more data units:
  - *Most Used* – Frequently-used data units.
  - *Packets* – Inbound packets/second (+ on Y-axis) and outbound packets/second (- on Y-axis).
  - *Bits* – Inbound bits/second (+ on Y-axis) and outbound bits/second (- on Y-axis).
  - *Applications* – Sensor can collect application-specific distribution data for: HTTP, HTTPS, SMTP, POP3, IMAP, SNMP, FTP, SSH, TELNET, SQL, NETBIOS, MS-DS, MS-RDP, DNS, ICMP and OTHERS. The graphs are updated when the Sensor configuration has the Top Generator parameter set to "Basic".
  - *Bytes* – Bytes/second throughput.
  - *Internal* or *External IPs* – Number of IP addresses that send or receive traffic. Internal and External IPs are hosts inside and respectively outside the IP Zone. The Top Generator parameter from the Sensor configuration enables or disables monitoring of External IPs. A spike in the Internal IPs graph usually means that an IP class scan was performed against your IP blocks. A spike in the External IPs graph usually means that you have received a spoofed attack.
  - *Received Frames* – For Packet Sensors, it represents the number of packets/s received before IP or MAC validation. For Flow Sensors, it represents the number of flows/s received before IP or AS validation.
  - *Dropped Frames* – For Packet Sensors, it represents the number of packets dropped by the packet capturing engine. A high number indicates a sniffing performance problem. For Flow Sensors, it

represents the number of unaccounted flows. A high number indicates a wrong configuration of the Flow Sensor or a network connectivity issue with the flow exporter.

- *Unknown Frames* – For Packet Sensors, it represents the rate of packets not passing IP validation. For Flow Sensors, it represents the rate of invalidated flows.
- *Unknown Sources* – Number of source IP addresses that did not pass IP validation.
- *Unknown Destinations* – Number of destination IP addresses that did not pass IP validation.
- *Avg. Packet Size* – Average packet size in bits/packet.
- *CPU%* – Percentage of CPU resources used by the Sensor process.
- *RAM* – Amount of RAM used by the Sensor process.
- *Load* – Load reported by the Linux kernel.
- *IP Graphs* – Number of updated IP graphs files.
- *IP Accounting* – Number of updated IP accounting records.
- *HW Graphs* – Number of updated traffic profiling files.
- *IP Graphs Time* – Number of seconds needed to update the IP graphs files.
- *HW Graphs Time* – Number of seconds needed to update the traffic profiling files.
- *Processing Time* – Number of seconds needed to perform traffic analysis functions.
- *IP Structures* – Number of internal IP structures.
- *IP Structure RAM* – Number of RAM bytes used by each IP structure.

- **Graphs Size** – Select a predefined dimension or enter a custom one in the "<X> x <Y>" format, where <X> and <Y> are the X-axis and Y-axis pixels.
- **Graphs Title** – Graphs can have an automatically-generated title for the "Auto" option, no title for the "None" option, or you can enter your own text to be rendered as a title.
- **Graph Legend** – Select the level of detail for the graph legend.
- **Consolidation** – If you are interested in spikes, select the *MAXIMUM* aggregation type. If you are interested in average values, select the *AVERAGE* aggregation type. If you are interested in low values, select the *MINIMUM* aggregation type.
- **Graph Options**
  - *Stack Sensors* – Select to generate a single stacked graph for all selected Sensors.
  - *Show Totals* – Select to show the summed up values from stacked Sensors.

Sensor Tops

This sub-tab allows you to generate various traffic tops for the selected Sensor(s). The Top Generator parameter from the Sensor configuration enables or disables data collection for various Sensor tops.

- **Top Type** – Select a top type:
  - *Talkers* – Hosts from your network that send or receive the most traffic for the selected decoder.

Available only when the Top Generator parameter from the Sensor configuration is set to “Basic”.

- *IP Groups* – IP groups that send or receive the most traffic for the selected decoder. Available only when the Top Generator parameter from the Sensor configuration is set to “Basic”.
- *External IPs* – External IPs that send or receive the most traffic for the selected decoder. Available when the Top Generator parameter from the Sensor configuration is set to “Extended” or “Full”.
- *Autonomous Systems* – Autonomous systems that send or receive the most traffic. Available only when the Top Generator parameter from the Sensor configuration is set to “Extended” or “Full”.
- *Countries* – Countries that send or receive the most traffic. Available when the Top Generator parameter from the Sensor configuration is set to “Extended” or “Full”.
- *TCP Ports* – Most-used TCP ports. Available when the Top Generator parameter from the Sensor configuration is set to “Basic”.
- *UDP Ports* – Most-used UDP ports. Available when the Top Generator parameter from the Sensor configuration is set to “Basic”.
- *IP Protocols* – Most-used IP protocols. Available when the Top Generator parameter from the Sensor configuration is set to “Basic”.
- *IP Versions* – Most-used IP versions: IPv4 or IPv6. Available when the Top Generator parameter from the Sensor configuration is set to “Basic”.

- **Decoder** – Select the decoder that analyzes the type of traffic that interests you.
- **Direction** – Direction of traffic, *Inbound* or *Outbound*.
- **Group Sensors** – When unchecked, each Sensor generates a different top. When checked, all selected Sensors generate a single top with combined data.
- **DNS** – When checked, it enables reverse DNS resolution for IP addresses. It may slow down generating tops for *Talkers* and *External IPs*.

You can increase the number of top records and change the available decoders in Configuration » General Settings » Graphs & Storage, see page 13.

Generating tops for many Sensors and long time frames may take minutes. If the report page timeouts, increase the *max_execution_time* parameter from *php.ini*.

Flow Records

You can list and filter the flow data collected by the selected Flow Sensors. The options are described in the “Flow Collectors” chapter on page 37. This sub-tab is visible only for tabs opened for Flow Sensors.

Flow Tops

You can generate tops from the flow data collected by the selected Flow Sensors. The options are described in the “Flow Collectors” chapter on page 37. This sub-tab is visible only for tabs opened for Flow Sensors.

AS Graphs

Flow Sensors and Packet Sensors can generate traffic and bandwidth histograms for autonomous systems. This feature is enabled for Packet Sensors that have the Top Generator parameter set to “Full”, and for Flow Sensors that have the Top Generator parameter set to “Full” or “Extended”.

- **AS Numbers** – Click the lightbulb icon on the right to open a window containing the correct syntax. Frequently-searched AS numbers can be saved there, and used at a later time. To see the list of AS numbers owned by a particular organization, go to Help » IP & AS Information » AS Numbers List.
- **Graphs Size** – Select a predefined dimension or enter a custom one in the “<X> x <Y>” format, where <X> and <Y> are the X-axis and Y-axis pixels.
- **Graphs Title** – Graphs can have an automatically-generated title for the “Auto” option or no title for the “None” option, or you can enter your own text to be rendered as a title.
- **Graph Options**
  - *Stack Sensors* – Select to generate a single stacked AS graph for all selected Sensors.
  - *Stack ASNs* – Select to show a single graph for multiple AS numbers.

Country Graphs

Flow Sensors and Packet Sensors can generate traffic and bandwidth histograms for countries. This feature is enabled for Sensors that have the Top Generator parameter set to “Full” or “Extended”.

- **Countries** – Select the country or countries from the drop-down list, or click the light bulb icon on the right to open a window with saved selections for continents and world regions.
- **Graphs Size** – Select a predefined dimension or enter a custom one in the “<X> x <Y>” format, where <X> and <Y> are the X-axis and Y-axis pixels.
- **Graphs Title** – Graphs can have an automatically-generated title for the “Auto” option or no title for the “None” option, or you can enter your own text to be rendered as a title.
- **Graph Options**
  - *Stack Sensors* – Select to generate a single stacked country graph for all selected Sensors.
  - *Stack Countries* – Select to show a single graph for multiple countries.

Sensor Events

This sub-tab lists events generated by the selected Sensor(s) for the selected time frame. The events are described in the “Event Reporting” chapter on page 32.

Reports » Dashboards

Wouldn't it be nice to see all the relevant data in a single tab? **Dashboards** allow you to group data from any report according to your needs.

Any dashboard can be configured to refresh itself on intervals ranging from 5 seconds to 15 minutes.

A few sample dashboards are included by default. If you are a Console administrator or operator you can **create** and configure your own dashboards by clicking Reports » Dashboards » <+> » Dashboard. Guest accounts are not allowed to add or make modifications to dashboards.

In the dashboard **configuration**, you can edit the name of the dashboard, set permissions, layout, or choose to override the time frame of widgets with the time frame of the dashboard.

The dashboard contains **widgets**. To sort them, click the title bar and move them around. To collapse a widget, click the first icon on the widget title bar. To configure a widget, click the second icon from its title bar. To delete a widget, click the third icon from its title bar.

Along with few specific fields, every widget has a configurable title and height. Leave the widget's height parameter set to “Auto” for the widget to take all the vertical space it needs. To restrict the height of a widget, enter a number of pixels instead.

Widget options are self-explanatory or described in other chapters.

Reports » IP Addresses & Groups

This chapter describes how to generate detailed traffic reports for any IP address, block or group included in Configuration » Network » IP Zones. Traffic graphs are available only for IP addresses, blocks or groups that have the IP graphing parameter set to “Yes”. Traffic accounting data is available only when the IP accounting parameter is set to “Yes”.

Reports » IP Addresses panel allows you to quickly generate traffic reports for IP addresses and blocks, either entered in the upper side of the panel, or selected from the expandable tree below.

Reports » IP Groups panel lists all IP groups defined in IP Zones. Select an IP group to generate a traffic report for all IP blocks belonging to it. To search for a specific IP group, enter a sub-string contained in its name in the upper side of the panel.

The traffic report tab includes few sub-tabs located at the lower side of the window. All sub-tabs share the following common toolbar fields:

- **Sensor** – Select the Sensors you are interested in or select “All” to select all Sensors. Administrators can restrict the Sensors accessible by guest accounts.
- **Time Frame** – Select a predefined time frame, or select “Custom...” to enter a specific time interval.

IP Dashboard

The IP dashboard allows you to group the most relevant data collected by the selected Sensors for the selected IP address, block or group. The configuration of IP dashboard does not apply to a particular IP address, block or group, and the changes you make will be visible for other IP dashboards as well. The operation of dashboards is described in the “Reports » Dashboards” chapter on page 50.

The configuration of Decoder Graph widget and IP Accounting widget is described by the following paragraphs.

IP Graphs

Allows you to view traffic histograms generated for the selected IP block, host or group:

- **Decoders & Data Unit** – Select the decoders and data unit you are interested in. Available data units: *Packets*, *Bits* and *Bytes*.
- **Graphs Size** – Select a predefined dimension or enter a custom one in the “<X> x <Y>” format, where <X> and <Y> are the X-axis and Y-axis pixels.
- **Graph Title** – Graphs can have an automatically-generated title for the “Auto” option or no title for the “None” option, or you can enter your own text to be rendered as a title.
- **Graph Legend** – Select the detail of the graph legend.
- **Consolidation** – If you are interested in spikes, select the *MAXIMUM* aggregation type. If you are

interested in average values, select the *AVERAGE* aggregation type. If you are interested in low values, select the *MINIMUM* aggregation type.

- **Graphs Stacking**
  - *Stack Sensors* – Generates a single stacked graph for all selected Sensors.
  - *Stack Decoders* – Generates a single stacked graph for all selected decoders.
  - *Stack IPs* – Uncheck this option if you want a different traffic graph displayed for every IP address contained in the selected IP block or IP group.
  - *Conflicting Decoders* – If decoders can be included one within the other (e.g. TOTAL contains TCP that contains HTTP and HTTPS), the graph will display stacked decoders to show the most specific ones. This generates both accurate and intuitive traffic graphs. In the example above, TOTAL will be displayed as TOTAL OTHER and TCP as TCP OTHER. However, when you select TCP, HTTP and TCP+SYN as decoders, the TCP+SYN decoder can be included in both TCP and HTTP, thus generating a decoder conflict. Check this option to stop detection of conflicting decoders, in order to generate intuitive but potentially inaccurate traffic graphs.
  - *Sum IPs* – Creates a subnet graph by aggregating IP graphs generated for every IP address contained in the subnet. This option will increase the load of the server.

The number of decoders, data units and aggregation types can be modified in Configuration » General Settings » Graphs & Storage (see page 13).

IP Accounting

Allows you to generate traffic accounting reports for the selected IP block, host or group:

- **Decoders & Data Unit** – Select the decoders and data unit that you are interested in. Available data units: *Packets*, *Bits* and *Bytes*.
- **Report Type** – Select the interval used to aggregate the accounting data: *Daily*, *Weekly*, *Monthly*, *Yearly*. The maximum accuracy of traffic accounting reports is 1 day, therefore when you select a shorter time frame you will still see the accounting data collected for the whole day.
- **Sum IPs** – Uncheck this option if you want a different traffic accounting report displayed for each IP address contained in the selected IP block or group.
- **Sum Sensors** – Generates a single traffic accounting report for multiple Sensors.

The number of decoders can be modified in Configuration » General Settings » Graphs & Storage (see page 13).

Flow Records

The sub-tab is visible only when there is at least one Flow Sensor in use.

You can list and filter the flow data collected by the selected Flow Sensors, for the selected IP block, host or group. The options are described in the “Flow Collectors” chapter on page 37.

Flow Tops

This sub-tab is visible only when there is at least one Flow Sensor in use.

You can generate tops from the flow data collected by Flow Sensors, for the selected IP block, host or group. The options are described in the “Flow Collectors” chapter on page 37.

Reports » Servers

Click on a server name anywhere in Console to open a tab containing specific information. The server tab includes a few sub-tabs, located at the lower side of the window. All sub-tabs share the following common toolbar fields:

- **Servers** – Select the servers you are interested in, or select "All" to select all servers. Administrators can restrict the servers accessible by guest accounts.
- **Time Frame** – Select a predefined time frame, or select "Custom..." to enter a specific time interval.

Console / Server Dashboard

Allows you to group the most relevant data collected for a server. The configuration for the server dashboard does not apply to a particular server, and the changes you make will be visible for other server dashboards as well. The operation of dashboards is described in the "Reports » Dashboards" chapter on page 50.

The configuration of Server and Console widgets is described by the following paragraphs.

Console / Server Graphs

Server Graphs allows you to generate various histograms for the selected server(s):

- **Data Units** – Select one or more data units:
  - *Most Used* – Frequently-used data units.
  - *System Load* – Load reported by the Linux kernel.
  - *Free RAM* – Available RAM. The swap memory is not counted.
  - *Database/Graphs/SSD/Flow Collector/Packet Dumps Disk - Free space* – How much disk space is available for each file-system path.
  - *Uptime* – Uptime of the operating system.
  - *CPU% system/userspace/niced/idle* – Percentages of CPU resources used by the system, userspace processes, processes running with increased (nice) priority, and idle loop.
  - *Number of processes* – Total number of processes that are running.
  - *Hardware/Software CPU Interrupts* – Number of CPU interrupts made by hardware and software events.
  - *Context Switches* – Indicates how much time the system spends on multi-tasking.
  - *Running Components* – Number of Sensors.
  - *Clock Delta* – Difference of time between the selected server and the Console server, in seconds. If the value is not zero run ntpd to keep the clock synchronized on all servers.

- *Database/Graphs/SSD/Packet Dumps/Flow Collector Disk - Total* – How much disk space is allocated for the partitions that store the paths.
- *Database/Graphs/SSD/Packet Dumps/Flow Collector Disk - Free Inodes* – Number of free inodes held by the partitions that store the paths.
- *Database/Graphs/SSD/Packet Dumps/Flow Collector Disk - Ops/s* – Number of reads and writes for the partitions that store the paths.
- *Database/Graphs/SSD/Packet Dumps/Flow Collector Disk - Bytes/s* – Number of bytes/s for the partitions that store the paths.
- *Server Interface(s) - Packets/Bits/Errors/Dropped* – Interface statistics collected for the network interfaces defined in the Configuration » Servers.

- **Graphs Size** – Select a predefined dimension or enter a custom one in the "<X> x <Y>" format, where <X> and <Y> are the X-axis and Y-axis pixels.
- **Graphs Title** – Graphs can have an automatically-generated title for the "Auto" option or title for the "None" option, or you can enter your own text to be rendered as a title.
- **Graph Legend** – Select the level of detail for the graph legend.
- **Consolidation** – If you are interested in spikes, select the *MAXIMUM* aggregation type. If you are interested in average values, select the *AVERAGE* aggregation type. If you are interested in low values, select the *MINIMUM* aggregation type.
- **Graph Options**
  - *Stack Servers & Interfaces* – Generate a single stacked graph for all selected servers and server interfaces.
  - *Show Totals* – Shows the summed up values from stacked servers.

Server Events

Lists events generated by the selected server(s). The events are described in the "Event Reporting" chapter on page 32.

Console Events

The sub-tab is visible only when opening the Console tab. It lists events generated by Console. Events are described in the "Event Reporting" chapter on page 32.

Server Commands

Console administrators can execute CLI commands on the selected server(s) and see the output in this sub-tab. The commands are executed by the WANsupervisor service with normal user (non-root) privileges. To prevent the execution of CLI commands through Console, start the WANsupervisor service with the "-n" option.

Appendix 1 – IPv4 Subnet CIDR Notation

WanSight uses extensively IP addresses and IP classes with the CIDR notation. To view details about any IPv4 subnet click Help → Subnet Calculator.

CIDR	CLASS	HOSTS NO.	MASK
/32	1/256 C	1	255.255.255.255
/31	1/128 C	2	255.255.255.254
/30	1/64 C	4	255.255.255.252
/29	1/32 C	8	255.255.255.248
/28	1/16 C	16	255.255.255.240
/27	1/8 C	32	255.255.255.224
/26	1/4 C	64	255.255.255.192
/25	1/2 C	128	255.255.255.128
/24	1 C	256	255.255.255.000
/23	2 C	512	255.255.254.000
/22	4 C	1024	255.255.252.000
/21	8 C	2048	255.255.248.000
/20	16 C	4096	255.255.240.000
/19	32 C	8192	255.255.224.000
/18	64 C	16384	255.255.192.000
/17	128 C	32768	255.255.128.000
/16	256 C, 1 B	65536	255.255.000.000
/15	512 C, 2 B	131072	255.254.000.000
/14	1024 C, 4 B	262144	255.252.000.000
/13	2048 C, 8 B	524288	255.248.000.000
/12	4096 C, 16 B	1048576	255.240.000.000
/11	8192 C, 32 B	2097152	255.224.000.000
/10	16384 C, 64 B	4194304	255.192.000.000
/9	32768 C, 128B	8388608	255.128.000.000
/8	65536 C, 256B, 1 A	16777216	255.000.000.000
/7	131072 C, 512B, 2 A	33554432	254.000.000.000
/6	262144 C, 1024 B, 4 A	67108864	252.000.000.000
/5	524288 C, 2048 B, 8 A	134217728	248.000.000.000
/4	1048576 C, 4096 B, 16 A	268435456	240.000.000.000
/3	2097152 C, 8192 B, 32 A	536870912	224.000.000.000
/2	4194304 C, 16384 B, 64 A	1073741824	192.000.000.000
/1	8388608 C, 32768 B, 128 A	2147483648	128.000.000.000
/0	16777216 C, 65536 B, 256 A	4294967296	000.000.000.000

Appendix 2 – Configuring NetFlow Data Export

This appendix is a brief guide to setting up the NetFlow data export (NDE) on Cisco and Juniper routers or intelligent Cisco Layer 2/Layer 3/Layer 4 switches. If you have problems with the configuration contact your network administrator or consultant. For devices that run hybrid mode on a Supervisor Engine (Catalyst 65xx series) it is recommended to configure IOS NDE on the MSFC card and CatOS NDE on the Supervisor Engine. For more information about setting up NetFlow on Cisco please visit http://www.cisco.com/go/netflow.

Configuring NDE on an IOS Device

In the configuration mode on the router or MSFC, issue the following to start NetFlow Export.

First enable Cisco Express Forwarding:

```
router(config)# ip cef
router(config)# ip cef distributed
```

And turn on flow accounting for each input interface with the interface command:

```
interface
ip route-cache flow
```

For example:

```
interface FastEthernet0
ip route-cache flow
interface Serial2/1
ip route-cache flow
```

It is necessary to enable NetFlow on all interfaces through which traffic (you are interested in) will flow. Now, verify that the router (or switch) is generating flow stats – try command 'show ip cache flow'. Note that for routers with distributed switching (GSR's, 75XX's) the RP cli will only show flows that made it up to the RP. To see flows on the individual line cards use the 'attach' or 'if-con' command and issue the 'sh ip ca fl' on each LC.

Enable the exports of these flows with the global commands:

```
router(config)# ip flow-export version 5
router(config)# ip flow-export destination <ip_address> 2000
router(config)# ip flow-export source FastEthernet0
```

Use the IP address of the server running the Flow Sensor and the configured listening port. UDP port 2000 is used as an example. The ‘ip flow-export source’ command is used to set up the source IP address of the exports sent by the equipment.

If your router uses the BGP protocol, you can configure AS to be included in exports with command:

```
router(config)# ip flow-export version 5 [peer-as | origin-as]
```

The following commands break up flows into shorter segments: 1 minute for active traffic and 30 seconds for inactive traffic. Flow Sensor drops flows older than 5 minutes!

```
router(config)# ip flow-cache timeout active 1
router(config)# ip flow-cache timeout inactive 30
```

In enable mode you can see current NetFlow configuration and state.

```
router# show ip flow export
router# show ip cache flow
router# show ip cache verbose flow
```

Configuring NDE on a CatOS Device

In privileged mode on the Supervisor Engine enable NDE:

```
switch> (enable) set mls nde <ip_address> 2000
```

Use the IP address of the server running the Flow Sensor and the configured listening port. UDP port 2000 is used only as an example.

```
switch> (enable) set mls nde version 5
```

The following command is required to set up flow mask to full flows.

```
switch> (enable) set mls flow full
```

The following commands break up flows into shorter segments: ~1 minute for active flows and ~ 30 seconds for inactive flows. Flow Sensor drops flows older than 5 minutes!

```
switch> (enable) set mls agingtime long 8
switch> (enable) set mls agingtime 4
```

If you want to account all traffic within the specified VLANs rather than inter VLAN traffic use CatOS 7.2 or higher and issue the following command:

```
switch> (enable) set mls bridged-flow-statistics enable
```

And enable NDE:

```
switch> (enable) set mls nde enable
```

To see current NetFlow configuration and state issue the following commands:

```
switch> (enable) show mls nde
switch> (enable) show mls debug
```

Configuring NDE on a Native IOS Device

To configure NDE use the same commands as for the IOS device. In the enable mode on the Supervisor Engine, issue the following to set up the NetFlow export version 5.

```
switch(config)# mls nde sender version 5
```

The following commands break up flows into shorter segments: ~1 minute for active flows and ~ 30 seconds for inactive flows. Flow Sensor drops flows older than 5 minutes!

```
switch(config)# mls aging long 8
switch(config)# mls aging normal 4
```

On the Supervisor Engine 1 issue the following to put full flows into the NetFlow exports:

```
switch(config)# mls flow ip full
```

If you have a Supervisor Engine 2 or 720 running IOS version 12.1.13(E) or higher, issue the following commands instead:

```
switch(config)# mls flow ip interface-full
switch(config)# mls nde interface
```

Configuring NDE on a 4000 Series Switch

Configure the switch the same as an IOS device, but instead of command 'ip route cache flow' use command 'ip route-cache flow infer-fields'. This series requires a Supervisor IV with a NetFlow Services daughter card to support NDE.

Configuring NDE on a Juniper Router (non-MX)

Juniper supports flow exports by the routing engine sampling packet headers and aggregating them into flows. Packet sampling is done by defining a firewall filter to accept and sample all traffic, applying that rule to the interface and then configuring the sampling forwarding option.

```
interfaces {
       ge-0/1/0 {
              unit 0 {
                     family inet {
                            filter {
                                   input all;
                                   output all;
                            }
                            address 192.168.1.1/24;
                     }
              }
       }
}
firewall {
       filter all {
              term all {
                     then {
                            sample;
                            accept;
                     }
              }
       }
}
```

```
forwarding-options {
       sampling {
              input {
                     family inet {
                            rate 100;
                     }
              }
              output {
                     cflowd 192.168.1.100 {
                            port 2000;
                            version 5;
                     }
              }
       }
}
```

Appendix 3 – Software Changelog

WanGuard / WanSight 6.1

Release date: December 3 2015

- Administrators can create custom decoders that identify flows or packets sharing a certain pattern (e.g. to differentiate and classify the underlying protocols) in Configuration » General Settings » Custom Decoders.
- New Filter mitigation options in Configuration » General Settings » Mitigation Options:
  - TCP SYN Proxy
  - invalid TCP flags
  - invalid DNS packets
  - private/reserved IPs
  - connection-oriented or connection-less traffic rate-limiting
  - blacklisting by IP reputation services
- Filter can apply new filtering rules for: specific packet payloads, countries, DNS transaction IDs.
- Filtering rules can be disabled, re-ordered and fine-tuned for each decoder.
- A tighter integration between Filter and the software firewall (Netfilter framework) and Chelsio hardware filters. Newly generated anomaly reports contain pass/drop graphs for mitigated attacks.
- Console users can create custom firewall rules in Reports » Tools » Firewall Rules.
- New Software Firewall options in the Filter Configuration window. A new “FW Policy” field on Whitelist rules that explicitly permits traffic through the Software Firewall.
- Configuration » General Settings » Anomaly Detection contains a new option for deduplicating anomalies that indicate the same attack matched by different decoders.
- Filter Clusters can be associated with other Filter Clusters.
- BGP Connections can be configured to allow BGP announcement withdrawals to be done after business hours.
- Sensor graphs now use RRDCached when it is defined in Configuration » General Settings » Graphs & Storage Configuration.
- Enhanced user authentication methods. New RADIUS options and a new HTTP authentication option.
- A new TCP-ALL decoder.
- The Latest Events tab from the South Region contains selectors for severity and components.
- User role renamed Guest. Administrators can allow Guest access to Reports » Tools with greater granularity.
- Configuration » General Settings » Anomalies renamed Anomaly Detection. Reports » Alerts & Tools renamed Tools.

- Unattended installation when the following shell environment variables are set: WANGUARD_INSTALL_DB_USER, WANGUARD_INSTALL_DB_PASS, WANGUARD_CONSOLE_IP, WANGUARD_CONSOLE_DB_PASS.
- User Guide updated. Contains new Appendixes describing advanced BGP configurations.
- Various small fixes.

WanGuard 6.0

Release date: February 16 2015

System

- The software can be installed on new Linux distributions: Red Hat 7, CentOS 7, Debian 7, Ubuntu Server 14.
- Console supports PHP 5.5 and PHP 5.6.
- Graphs for iowait in Reports » Servers » Server Graphs.
- Configuration » General Settings » Software Updates displays the latest software version and upgrading instructions.
- Emails can be sent directly by Console without requiring a local MTA. New Configuration » General Settings » Outgoing Email Settings, with configurable Sender Email.
- Fixed sending emails to CC addresses.
- Corrupted Console database can be repaired with "/opt/andrisoft/bin/WANmainenance repair".
- 32-bit architectures are no longer supported.

Console

- A new graphical slider for quick selection of custom time frames in Reports.
- Reports and Configuration side regions can be set apart by user preference, e.g. one on the right and one on the left. New Ctrl→R keyboard shortcut toggles side regions.
- Configuration » General Settings » Data Retention shows disk usage for newly created RRD files containing IP graph data.
- Graphing IP sweeps can be enabled or disabled for IPv6 and/or IPv4 in Configuration » General Settings » Graphs & Storage.
- Changed Conditional and Dynamic Parameters: {operation}, {sensor_type}, {domain}, {class}, {filter_*}, {filter_tcpdump_size}.
- New Dynamic Parameters: {from_year}, {from_month}, {from_day}, {from_dow}, {from_hour}, {from_minute}, {until_year}, {until_month}, {until_day}, {until_dow}, {until_hour}, {until_minute}, {direction_to_from}, {software_version}, {comparison}, {direction_receives_sends}, {duration_clock}, {*_decoder_prefix} for {*_prefix}, {filter_type}, {filter}, {filter_id}, {response_actions},

{filtering_rule_log_size}, {filtering_rule_max_unit}, {filtering_rule_unit}.

- Redesigned Response Configuration window. New email templates.
- Redesigned IP Zone Configuration window.
- New widgets: Flow Records and Flow Tops.
- Dashboards can be configured to have a unique time frame for all containing widgets.
- Unprivileged users can open reports for IPs included in the allowed subnets.
- Loading of IP Zones with thousands of IPs and subnets is around 8 times faster.
- Moved Configuration » General Settings » User Management » Authentication & Login to Configuration » General Settings » User Authentication.
- Add Configuration » General Settings » User Authentication » Login Window Notification and Successful Login Notification.
- Radius authentication fixed.
- New statistics in by Reports » Components » Overall » Console.
- Reports » Attacks & Tools » Anomalies » Active Anomalies » Reverse DNS unchecked by default.
- Reports » Attacks & Tools » Anomalies » Active Anomalies shows a Flow Trace button for anomalies detected by Flow Sensors.
- The visibility of items in Reports » Components and Reports » Servers can be toggled. Right-click opens their configuration.
- Configuration » Components and Configuration » Schedulers items can be activated/inactivated with a single right click.
- Configuration » General Settings » License Manager » Requirements lists all the required licensing data.
- Various aesthetic improvements.

Sensor

- Add a new SNMP Sensor, able to monitor networking devices supporting SNMP v1, v2c or v3. One SNMP Sensor license is free.
- The Sniffing Sensor renamed Packet Sensor.
- The Virtual Sensor renamed Sensor Cluster.
- New decoders: IP fragmented, TCP-NULL, TCP+RST, TCP+ACK, TCP+SYNACK, SSDP.
- The BAD decoder matches IP NULL, SYN decoder doesn't match packets/flows with ACK flag set anymore.
- The Packet Sensor is compatible with PF_RING version 6 (Zero Copy, LibZero or DNA license not needed). PF_RING version 5 is not compatible anymore.
- The Packet Sensor supports new capturing engines: System PCAP, Myricom Sniffer10G, SolarCapture (beta).
- The Sensor Cluster can aggregate IP graphs data.
- Packet Sensors listening to the same interface (e.g. for multi-queue load balancing) do not require additional

licenses.

- The Packet Sensor has a new CPU affinity option.
- A new "Manage Interfaces" button in the Flow Sensor Configuration window that provides a quick way to add multiple interfaces.
- The Flow Sensor Configuration window has advanced SNMP options.
- On Flow Sensor's Traffic Direction option. "Mixed" renamed "Auto", "Inbound" renamed "Upstream", "Outbound" renamed "Downstream".

BGP

- Reports » Attacks & Tools » BGP Prefixes renamed BGP Operations.
- Added buttons Reports » Attacks & Tools » BGP Operations » Black Hole, Divert Traffic and Remove All.
- BGP Connections can be configured to announce subnets with configurable masks for BGP peers that do not accept /32 prefixes for null-routing or cloud-based DDoS mitigation services.
- All connections to remote quagga/bgpd services are initialized solely from the Console server.
- Deleting BGP announcements manually works for delayed announcements.
- BGP Announcement Archive displays BGP Connection Role.

Filter

- The Filter renamed Packet Filter.
- A new Flow Filter, able to detect attackers from flow data analyzed by a Flow Sensor.
- A new Filter Cluster, able to cluster multiple Packet Filters and Flow Filters.
- The Filters can use the hardware-based packet filter from Chelsio T4 and T5 10/40 gigabit adapters.
- New Whitelist Templates, for sharing whitelists between Filters. Add them in Configurations » Network & Policy » <+>.
- Support for adding IPv4 and IPv6 subnets in Whitelists and Whitelist Templates.
- The Packet Filter supports new capturing engines: System PCAP, Myricom Sniffer10G, SolarCapture (beta).
- The Packet Filter has a new CPU affinity option.
- The Packet Filter can block private IPs when using the Software Firewall.
- The Filter also works for outgoing attacks.
- The Packet Filter is compatible with PF_RING version 6 (Zero Copy, LibZero or DNA license not needed). PF_RING version 5 is not compatible anymore.