WANGuard Lite 3.1

User Manual

WANGuard Console + WANGuard Sensor

Revision 1.10

Copyright & trademark notices

This edition applies to version 3.1 of the licensed program WANGuard Lite 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. marketing department, sales@andrisoft.com.

Copyright Acknowledgment

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 Lite is a SOFTWARE PRODUCT of ANDRISOFT S.R.L. ANDRISOFT and WANGuard 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.

Str. Lunei L30 Ap. 11, 300109 Timisoara, Timis, Romania
phone: +40721250246; fax: +40256209738

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

Table of Contents

1. Traffic Monitoring and Traffic Accounting with WANGuard™ Lite....4
Why WANGuard™ Lite Is Important....4
What WANGuard™ Lite Can Do For You....4
WANGuard™ Lite Components....4
WANGuard Sensor....5
WANGuard Console....5
2. How To Choose A Method Of Traffic Capturing....7
Supported Traffic Capturing Methods....7
Port Mirroring (Switched Port Analyzer - SPAN, Roving Analysis Port), Network TAP, In-line deployment....7
How Port Mirroring, Network TAP, In-line Deployment works 8
Reasons to choose Port Mirroring, Network TAP, In-line Deployment....8
NetFlow® Monitoring....8
How NetFlow® Monitoring Works....8
Reasons to choose NetFlow® Monitoring 9
Comparison between Packet Sniffing and NetFlow® Monitoring....9
3. Installation....10
System Requirements....10
WANGuard Sensor System Requirements for 1 Gigabit Network Interface....10
WANGuard Console System Requirements for < 5 WANGuard Sensors....11
Download 12
Software Installation....12
4. Network Basics You Should Be Aware Of....13
Who Should Read This Section....13
A Short Introduction To IP Addresses & Classes....13
IP Addresses....13
IP Classes....14
Subnet CIDR Notation....15
5. Getting Started with WANGuard™ Lite....16
Basic Concepts....16
Menu Bar....16
Views....16
Tables....16
IP Zones 17
Opening WANGuard Console for the first time....17
A First Look at the Systems View....18
Managing WANGuard Console Users....18
6. IP Zones Setup....21
Understanding IP Zones....21
Inheritance....21
IP Zone Selection....22
Adding a new IP Zone....22
Changing Description, Copying & Deleting IP Zones....23
IP Zone Configuration....24
Accounting....25
Graphing....25
Description....25
IP Zone Configuration Example....26
7. WANGuard Sensor Setup....28

WANGuard Sniff Configuration........ 28
WANGuard Flow Configuration........ 32
8. Views........37
Systems View........ 37
Active WANGuard Sniff Systems Table........ 38
Active WANGuard Flow Systems Table........39
WANGuard Sensor Live Graphs Tab........ 40
Events Tab........40
Reports View........ 41
WANGuard Sensors Section........ 41
IP Descriptions Section........42
IP Addresses Section........43
9. Traffic Accounting and Graphing........44
IP Traffic Graphs Setup........ 44
IP Traffic Graphs........ 45
By IP Description........ 46
By IP Address / Subnet........47
IP Traffic Accounting........ 47
By IP Description........ 48
By IP Address / Subnet........49
Protocols Distribution Graphs........49
WANGuard Sensor Tops 50
WANGuard Sensor Graphs 51
WANGuard Flow ASN Graphs 52
10. Archive 53
Events Logs........53
Stats Logs........53
11.Help Menu........54
Contextual Help........54
AS Information 54
IP Information........ 54
IP Protocols........ 54
Subnet Calculator........ 54
TCP&UDP Ports........ 54
About........54
12.Appendix 1 – Configuring NetFlow Data Export........55
Configuring NDE on an IOS Device........55
Configuring NDE on a CatOS Device........ 56
Configuring NDE on a Native IOS Device........ 57
Configuring NDE on a 4000 Series Switch........ 57
Configuring NDE on a Juniper Router........ 57

Traffic Monitoring and Traffic Accounting with WANGuard™ Lite

Why WANGuard™ Lite Is Important

Most businesses today rely more and more on network infrastructure. So, the computer network's reliability and speed are crucial for these businesses to be successful, and an efficient use of the available resources must be assured. The significant degradation of the services can seriously damage the businesses including loss of customers and subsequent loss of revenue.

For the network administrator this means that he has to ensure the network's uptime, reliability, speed as well as the efficient use of the existing resources.

Andrisoft WANGuard Lite is an enterprise-grade Linux-based software solution that delivers the functionality NOC and IT teams need to effectively monitor their network through a single, integrated package. The components have been built from the ground up to be high performing, reliable and secure. WANGuard Lite is feature rich, simple to deploy and configure, causing no disruption within the network.

What WANGuard™ Lite Can Do For You

Andrisoft WANGuard Lite is an easy to use software that provides network traffic monitoring and accounting.

It allows you to quickly and easily set up and run monitoring server(s) for networks. Using the integrated web interface, with just a few mouse clicks you can view:

- Historic and real-time network traffic parameters about the data flowing through router interfaces and switch ports (packets/s, bits/s, bytes/s, IPs/s, flows/s etc.)
- MRTG-style traffic graphs and traffic accounting reports for IP addresses and IP classes in your network for any time-frame
- Historic and real-time network traffic statistics (top talkers per protocol, number of IPs, top protocols, protocols distribution, ASN distribution, TCP and UDP ports distribution etc.)

The recorded data is stored in an internal SQL database that can be easily queried and referenced. The recorded monitoring statistics can be viewed through a rich, Ajax-based (Web 2.0) web interface.

WANGuard™ Lite Components

The WANGuard Lite has two main components:

WANGuard Sensor

WANGuard Sensor is an advanced Linux-based software created to do both incoming and outgoing traffic monitoring and accounting. At it's core, WANGuard Sensor has a highly scalable traffic correlation engine capable of continuously monitoring hundreds of thousands of IP addresses. Complex statistical algorithms integrate traffic data to build accurate and detailed picture of real-time and historical traffic flows across the network.

WANGuard Lite does **not** enable WANGuard Sensor's traffic anomaly detection and reaction features.

WANGuard Sensor Features and Benefits:

- Any number of instances can be deployed across the network and all collected data will be centralized and available through a single web interface that you can quickly access from any location
- The supported traffic monitoring methods are: Port Mirroring (Switched Port Analyzer - SPAN, Roving Analysis Port), Network TAP, In-line Deployment, Cisco NetFlow® and Huawei NetStream®
- You can access various real-time parameters (top talkers, number of IP addresses, top protocols, protocols distribution etc.) about the data flowing through router interfaces and switch ports
- Provides on-demand MRTG-style traffic graphs for any IP address or IP class in your network, for any time frame. Traffic graphs accuracy can be defined between 5 seconds and 10 minutes
- WANGuard Sensor is completely scalable and can monitor and generate graphs for hundreds of thousands of IP addresses
- Includes a very flexible billing system for bandwidth based billing
- Easy and non-disruptive installation on common server hardware
- The most cost-effective traffic monitoring and accounting solution on the market

WANGuard Console

WANGuard Console provides a tightly integrated and highly graphical, interactive Ajax-based (Web 2.0) interface for all aspects of network traffic monitoring and accounting. Included in the WANGuard Console is the advanced graphing engine that provides quick and easy ad-hoc graphing functionality. WANGuard Console offers single-point management and reporting by consolidating the data from all WANGuard Sensor systems deployed within the network.

WANGuard Console Features and Benefits:

- Consolidated, real-time WANGuard Sensor management and monitoring using a rich Ajax-based (Web 2.0) web interface
- IP Zones support for segmenting your network by departments, clients, server clusters etc.
- Intuitive desktop applications-like menu system
- Easy to use navigation allows to drill into the live monitoring results
- Graphs are always generated on-the-fly for live reporting. Live traffic graphs are animated
- Integrated contextual help system
- Integrated web-based tools that provide:
    - AS (Autonomous System) information
    - IP information (reverse DNS, domain URL, IP range, AS, ISP, Country, ping, traceroute, whois)
    - IP Protocols information
    - TCP and UDP ports information
    - Subnet calculator
- The recorded data is stored in an internal SQL database that can be easily queried and referenced
- Authenticated access (username/password necessary) for an unlimited number of users with different security profiles

How To Choose A Method Of Traffic Capturing

This section explains the available methods you can use for traffic capturing. Reading this chapter is strongly recommended, as it will help you understand how to deploy WANGuard Sensor.

Supported Traffic Capturing Methods

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

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

Depending on your network configuration, your needs and your hardware, you must choose between the three methods of traffic capturing. For high availability scenarios it's recommended to use in parallel more than one method of traffic capturing.

Please read on to further understand the differences between the supported methods of traffic capturing, and the differences between WANGuard Sniff and WANGuard Flow.

Port Mirroring (Switched Port Analyzer - SPAN, Roving Analysis Port), Network TAP, In-line deployment

In order to do traffic monitoring and accounting, ***WANGuard Sniff*** inspects all network data packets passing the host server's network card, including the network data packets sent by a monitoring port of a switch or router.

How Port Mirroring, Network TAP, In-line Deployment works

It is very important to understand that WANGuard Sniff can only inspect data packets that actually flow through the network interface(s) of the host server. In switched networks, only the traffic for a specific device is sent to the device's network card. If the server running WANGuard Sniff is not deployed in-line, it can't capture the traffic of other network components.

For WANGuard Sniff to analyze the traffic of other hosts in your network you must use a network TAP, or a switch or router that offers a “monitoring port” or “port mirroring” configuration (Switched Port Analyzer - “SPAN” for Cisco devices, Roving Analysis Port for 3Com devices). In this case the network device sends a copy of data packets traveling through a port or VLAN to the monitoring port. After you configure the network device, install WANGuard Sensor on a Linux server and connect it to the monitoring port. WANGuard Sniff will be able to analyze the whole traffic that passes through the selected port or VLAN, with or without VLAN tag stripping.

If you don't have network devices that can do port mirroring, you can deploy a Linux server on the main data-path and WANGuard Sniff will be able to analyze the traffic flows that are routed through the server. Note that the server will become a single point of failure system, if you don't configure VRRP.

Reasons to choose Port Mirroring, Network TAP, In-line Deployment

Packet sniffing comes into consideration if you can provide the higher CPU power needed by WANGuard Sniff. Packet sniffing provides extremely fast and accurate traffic accounting and analysis results.

NetFlow® Monitoring

NetFlow Monitoring is the domain of networks that usually use Cisco or Huawei L3 switch or router flows. These can be configured to send data streams with the network's usage data to a Linux server running ***WANGuard Flow***.

How NetFlow® Monitoring Works

One option to measure bandwidth usage “by IP Address” is to use the NetFlow protocol which is especially suited for high traffic, remote networks. Many routers and Layer 3 switches from Cisco support this protocol, as well as vendors like Huawei (NetStream), Juniper, Extreme Networks, 3COM and others.

Network devices with NetFlow support, track the bandwidth usage of the network internally, and can be configured to send pre-aggregated data to a Linux server running WANGuard Flow for traffic analysis and accounting purposes.

Reasons to choose NetFlow® Monitoring

Because the NetFlow protocol already performs a pre-aggregation of traffic data, the flows of data sent to the monitoring server running WANGuard Flow is much smaller than the monitored traffic. This makes NetFlow the ideal option for monitoring remote, high-traffic networks.

The downside of the NetFlow monitoring is that computing the pre-aggregation of traffic data requires large amounts of RAM, it has significant delays, and the accuracy of traffic parameters is lower than when directly inspecting network packets, especially when flow/packet sampling is used.

Comparison between Packet Sniffing and NetFlow® Monitoring

The table below provides a quick comparison between the three available traffic capturing technologies. The hardware requirements for each method are different. The requirements are listed in the next chapter.

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

* Manufacturer devices supporting WANGuard Flow are: Cisco Systems (1400, 1600, 1700, 2500/2600, 3600, 4500/4700, AS5300/5800, 7200/7500, Catalyst 4500, Catalyst 5000/6500/7600, ESR 10000,GSR 12000), Juniper, Extreme Networks, Huawei, 3COM and others.

Installation

WANGuard Lite can be installed on common server hardware, provided that the system requirements listed later in this chapter are met. If you have some basic Linux operation skills then no training is required for the software installation. Feel free to contact our support team for any issues.

Installing WANGuard Lite does not generate any negative side effects on your network's performance. Installation and configuration may take less than an hour; after that your network will be monitored immediately. No baseline data gathering is required.

System Requirements

WANGuard Lite 3.1 has been tested with the following Linux distributions: **Red Hat Enterprise Linux 5.0 (** commercial Linux distribution), **CentOS 4.0, 5.0, 5.1, 5.2** (free, Red Hat Enterprise Linux based distribution), **OpenSuSE 10.3 (** free, Novel Enterprise Linux based distribution), **Debian Linux 4.0** (free, community supported distribution). Other distributions should work but haven't been tested yet.

The WANGuard Lite architecture is completely **scalable**. By installing the software on better hardware, the number of monitored endpoints and networks increases. All WANGuard Lite components can be installed on a single server if enough resources are provided (RAM, CPU, Disk Space, Network Cards). You can also install the components on multiple servers distributed across your network.

WANGuard Sensor System Requirements for 1 Gigabit Network Interface

	WANGuard Sensor	
	WANGuard Sniff 3.1	**WANGuard Flow 3.1**
Architecture	x86 (32 or 64 bit)	x86 (32 or 64 bit)
CPU	1 x Pentium IV 2.0 GHz	1 x Pentium IV 1.6 GHz
Memory	500 MBytes	2 GBytes
Network Cards	1 x Gigabit Ethernet (with NAPI support) 1 x Fast Ethernet	1 x Fast Ethernet
Operating System	Linux 2.6.x kernel	Linux 2.6.x kernel
Installed Packages	tcpdump WANGuard-Sensor 3.1 WANGuard-Controller 3.1	WANGuard-Sensor 3.1 WANGuard-Controller 3.1
Disk Space	5 GB (including OS)	5 GB (including OS)

When using WANGuard Flow, network devices must be configured to send NetFlow® version 5 data packets to the the server. For detailed instructions on how to enable NetFlow on your network devices please consult the vendor's website. Some examples are included in Appendix 1 – Configuring NetFlow Data Export (page 55).

When using WANGuard Sniff, you must know that by default, only data packets passing the local machine's network card can be analyzed. Either you deploy the WANGuard Sniff server in-line, or for network-wide monitoring in switched networks the use of switches or routers with so-called “monitoring port” is required. For configuring Cisco switches please consult Catalyst Switched Port Analyzer (SPAN) Configuration Example on http://www.cisco.com/warp/public/473/41.html. To configure TAP's or other devices that support port mirroring please consult the producer's documentation.

WANGuard Console System Requirements for < 5 WANGuard Sensors

Architecture	x86 (32 or 64 bit)
CPU	1 x Pentium IV 2.4 GHz
Memory	500 MBytes
Network Cards	1 x Fast Ethernet or Gigabit Ethernet
Operating System	Linux kernel 2.6.x
Installed Packages	apache 2.x php 5 mysql 5.x rrdtool 1.2.x perl 5.x perl-rrdtool perl-MailTools perl-DBD-MySQL ping, whois, traceroute, telnet WANGuard-Console 3.1 WANGuard-Controller 3.1
Disk Space	5GB (including OS) + additional storage when storing IP graphs data

To access the web interface provided by WANGuard Console, one of the following web browsers is required (other should also work but have not been tested): Firefox 2.0 or later, Internet Explorer 6.0 or later, Apple Safari 3.0 or later, Konqueror 3.5 or later, Opera 8.0 or later.

The web browser must javascript and cookies support activated. Java support is not required. To access the Contextual Help please install Adobe PDF Reader.

For the best WANGuard Console experience we highly recommend the Firefox 3 browser, and a 1280x1024 pixels or higher resolution monitor.

Download

All WANGuard Lite components can be downloaded directly from the Andrisoft website:

http://www.andrisoft.com/download/rpm for RedHat-based Linux distributions packages

http://www.andrisoft.com/download/suse for SuSE-based Linux distributions packages

http://www.andrisoft.com/download/deb for Debian-based Linux distributions packages.

You may a try a fully functional version of WANGuard Lite for 30 days. You can switch to a full-time, registered version by applying a purchased license key.

Binary WANGuard Lite components are packaged differently for i686 architectures (32 bit Pentium and beyond) and for x86_64 architectures (64 bit Intel / AMD processors).

Software Installation

Software installation instructions are listed and updated on the Andrisoft website, under the download links:

http://www.andrisoft.com/download/rpm#installation for RedHat-based Linux distributions

http://www.andrisoft.com/download/suse#installation for SuSE-based Linux distributions

http://www.andrisoft.com/download/deb#installation for Debian-based Linux distributions.

Network Basics You Should Be Aware Of

Who Should Read This Section

If you are new to network administration and network monitoring, read about the technical basics in this section! It will help you understand how WANGuard Lite works! If you are already used to IP addresses and IP classes you can skip this section.

A Short Introduction To IP Addresses & Classes

IP Addresses

In order for systems to locate each other in a distributed environment, nodes are given explicit addresses that uniquely identify the particular network the system is on and uniquely identify the system to that particular network. When these two identifiers are combined, the result is a globally-unique address. This address, known as “IP address”, as “IP number”, or merely as “IP” is a code made up of numbers separated by three dots that identifies a particular computer on the Internet. These addresses are actually 32-bit binary numbers, consisting of the two sub addresses (identifiers) mentioned above which, respectively, identify the network and the host to the network, with an imaginary boundary separating the two.

An IP address is, as such, generally shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.

For example, the address 168.212.226.204 represents the 32-bit binary number 10101000.11010100.11100010.11001100.

The binary number is important because that will determine which class of network the IP address belongs to. The Class of the address determines which part belongs to the network address and which part belongs to the node address (see IP address Classes further on).

The location of the boundary between the network and host portions of an IP address is determined through the use of a subnet mask. This is another 32-bit binary number which acts like a filter when it is applied to the 32-bit IP address. By comparing a subnet mask with an IP address, systems can determine which portion of the IP address relates to the network and which portion relates to the host. Anywhere the subnet mask has a bit set to “1”, the underlying bit in the IP address is part of the network address. Anywhere the subnet mask is set to “0”, the related bit in the IP address is part of the host address. The size of a network is a function of the number of bits used to identify the host portion of the address. If a subnet mask shows that 8 bits are used for the host portion of the address block, a maximum of 256 host addresses are available for that specific network. If a subnet mask shows that 16 bits are used for the host portion of the address block, a maximum of 65,536 possible host addresses are available for use on that network.

An Internet Service Provider (ISP) will generally assign either a static IP address (always the same) or a dynamic address (changes every time one logs on). ISPs and organizations usually apply to the InterNIC for a range of IP addresses so that all clients have similar addresses. There are about 4.3 billion IP addresses. The class-based, legacy addressing scheme places heavy restrictions on the distribution of these addresses. TCP/IP networks are inherently router-based, and it takes much less overhead to keep track of a few networks than millions of them.

IP Classes

Class A addresses always have the first bit of their IP addresses set to “0”. Since Class A networks have an 8-bit network mask, the use of a leading zero leaves only 7 bits for the network portion of the address, allowing for a maximum of 128 possible network numbers, ranging from 0.0.0.0 – 127.0.0.0. Number 127.x.x.x is reserved for loopback, used for internal testing on the local machine.

Class B addresses always have the first bit set to “1” and their second bit set to “0”. Since Class B addresses have a 16-bit network mask, the use of a leading “10” bit-pattern leaves 14 bits for the network portion of the address, allowing for a maximum of 16,384 networks, ranging from 128.0.0.0 – 181.255.0.0.

Class C addresses have their first two bits set to “1” and their third bit set to “0”. Since Class C addresses have a 24-bit network mask, this leaves 21 bits for the network portion of the address, allowing for a maximum of 2,097,152 network addresses, ranging from 192.0.0.0 – 223.255.255.0.

Class D addresses are used for multicasting applications. Class D addresses have their first three bits set to “1” and their fourth bit set to “0”. Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group’s IP address for receiver purposes.

Class E addresses are defined as experimental and are reserved for future testing purposes. They have never been documented or utilized in a standard way.

The WANGuard Lite uses extensively, throughout its components, IP Addresses and IP Classes with the CIDR notation.

Subnet CIDR Notation

CIDR	Class	Hosts	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

Getting Started with WANGuard™ Lite

Please read the following “Basic Concepts” section in order to get a clear overview of the basic premises required for the proper operation of the software.

Basic Concepts

To understand the concepts of WANGuard Lite please be aware of following phrases:

Menu Bar

Every browser window has on top, a fixed drop-down menu bar used for navigation throughout the WANGuard Console. The Menu Bar contains drop-down menus similar with the ones used in common desktop applications.

Views

WANGuard Console offers various ways to look at live collected data. We call these “Views”. You can switch between them by selecting the Views menu from the Menu Bar. There are two different types of Views available in the Lite version:

- **Systems View**
  Displays a table with live information about all running WANGuard Sensor systems. On the bottom section it displays tabbed live traffic graphs and events.
- **Reports View**

  Displays graphs and reports that contain traffic parameters collected from monitored network links, IP classes and IP Zones. Includes a live, top like network traffic visualizer supporting multiple protocols such as IPv4, TCP (+syn), UDP, ICMP as well as TCP and UDP ports and AS Numbers.

More information about Views is available on the Views chapter (page 37).

Tables

All WANGuard Lite modules store traffic and operational details in a MySQL database. The contents of the database is presented in WANGuard Console in form of tables with an unified look-and-feel.

Records can be queried using the top-left <Search> button. Sorting can be done by clicking the column name. By default, the records are sorted by the insertion time with the latest records being displayed first.

To prevent clutter and high loading times, the records are listed on multiple pages. You can navigate through the pages with the bottom navigation buttons.

The first column on every record is populated with icons that engage actions such as viewing details about the record, changing the record and deleting the record. Users with *Normal User* privileges can only view details about records. Users with *Administrator* privileges can view, change and delete records.

IP Zones

IP Zones are hierarchical, tree-like structures that contain user provided details about your network elements and segments. Each WANGuard Sensor uses an IP Zone from which it extracts information such as: what IP classes must be monitored, what IP classes should generate traffic graphs and accounting data, IP classes descriptions.

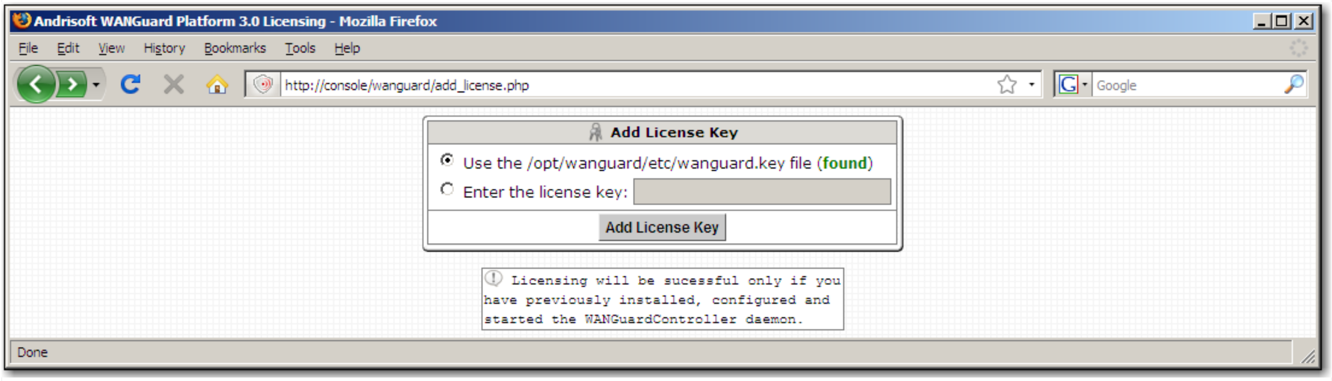
The same IP Zone may be used by different WANGuard Sensor systems.

Opening WANGuard Console for the first time

WANGuard Console is essentially the web interface through which you will control and monitor all other components. If you followed correctly the installation instructions, from now on you will only need to log into WANGuard Console to manage the components.

To log into WANGuard Console, use a compatible web browser (listed at page 11) and access http://<hostname>/wanguard (where <hostname> is the name of the server where WANGuard Console is installed). 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.

If you haven't licensed WANGuard Lite yet, you will be asked to do so:



http://console/wanguard/add_license.php

● Use the /opt/wanguard/etc/wanguard.key file (found)

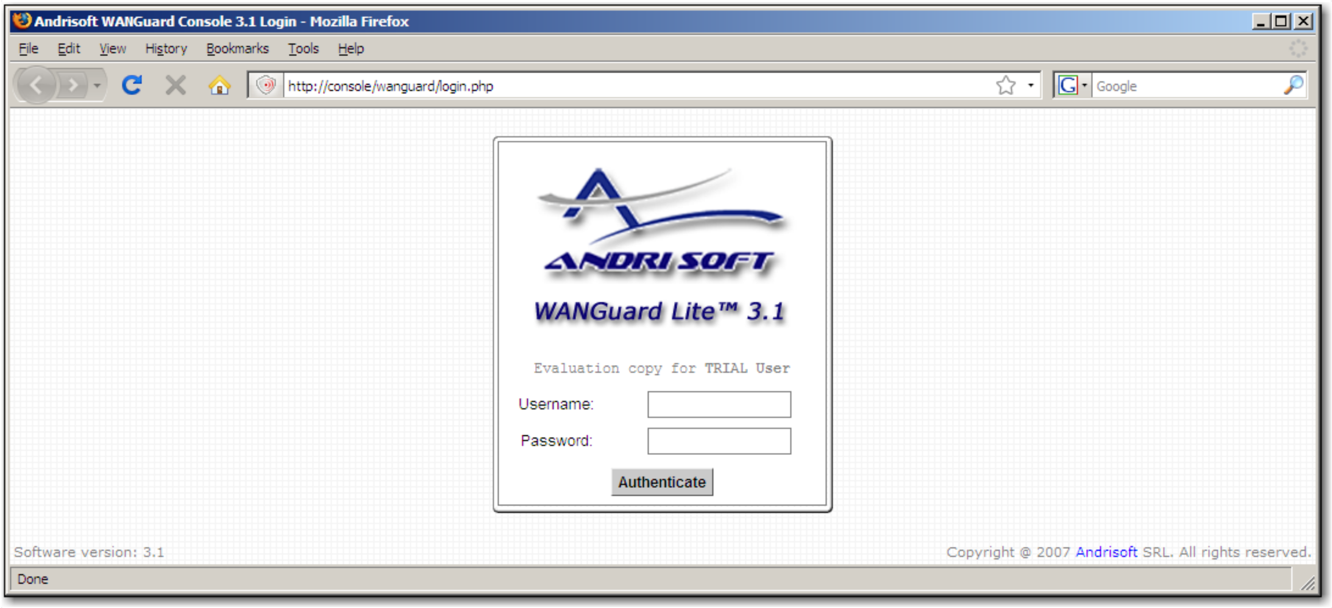
○ Enter the license key:

Licensing will be sucessful only if you have previously installed, configured and started the WANGuardController daemon.

You can add a license key by two methods. You can either copy the *wanguard.key* file we sent you by email in */opt/wanguard/etc*, or you can paste directly the file's content in the input field.

The license key contains encrypted information about the licensed capabilities of the software. You can upgrade to the Full version (incl. traffic anomalies detection & protection) or downgrade to the Lite version (without traffic anomalies detection & protection) solely by changing the license key.

Log into WANGuard Console using the default username / password combination of **admin** / **wanguard**.


Andrisoft WANGuard Console 3.1 Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://console/wanguard/login.php
Google
ANDRI SOFT
WANGuard Lite™ 3.1
Username:
Password:
Authenticate
Done

Evaluation copy for TRIAL User

Software version: 3.1

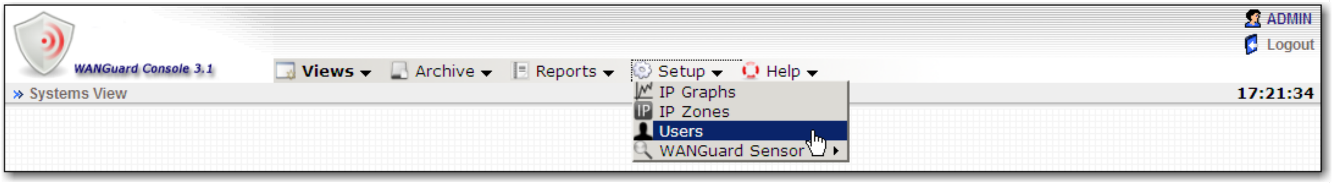
Copyright @ 2007 Andrisoft SRL. All rights reserved.

A First Look at the Systems View

Immediately after logging into WANGuard Console, the layout of the Systems View will be displayed. You can change the default View by editing your User preferences.

Because no WANGuard Sensor system was previously configured and enabled and no data was gathered, the Systems View will be mostly empty. More information about Views can be found in the Views chapter (Page 37). You can navigate throughout WANGuard Console using the drop-down menu located in the upper side of every page.

Managing WANGuard Console Users

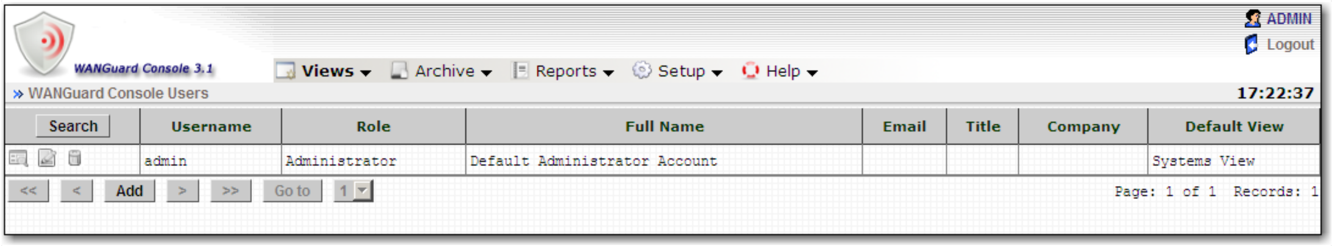


If you install WANGuard Console on a publicly available server, you should immediately change the default password for the **admin** user, and eventually add new users. To manage WANGuard Console users you must select Users from the Setup menu. A list of existing users will be displayed.

To **view** additional information about a user you must click the first icon in the first column.

To **change** user passwords or to edit user details you must click the second icon in the first column.

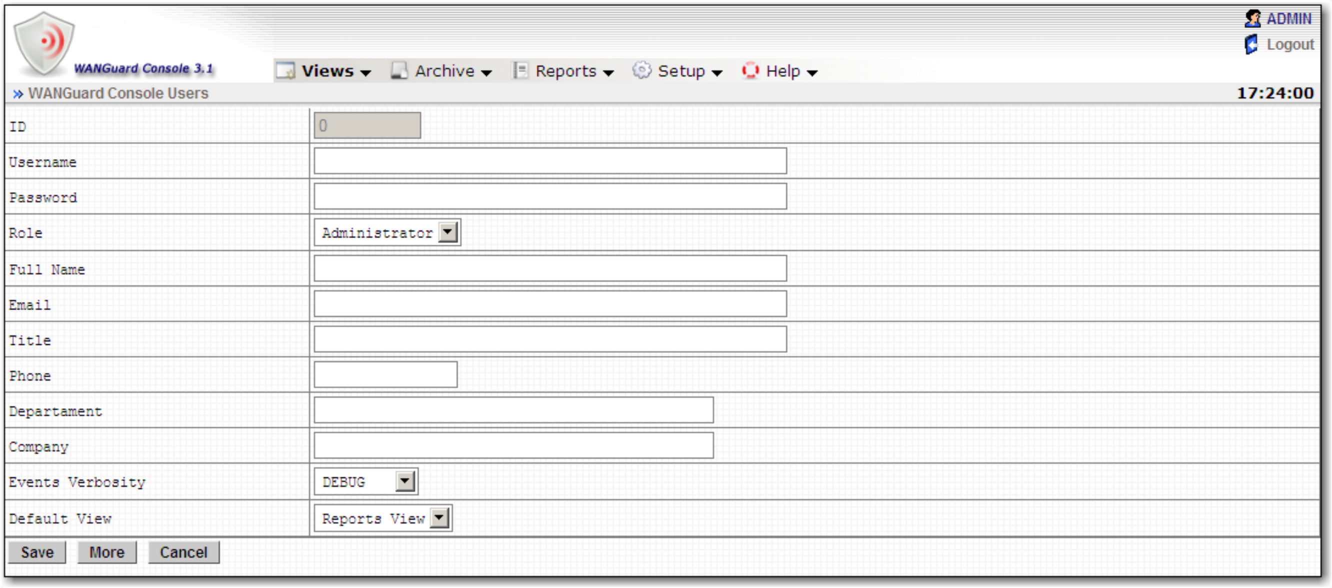
To **delete** a user you must click the third icon in the first column.



Search	Username	Role	Full Name	Email	Title	Company	Default View
	admin	Administrator	Default Administrator Account				Systems View

Page: 1 of 1 Records: 1

To **add** a new user click the <Add> button. Fill the following fields and click the <Save> button to add the new user.



ID	0
Username	
Password	
Role	Administrator
Full Name	
Email	
Title	
Phone	
Departament	
Company	
Events Verbosity	DEBUG
Default View	Reports View

The **Username** and **Password** fields are mandatory. Enter unique names for users.

Currently there are two available access levels (**Roles**) for users:

- *Normal User* - The user can access all Views, generate traffic accounting and traffic graphs reports, read event logs and archives, but cannot view or manage WANGuard Sensor configurations nor can it add or delete users.

- *Administrator* - The user has all privileges to view and manage WANGuard Lite components, including adding new users and changing users passwords (existing users passwords are always shown encrypted).

The **Full Name**, **Email**, **Title**, **Phone**, **Department** and **Company** fields are optional.

The **Events Verbosity** field lets you select the minimum severity level of the events that will be displayed in the Systems View:

- *MELTDOWN* - Meltdown events are generated when a very serious error is detected in the system such as a hardware error.
- *CRITICAL* - Critical events are generated when a significant software error is detected such as a memory exhaustion.
- *ERROR* - Error events are caused by misconfiguration or communication errors between WANGuard Lite components.
- *WARNING* - Warning events are generated when authentication errors occur, when there are errors updating graph data files and when there are synchronization issues.
- *INFO* - Informational events are generated when configurations are changed and when users log into WANGuard Console.
- *DEBUG* - Debug events are used only for troubleshooting purposes.

The **Default View** field lets you select what View will be displayed immediately after logging into WANGuard Console:

- *Systems View* - recommended for systems administrators.
- *Reports View* - recommended for network administrators.

IP Zones Setup

This chapter describes how to create, manage and understand IP Zones.

Understanding IP Zones

IP Zones are hierarchical, tree-like structures that contain user provided information about any combination of the following elements:

- a network server, client or router
- a network link, subnet, or an entire network
- an individual Internet user or company
- an Internet Service Provider (ISP)

Each WANGuard Sensor extracts from IP Zones the following information:

- the IP classes that will be monitored
- the IP classes that will generate traffic graphs and accounting data
- IP classes descriptions

When configuring a WANGuard Sensor (Page 28) you have to select the IP Zone that will be used. An IP Zone may be used by multiple WANGuard Sensor systems, but a WANGuard Sensor system can use only one IP Zone.

An IP Zone must contain the IP classes that are routed within your Autonomous System or the IP classes owned by your organization. If you don't populate the IP Zone with your IP classes, then WANGuard Sniff can only validate the traffic it captures by analyzing the MAC address of the upstream or downstream router. If you don't populate the IP Zone with your IP classes, then WANGuard Flow can only validate the traffic it captures by analyzing the ASN or the interface type.

Keep in mind that WANGuard Lite defines IP classes (subnets) using the CIDR notation. To enter individual hosts in IP Zones you must use the /32 CIDR. For more about CIDR notation you can consult Chapter 4 - Network Basics You Should Be Aware Of (Page 13).

Inheritance

One very special IP class that is defined by default in every IP Zone is the 0.0.0.0/0 IP class. The 0.0.0.0/0 “supernet” contains all private and public IP addresses available for IPv4.

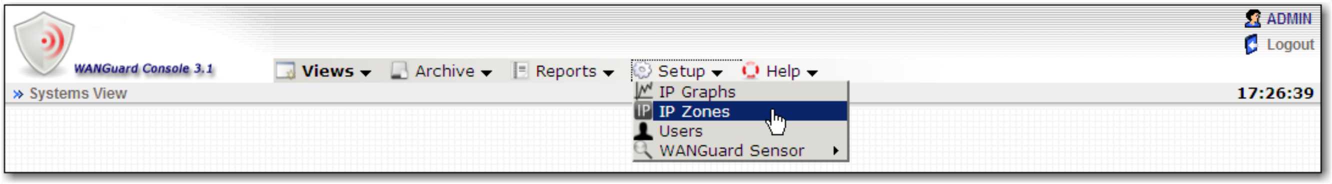
To ease the configuration of IP Zones, every new IP class that you define, inherits by default the properties of the closest (having the biggest CIDR) IP class that includes it. The only IP class that does not inherit any properties is the 0.0.0.0/0 IP class, because there is no other IP class that includes it.

WANGuard Sensor must learn from it's IP Zone the properties of the IP addresses it analyzes. This is why, if WANGuard Sensor cannot include a detected IP address in the IP classes you defined, it applies the properties of the 0.0.0.0/0 IP class. So, for unknown IP addresses, the 0.0.0.0/0 properties are applied.

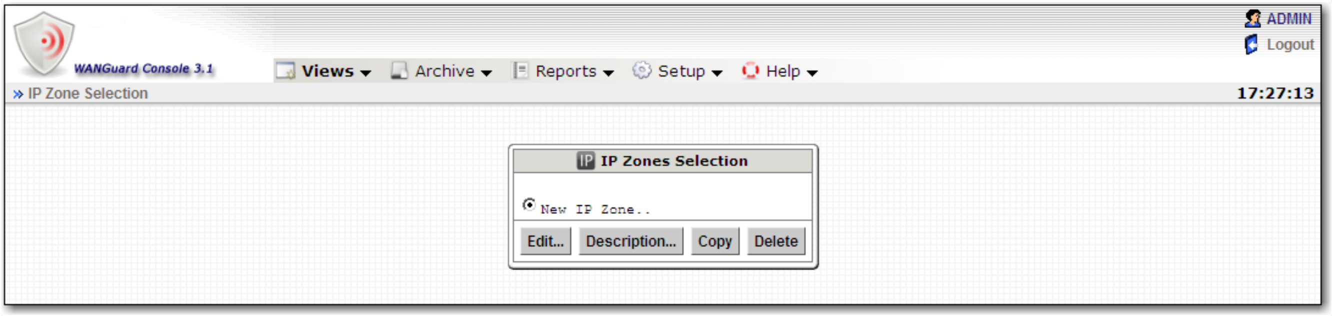
In the last section of this chapter you can see an example on how inheritance works.

IP Zone Selection

To manage IP Zones you must first select IP Zones from Setup menu. You will enter the IP Zones Selection window.

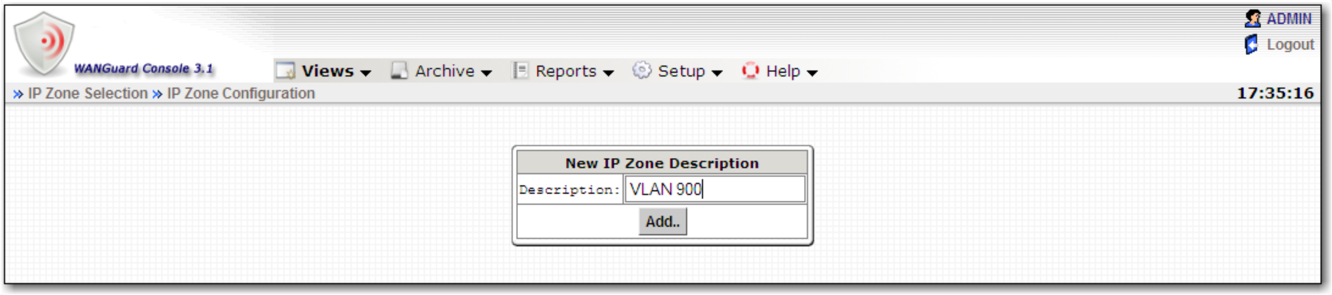


The IP Zones Selection window lets you select existing IP Zones to edit, change description, copy or delete. If no IP Zones were previously added, then the form will only have the option to add a new IP Zone.



Adding a new IP Zone

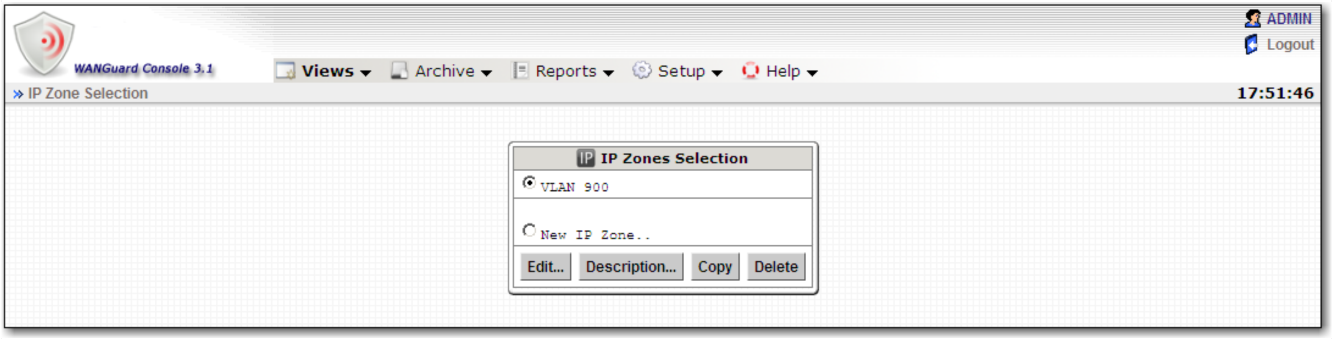
To add a new IP Zone you must select the New IP Zone from the IP Zone Selection form, and then click <Edit...>. Then, you will be asked to enter a generic description that will help you identify the new IP Zone.



Description: VLAN 900

Changing Description, Copying & Deleting IP Zones

Adding a new IP Zone will update the IP Zones Selection window.



● VLAN 900

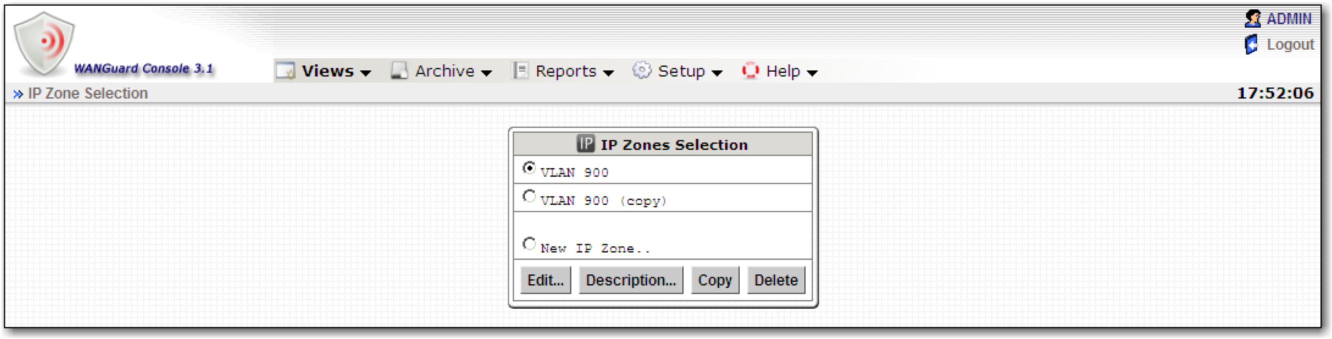
○ New IP Zone..

You can **configure** the selected IP Zone by clicking the <Edit...> button.

To **change the description** of the selected IP Zone you must click the <Description...> button and then provide a different description.

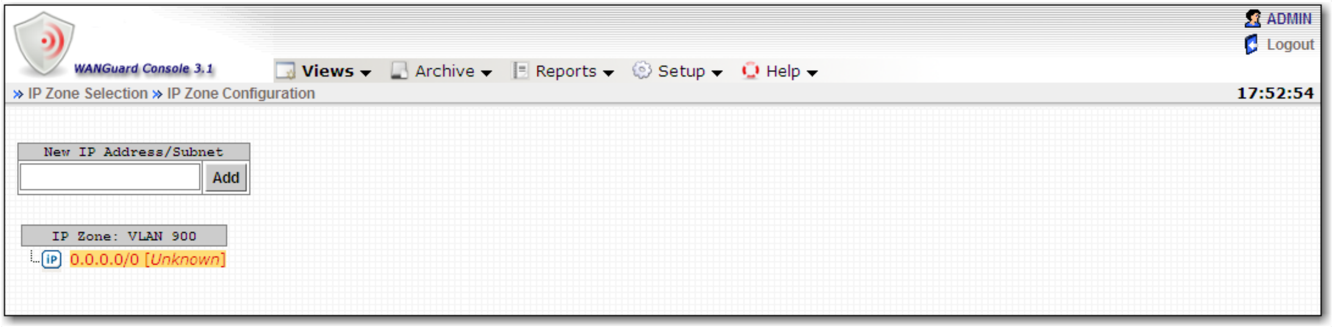
To **copy** the selected IP Zone you must click the <Copy> button. A new IP Zone will be created that will have the same information and the same description with the word “(copy)” attached. In some cases when you have multiple WANGuard Sensor systems, you may have to create multiple IP Zones that share the same IP classes. Instead of recreating the same IP classes for each new IP Zone you can copy an existing IP Zone and modify only the IP classes parameters.

To **delete** the selected IP Zone you must click the <Delete> button and then confirm the deletion.



IP Zone Configuration

After a new IP Zone is added, the IP Zone Configuration window will look like in the image below.

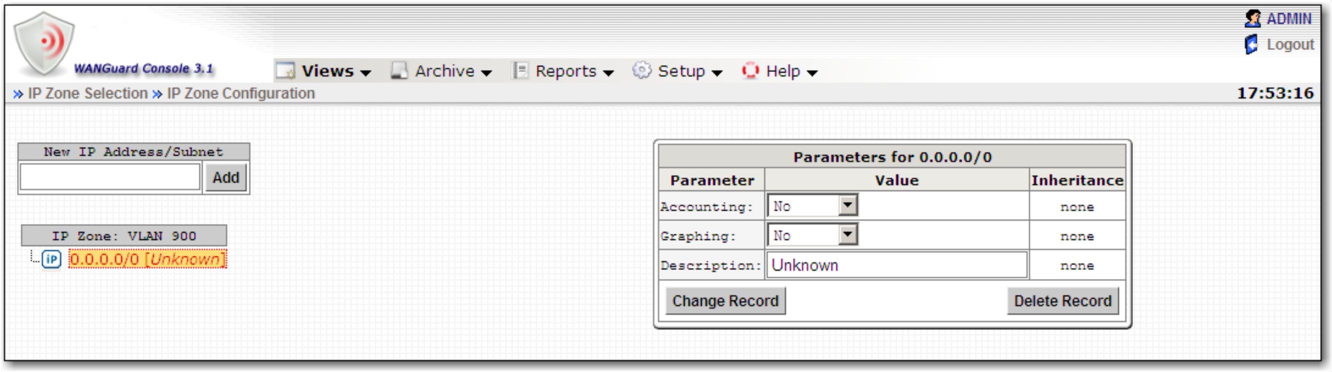


The IP Zone configuration window is divided in two sections, one on the left and one on the right.

In the upper side of the left section you will see a form that is used to add IP addresses / classes to the IP Zone. Below you will see the name of the current IP Zone and the allocated IP classes tree. When adding a new IP class, the tree is automatically updated.

In the right section you will see detailed information about the selected IP class or IP address. The right section will be empty if there is no IP class or IP address selected.

As explained in the Understanding IP Zones: Inheritance section, every IP Zone contains the 0.0.0.0/0 “supernet”. To edit the 0.0.0.0/0 IP class properties click 0.0.0.0/0 from the IP classes tree.



New IP Address/Subnet

IP Zone: VLAN 900

0.0.0.0/0 [Unknown]

Parameters for 0.0.0.0/0

Parameter	Value	Inheritance
Accounting:	No	none
Graphing:	No	none
Description:	Unknown	none

The right section will be populated with properties that apply to all IP addresses included in the selected IP class, if the properties are not subsequently overwritten. The Inheritance column shows from which parent IP class was the value inherited from. Every IP class has the following properties:

Accounting

If the Accounting parameter is set to “Yes” then WANGuard Sensor records traffic accounting data for every IP address included in the selected IP class. Accounting data contains the number of inbound and outbound packets and bits, and averages of packets and bits rates. If the Accounting parameter is set to “Inherit” then the value is inherited from the parent IP class. If the parameter is set to “No” then no accounting data is recorded.

Graphing

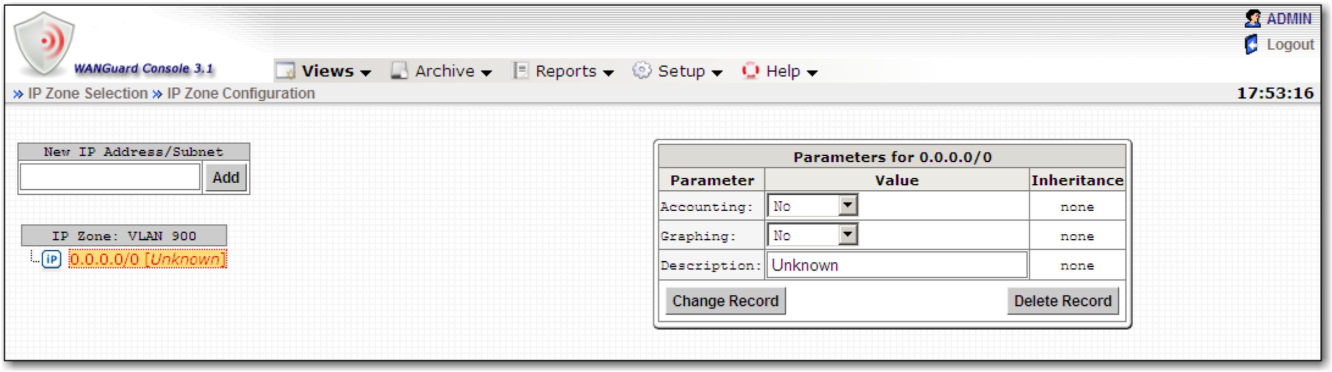
If the Graphing parameter is set to “Yes” then WANGuard Sensor records graphing data for every IP address included in the selected IP class. Graphing data contains accurate information about inbound and outbound packets/second and bits/second rates. If the Graphing parameter is set to “Inherit” then the value is inherited from the parent IP class. If the Graphing parameter is set to “No” then no graphs will be generated for the current IP class.

Description

This parameter should contain a short description for the selected IP class or IP address. If the description field is empty then the description is inherited from the parent IP class.

IP Zone Configuration Example

In the following images you will see how IP Zone inheritance works and how you can define the monitored IP classes.

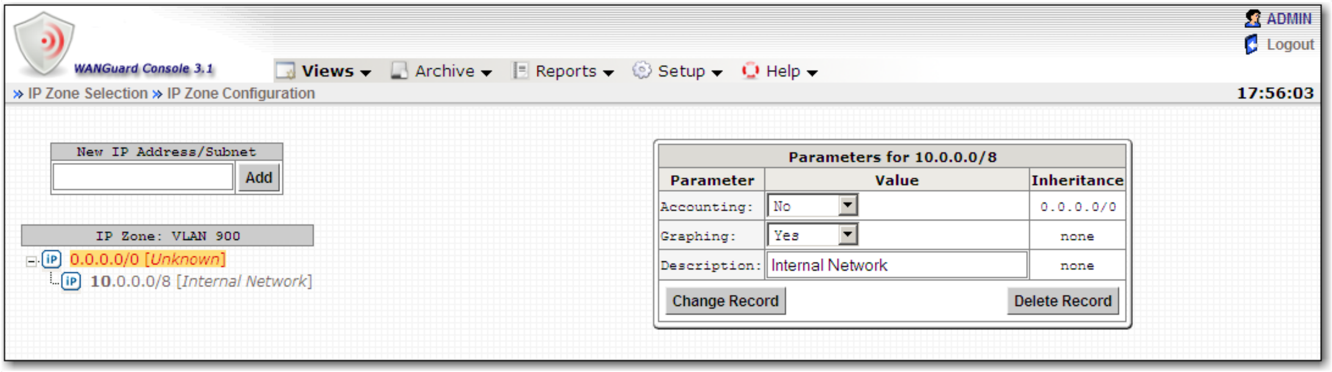


New IP Address/Subnet

IP Zone: VLAN 900
- 0.0.0.0/0 *[Unknown]*

Parameters for 0.0.0.0/0		
Parameter	Value	Inheritance
Accounting:	No	none
Graphing:	No	none
Description:	Unknown	none

By default, the 0.0.0.0/0 “supernet” has *Accounting* and *Graphing* parameters set to “No”. We don't recommend to generate traffic parameters for unknown IP addresses.



New IP Address/Subnet

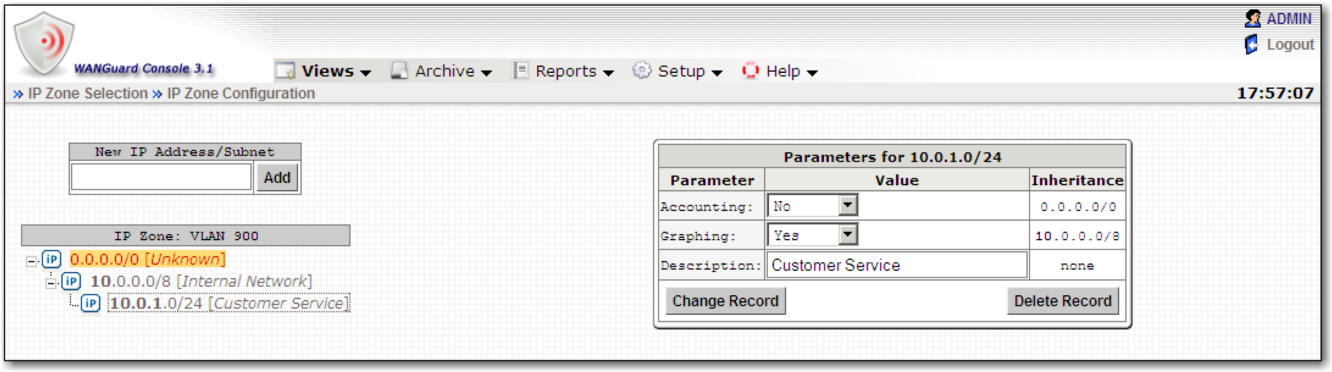
IP Zone: VLAN 900
- 0.0.0.0/0 *[Unknown]*
  - 10.0.0.0/8 *[Internal Network]*

Parameters for 10.0.0.0/8		
Parameter	Value	Inheritance
Accounting:	No	0.0.0.0/0
Graphing:	Yes	none
Description:	Internal Network	none

After adding the 10.0.0.0/8 IP class using the top-left form, the tree is immediately updated to contain the new IP class. The Inheritance column shows what are the inherited values, and from which parent IP class.

In the image above you can see that the *Accounting* value is inherited from 0.0.0.0/0 because it is the only unmodified parameter. Every IP that belongs to the “Internal Network” will generate traffic graphs because the *Graphing* parameter is set to “Yes”.

In the next image a new IP class named “Customer Service” was added. Because this IP class is included in the “Internal Network” it is displayed under it. All parameters except the *Description* were not modified, so the values are inherited from the direct parent IP class.

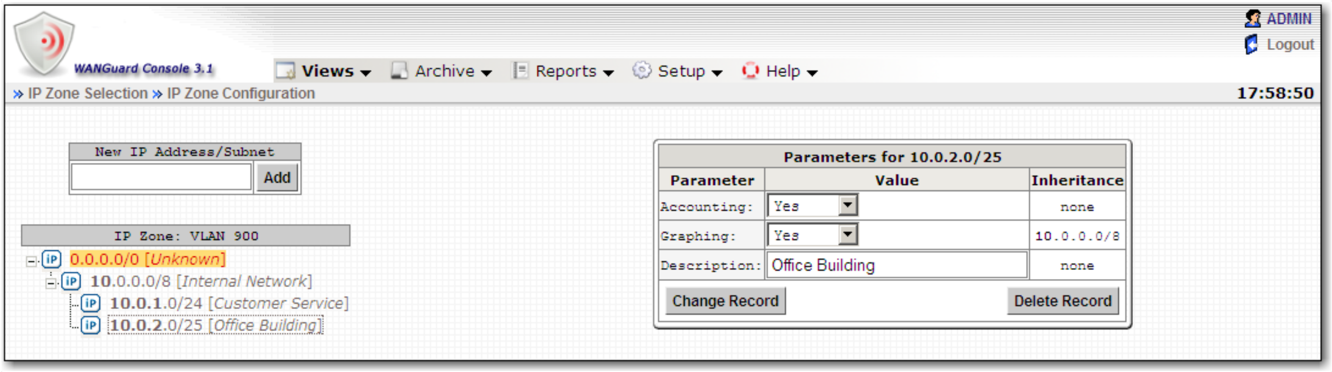


IP Zone: VLAN 900

- 0.0.0.0/0 [*Unknown*]
  - 10.0.0.0/8 [*Internal Network*]
    - 10.0.1.0/24 [*Customer Service*]

Parameters for 10.0.1.0/24		
Parameter	**Value**	**Inheritance**
Accounting:	No	0.0.0.0/0
Graphing:	Yes	10.0.0.0/8
Description:	Customer Service	none

In the image below you can see that a new IP class called “Office Building” was added. Because the *Accounting* parameter was modified to “Yes”, every IP address included in 10.0.2.0/25 will generate accounting data.

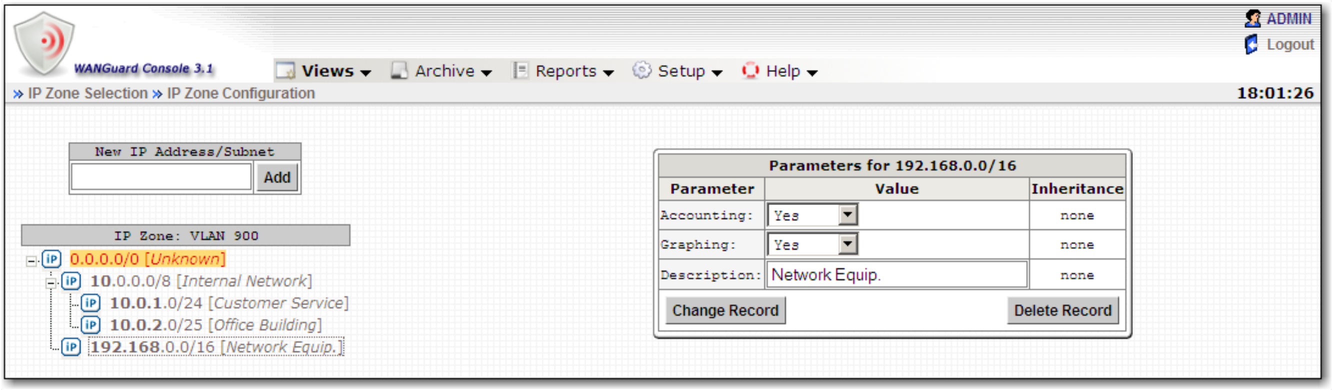


IP Zone: VLAN 900

- 0.0.0.0/0 [*Unknown*]
  - 10.0.0.0/8 [*Internal Network*]
    - 10.0.1.0/24 [*Customer Service*]
    - 10.0.2.0/25 [*Office Building*]

Parameters for 10.0.2.0/25		
Parameter	**Value**	**Inheritance**
Accounting:	Yes	none
Graphing:	Yes	10.0.0.0/8
Description:	Office Building	none

In the image below you can see that 192.168.0.0/16 IP class was added and placed automatically within the 0.0.0.0/0 IP class. WANGuard Sensor will generate traffic graphs and will record accounting data for all IPs that belong to this IP class.



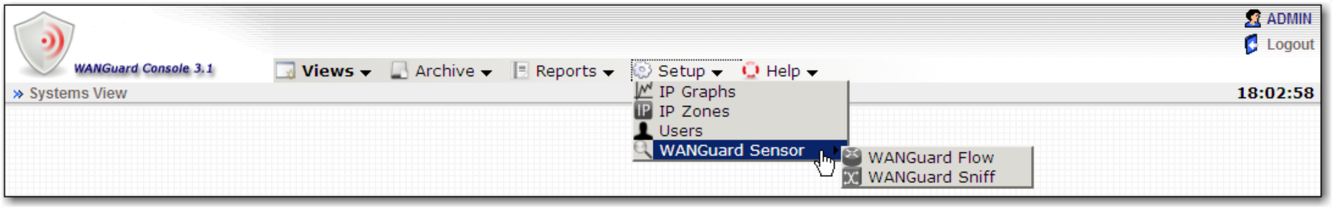
IP Zone: VLAN 900

- 0.0.0.0/0 [*Unknown*]
  - 10.0.0.0/8 [*Internal Network*]
    - 10.0.1.0/24 [*Customer Service*]
    - 10.0.2.0/25 [*Office Building*]
  - 192.168.0.0/16 [*Network Equip.*]

Parameters for 192.168.0.0/16		
Parameter	**Value**	**Inheritance**
Accounting:	Yes	none
Graphing:	Yes	none
Description:	Network Equip.	none

WANGuard Sensor Setup

This chapter describes how to add, configure and delete WANGuard Sensor systems through WANGuard Console. To manage WANGuard Sensor systems you must first select the WANGuard Sensor type from the Setup menu. Keep in mind that our support team can help you with any configuration issues.

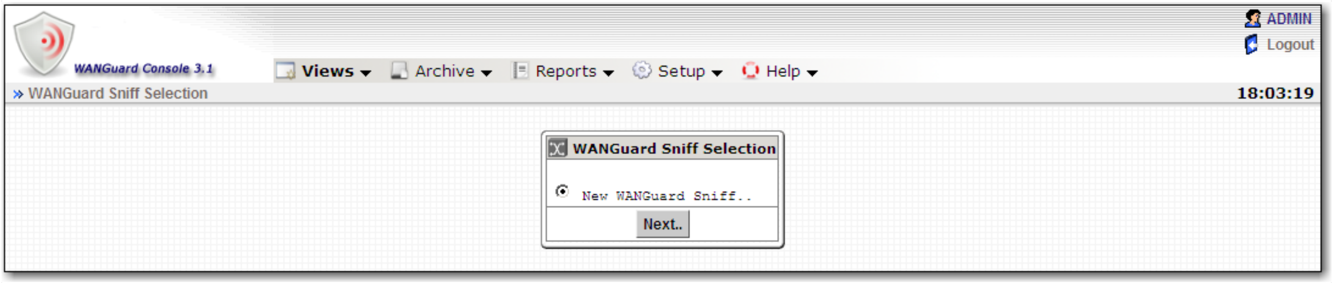


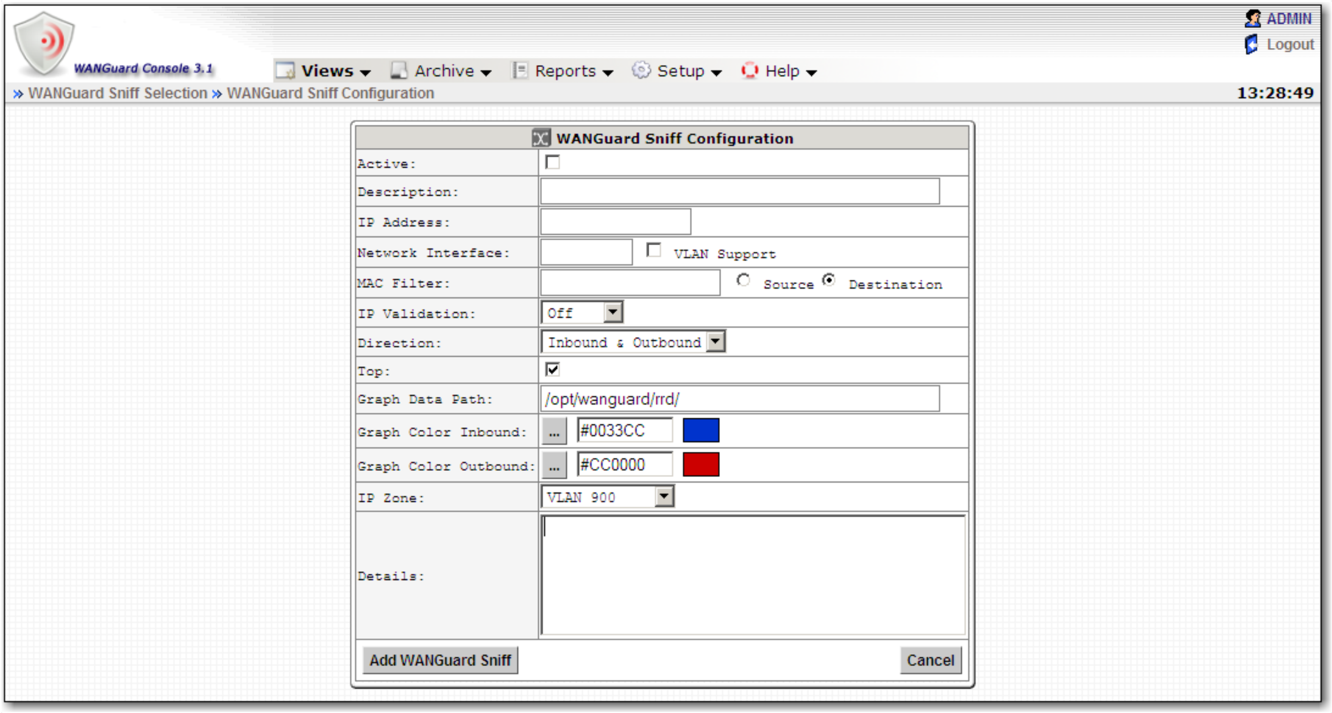
To learn more about the differences between the two types of WANGuard Sensor please consult Chapter 2 - How To Choose A Method Of Traffic Capturing (Page 7).

WANGuard Sniff Configuration

When using WANGuard Sniff, you must know that by default, only data packets passing the local machine's network card can be analyzed. Either you deploy the WANGuard Sniff server in-line, or for network-wide monitoring in switched networks the use of switches or routers with so-called “monitoring port” is required. For configuring Cisco switches please consult Catalyst Switched Port Analyzer (SPAN) Configuration Example on http://www.cisco.com/warp/public/473/41.html. To configure TAPs or other devices that support port mirroring, please consult the producer's documentation.

The WANGuard Sniff Selection window lets you select which WANGuard Sniff system you wish to edit or delete. To add a new WANGuard Sniff system select New WANGuard Sniff and then click <Next..>. If no WANGuard Sniff system was previously configured then the WANGuard Sniff Selection form will have only the option to add a new WANGuard Sniff system.





WANGuard Sniff Configuration

Active:	□
Description:	
IP Address:	
Network Interface:	□ VLAN Support
MAC Filter:	○ Source ● Destination
IP Validation:	Off
Direction:	Inbound & Outbound
Top:	☑
Graph Data Path:	/opt/wanguard/rrd/
Graph Color Inbound:	... #0033CC 🟦
Graph Color Outbound:	... #CC0000 🟥
IP Zone:	VLAN 900
Details:	

Add WANGuard Sniff | Cancel

The WANGuard Sniff Configuration window contains the following fields:

- **Active**

  WANGuard Sniff is automatically activated by the *WANGuardController* daemon if the Active checkbox is checked. If the Active checkbox is unchecked and the WANGuard Sniff system is running then the *WANGuardController* daemon stops it.

- **Description**

  A short, generic description that helps you identify the WANGuard Sniff system.

- **IP Address**

  A unique IP address configured on the server that must run the selected WANGuard Sniff. This field is used by the *WANGuardController* daemon for system identification.

- **Network Interface**

  This field must contain the network interface that receives the port mirrored traffic. If the WANGuard Sniff server is deployed in-line then it must contain the network interface that receives the traffic towards your network.

  If the traffic is tagged with a VLAN header and you check **VLAN Support** then the VLAN header will be ignored. If you want to split the traffic by VLANs then you must create a virtual network interface for each VLAN using the *vconfig* command and then add a WANGuard Sniff for each new virtual interface.

The network interface name must use the network interface naming conventions of the Linux operating system: eth0 for the first interface, eth1 for the second, eth0.900 for the first interface with VLAN 900 and so on.

- **MAC Filter**

  For WANGuard Sniff to distinguish between inbound and outbound traffic it must use at least one of the two techniques available: MAC filtering or IP Validation (next parameter).

  The MAC Filter together with the Source / Destination switch allows WANGuard Sniff to validate the inbound traffic and the outbound traffic. The MAC Filter should contain the MAC address of the upstream router (with the Source switch on) or the MAC address of the downstream router (with the Destination switch on). The MAC address must be written using the Linux convention - six groups of two hexadecimal values separated by colons (**:**).

- **IP Validation**

  For WANGuard Sniff to distinguish between inbound and outbound traffic it must must use at least one of the two techniques available: MAC filtering (previous parameter) or IP Validation.

  IP Validation parameter has three options:

  - *Off* - Will disable IP Validation. Make sure MAC Filter is configured instead.
  - *On* - WANGuard Sniff will only analyze the traffic that has the source and / or the destination IP addresses in the selected IP Zone, excluding 0.0.0.0/0.
  - *Strict* - WANGuard Sniff will only analyze the traffic that has either the source or the destination IP addresses in the selected IP Zone, excluding 0.0.0.0/0.

- **Direction**

  You can configure the direction of the traffic that should be analyzed by WANGuard Sniff:

  - *Inbound + Outbound* - WANGuard Sniff will monitor both inbound and outbound traffic. Using this option generates a minor performance penalty under very high loads.
  - *Inbound* - WANGuard Sniff will only monitor inbound traffic.

- **Top**

  This checkbox lets you choose if you want WANGuard Sniff to sort the traffic statistics for top-like visualizations. It is recommended to leave it on because the performance penalty is extremely low.

- **Graph Data Path**

  This field contains the path on the WANGuard Console server where the traffic graphs data collected from the WANGuard Sniff system is stored. It's safe to save multiple WANGuard Sensors graph data in the same path. If you set the data path on a larger partition, on RAM with tmpfs etc., make sure that the *wanguard* user has writing privileges there.

- **Graph Color Inbound**

  Here you can select the color you will see on graphs as inbound traffic for the current WANGuard

Sniff. By default a random color will be chosen. To change the color you can enter the color as a HTML Color Code or you can manually select the color by pressing the <...> button.

- **Graph Color Outbound**

  Here you can select the color you will see on graphs as outbound traffic for the current WANGuard Sniff. By default a random color will be chosen. To change the color you can enter the color as a HTML Color Code or you can manually select the color by pressing the <...> button.

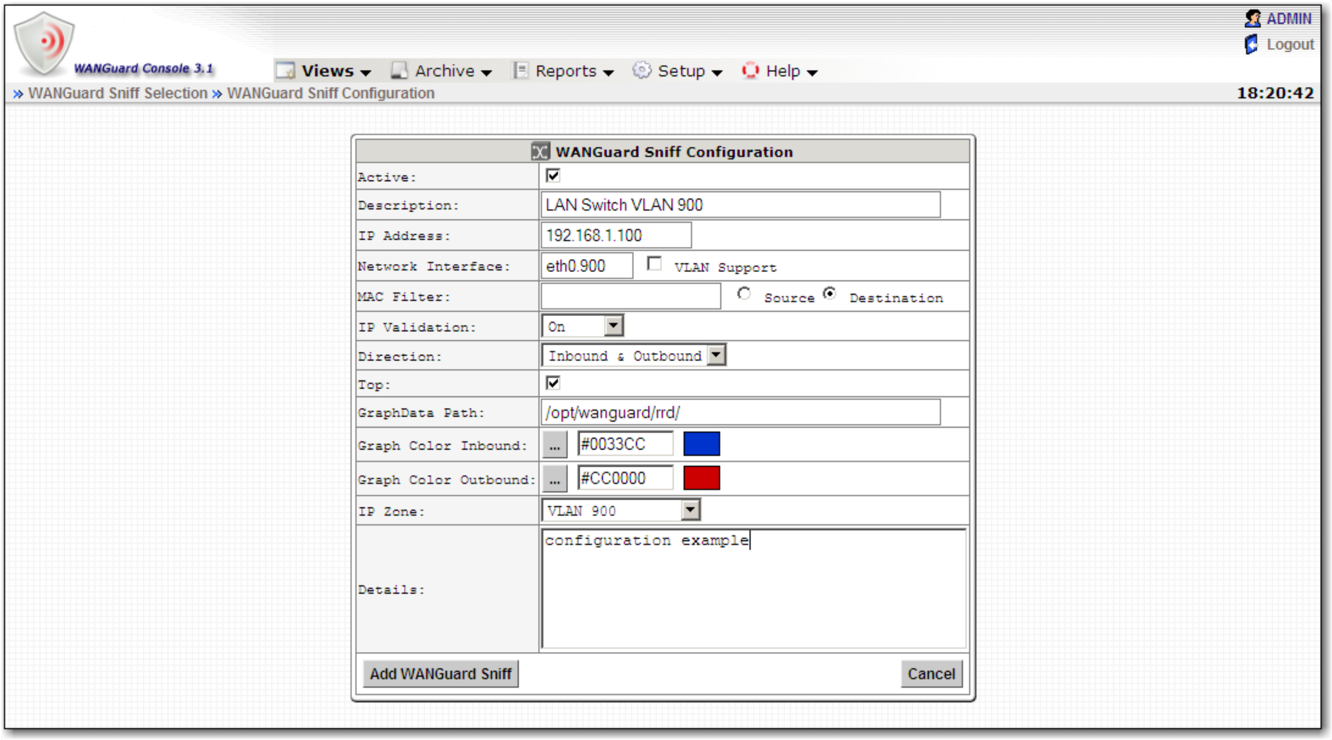
- **IP Zone**

  The IP Zone field provides a selection of currently defined IP Zones that can be used by WANGuard Sniff. If the field has no options then you must first define an IP Zone. For more information about IP Zones please read the previous chapter.

- **Details**

  You can use this field to store comments about the current WANGuard Sniff configuration.

An example of a working WANGuard Sniff configuration is displayed below. This WANGuard Sniff system analyzes all VLAN 900 traffic it receives on the first network interface, it generates Top statistics and will use IP class information found in the "VLAN 900" IP Zone.

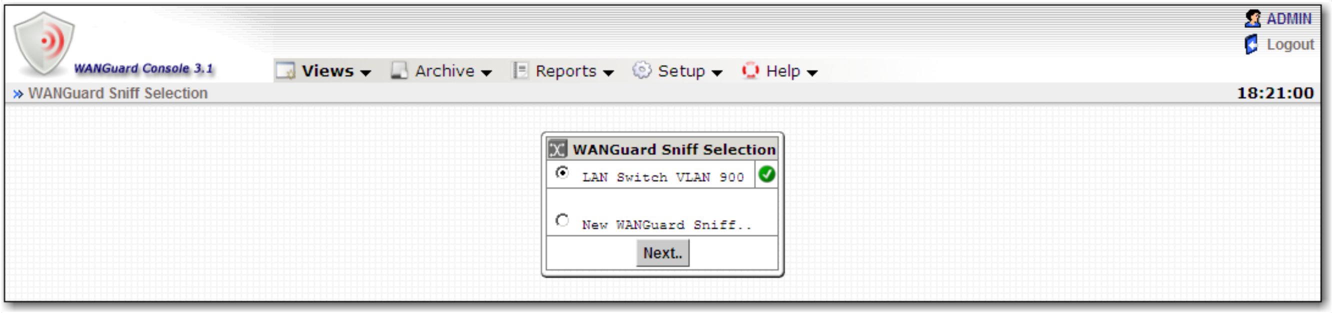


WANGuard Sniff Configuration

Active:	☑
Description:	LAN Switch VLAN 900
IP Address:	192.168.1.100
Network Interface:	eth0.900 ☐ VLAN Support
MAC Filter:	○ Source ● Destination
IP Validation:	On
Direction:	Inbound & Outbound
Top:	☑
GraphData Path:	/opt/wanguard/rrd/
Graph Color Inbound:	... #0033CC 🟦
Graph Color Outbound:	... #CC0000 🟥
IP Zone:	VLAN 900
Details:	configuration example

After a new WANGuard Sniff system is added, the WANGuard Sniff Selection window is updated. If there is a green “OK” sign on the right of the WANGuard Sniff then the WANGuard Sniff is running. If there is a “X” red sign instead, then the WANGuard Sniff is inactive or not running.

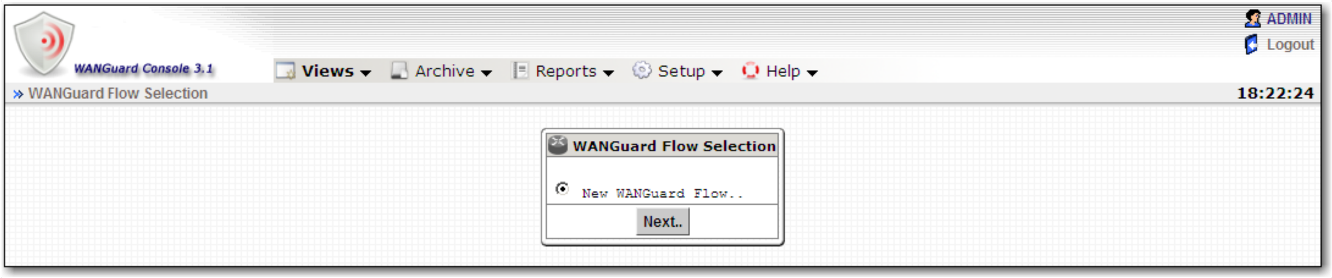
If you checked the Active switch but the WANGuard Sniff is still not running, you can find a description of the error in the WANGuard Sniff Events Logs (see Archive chapter – Page 53) or in the Events Tab (see Views chapter – Page 40) .

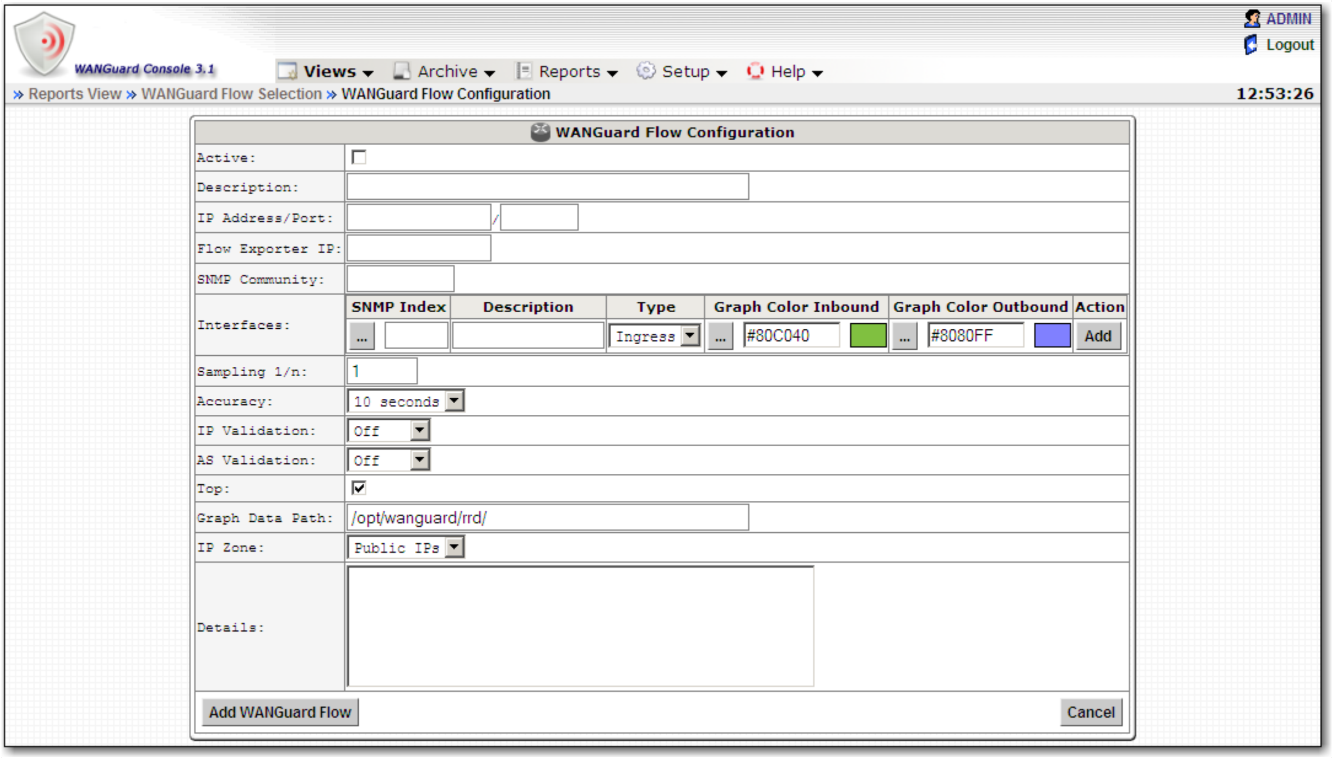


WANGuard Flow Configuration

When using WANGuard Flow, network devices must be configured to send NetFlow® version 5 data packets to the the server. For detailed instructions on how to enable NetFlow on your network devices please consult the vendor's website. Some examples are included in Appendix 1 – Configuring NetFlow Data Export (page 55).

The WANGuard Flow Selection window lets you select which WANGuard Flow system you wish to edit or delete. To add a new WANGuard Flow system select New WANGuard Flow and then click <Next..>. If no WANGuard Flow system was previously configured then the WANGuard Flow Selection form will have only the option to add a new WANGuard Flow system.





» Reports View » WANGuard Flow Selection » WANGuard Flow Configuration 12:53:26

WANGuard Flow Configuration

Active:	□
Description:	
IP Address/Port:	/
Flow Exporter IP:	
SNMP Community:	
Interfaces:	SNMP Index … | Description | Type: Ingress | Graph Color Inbound: #80C040 🟩 | Graph Color Outbound: #8080FF 🟦 | Action: Add
Sampling 1/n:	1
Accuracy:	10 seconds
IP Validation:	Off
AS Validation:	Off
Top:	☑
Graph Data Path:	/opt/wanguard/rrd/
IP Zone:	Public IPs
Details:	

The WANGuard Flow Configuration window contains the following fields:

- **Active**

  WANGuard Flow is automatically activated by the *WANGuardController* daemon if the Active checkbox is checked. If the Active checkbox is unchecked and the WANGuard Flow system is running then the *WANGuardController* daemon stops it.

- **Description**

  A short, generic description that helps you identify the WANGuard Flow system.

- **IP Address/Port**

  The IP address of the network interface that receives the flows and the port as configured on the flow exporter.

- **Flow Exporter IP**

  The IP address of the flow exporter, usually the Loopback0 interface IP on the network device. Each server running WANGuard Flow must have it's system time synchronized with the flow exporter.

- **SNMP Community**

  The read-only SNMP community of the network device. The community is used by WANGuard Console when it connects to the flow exporter to get SNMP indexes.

- **Interfaces**

Here you must define the network interfaces that will be monitored. Each interface must contain the following information:

- SNMP Index - The SNMP index of the interface. You can click the <…> button to allow WANGuard Console to connect to the network device (using the Flow Exporter IP and SNMP Community defined earlier) and to display the available interfaces and indexes.
- *Description* - A short, generic description used for interface identification.
- *Type* - Specifies the type of the interface:
  - *Ingress* - Traffic entering an Ingress interface also enters your network. Traffic that leaves an Ingress interface leaves your network. Upstream provider interfaces are always Ingress.
  - *Egress* - Traffic entering an Egress interface leaves your network. Traffic that leaves an Egress interface enters your network. On border routers, interfaces towards your network are always Egress.
  - *Null* - Traffic entering the Null interface is discarded by the router and by the WANGuard Flow.
- *Graph Color Inbound* - Here you can select the color you will see on graphs as inbound (ingress) traffic for the current interface. By default a random color will be chosen. To change the color you can enter the color as a HTML Color Code or you can manually select the color by pressing the <...> button.
- *Graph Color Outbound* - Here you can select the color you will see on graphs as outbound (egress) traffic for the current interface. By default a random color will be chosen. To change the color you can enter the color as a HTML Color Code or you can manually select the color by pressing the <...> button.

- **Sampling**

  This parameter must contain the same sampling rate configured on the router. If no flows/packet sampling is used then sampling is 1/1 (default).

- **Accuracy**

  RAM usage using the highest accuracy (5 seconds) can be very high. Decreasing the accuracy will decrease RAM usage, and won't have any negative effects in most scenarios. A very low accuracy increases the traffic anomaly detection time.

- **IP Validation**
  - *Off* - Will disable IP Validation.
  - *On* - WANGuard Flow will only analyze the traffic that has the source and / or the destination IP addresses in the selected IP Zone, excluding 0.0.0.0/0.
  - *Strict* - WANGuard Flow will only analyze the traffic that has either the source or the destination IP addresses in the selected IP Zone, excluding 0.0.0.0/0.

- **AS Validation**

Flows might contain the source and destination ASN (Autonomous System Number). In most configurations, if the ASN is set to 0 then the IP address belongs to your Autonomous System.

AS Validation has three options:

- *Off* **-** Will disable 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.

- **Top**

  This checkbox lets you choose if you want WANGuard Flow to sort the traffic statistics for top-like visualizations. It is recommended to leave it on because the performance penalty is extremely low.

- **Graph Data Path**

  This field contains the path on the WANGuard Console server where the traffic graphs data collected from the WANGuard Flow system is stored. It's safe to save multiple WANGuard Sensors graph data in the same path. If you set the data path on a larger partition, on RAM with tmpfs etc., make sure that the *wanguard* system user has writing privileges there.

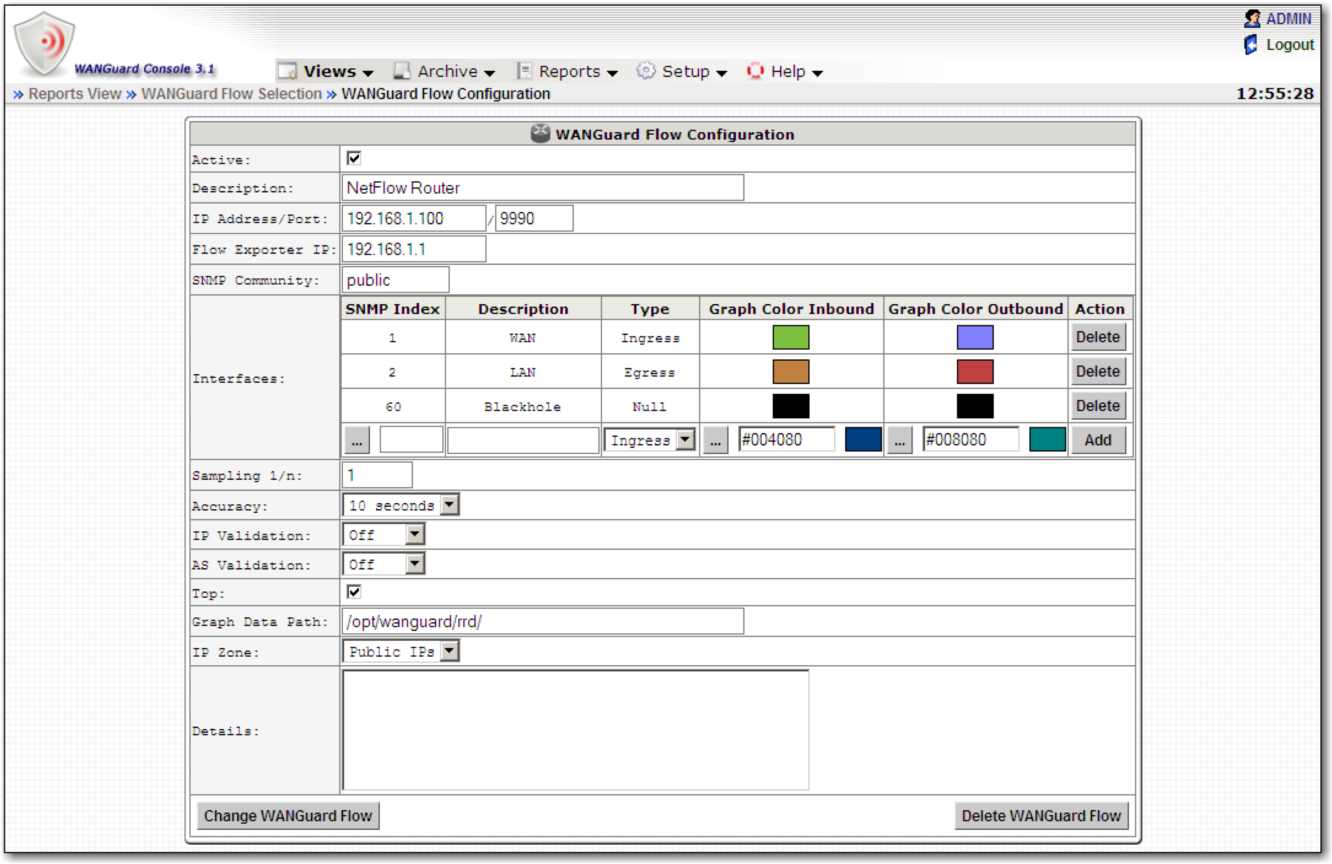
- **IP Zone**

  The IP Zone field provides a selection of currently defined IP Zones that can be used by WANGuard Flow. If the field has no options then you must first define an IP Zone. For more information about IP Zones please read the previous chapter.

- **Details**

  You can use this field to store comments about the current WANGuard Flow configuration.

In the following configuration example, WANGuard Flow monitors traffic passing the “WAN” and “LAN” interfaces, it generates Top statistics and uses IP class information found in the “Public IPs” IP Zone.


WANGuard Console 3.1
Views
Archive
Reports
Setup
Help
ADMIN
Logout
» Reports View » WANGuard Flow Selection » WANGuard Flow Configuration
12:55:28

WANGuard Flow Configuration

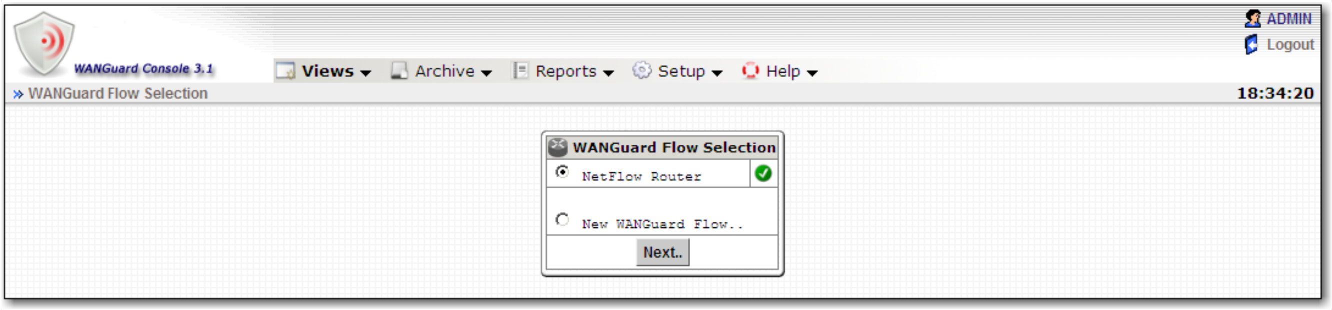
Active:	☑
Description:	NetFlow Router
IP Address/Port:	192.168.1.100 / 9990
Flow Exporter IP:	192.168.1.1
SNMP Community:	public
Interfaces:	
Sampling 1/n:	1
Accuracy:	10 seconds
IP Validation:	Off
AS Validation:	Off
Top:	☑
Graph Data Path:	/opt/wanguard/rrd/
IP Zone:	Public IPs
Details:	

Interfaces:

SNMP Index	Description	Type	Graph Color Inbound	Graph Color Outbound	Action
1	WAN	Ingress	🟩	🟦	Delete
2	LAN	Egress	🟧	🟥	Delete
60	Blackhole	Null	⬛	⬛	Delete
...		Ingress	... #004080 🟦	... #008080 🟦	Add

After a new WANGuard Flow system is added, the WANGuard Flow Selection window is updated. If there is a green “OK” sign on the right of the WANGuard Flow then the WANGuard Flow is running. If there is a “X” red sign instead, then the WANGuard Flow is inactive or not running.

If you checked the Active switch but the WANGuard Flow is still not running, you can find a description of the error in the WANGuard Flow Events Logs (see Archive chapter – Page 53) or in the Events Tab (see Views chapter – Page 40) .



WANGuard Flow Selection

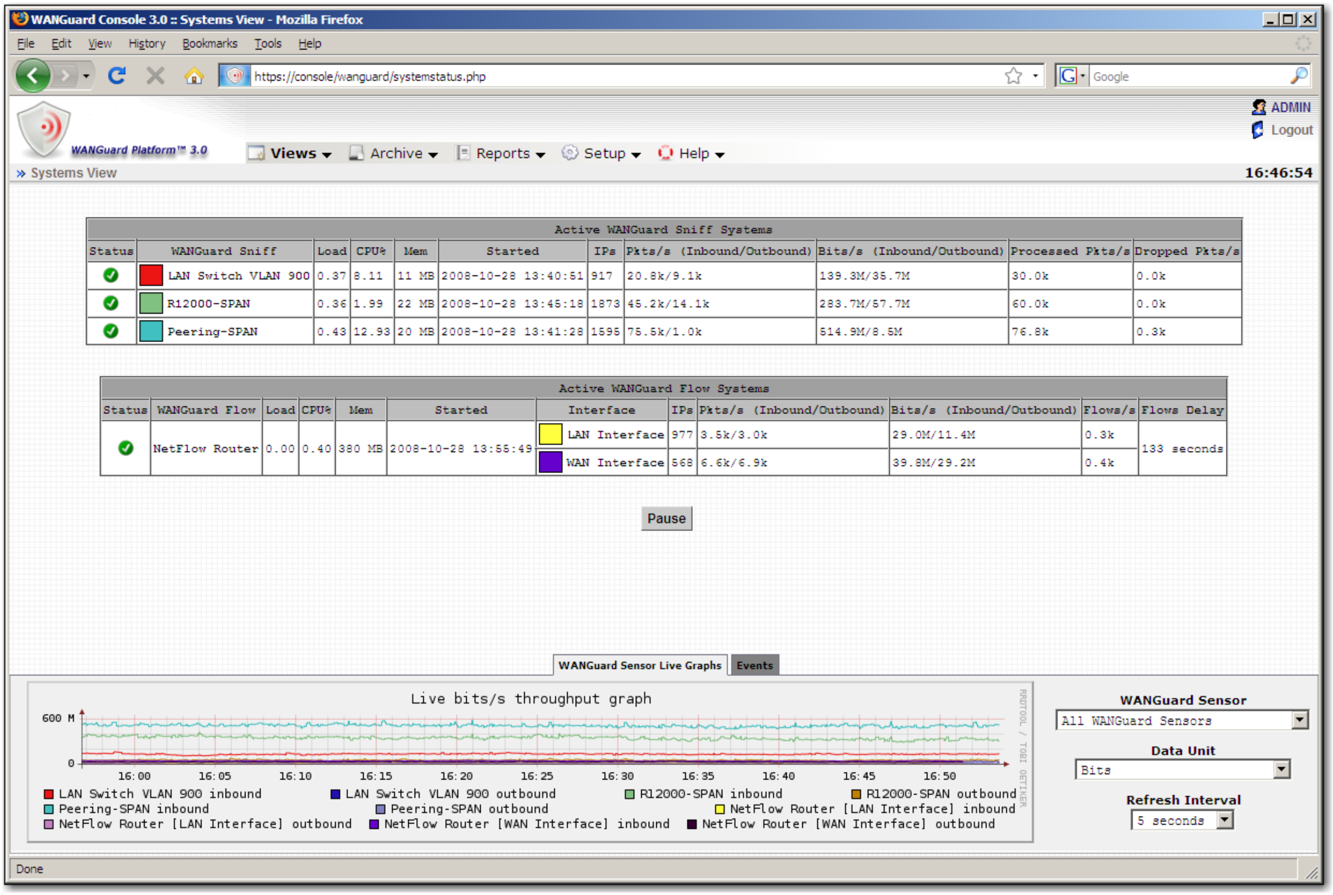
- ● NetFlow Router ✓
- ○ New WANGuard Flow..

Views

Views are WANGuard Console windows that display the latest information collected from WANGuard Lite components. Every View displays text and graphical elements using the Ajax technology (Web 2.0) that offers flicker-free web page updates every **5 seconds**. To browse through available Views click the Views menu and then select **Systems View** (for systems administrators), or **Reports View** (for network administrators).

Systems View

The Systems View displays tables with the latest system parameters collected from active WANGuard Lite components.


WANGuard Console 3.0 :: Systems View - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://console/wanguard/systemstatus.php
Google
ADMIN
Logout
WANGuard Platform™ 3.0
Views
Archive
Reports
Setup
Help
» Systems View
16:46:54
Pause
WANGuard Sensor Live Graphs
Events
Live bits/s throughput graph
600 M
0
16:00
16:05
16:10
16:15
16:20
16:25
16:30
16:35
16:40
16:45
16:50
LAN Switch VLAN 900 inbound
LAN Switch VLAN 900 outbound
R12000-SPAN inbound
R12000-SPAN outbound
Peering-SPAN inbound
Peering-SPAN outbound
NetFlow Router [LAN Interface] inbound
NetFlow Router [LAN Interface] outbound
NetFlow Router [WAN Interface] inbound
NetFlow Router [WAN Interface] outbound
RRDTOOL / TOBI OETIKER
Done

Active WANGuard Sniff Systems

Status		WANGuard Sniff	Load	CPU%	Mem	Started	IPs	Pkts/s (Inbound/Outbound)	Bits/s (Inbound/Outbound)	Processed Pkts/s	Dropped Pkts/s
✓	🟥	LAN Switch VLAN 900	0.37	8.11	11 MB	2008-10-28 13:40:51	917	20.8k/9.1k	139.3M/35.7M	30.0k	0.0k
✓	🟩	R12000-SPAN	0.36	1.99	22 MB	2008-10-28 13:45:18	1873	45.2k/14.1k	283.7M/57.7M	60.0k	0.0k
✓	🟦	Peering-SPAN	0.43	12.93	20 MB	2008-10-28 13:41:28	1595	75.5k/1.0k	514.9M/8.5M	76.8k	0.3k

Active WANGuard Flow Systems

Status	WANGuard Flow	Load	CPU%	Mem	Started		Interface	IPs	Pkts/s (Inbound/Outbound)	Bits/s (Inbound/Outbound)	Flows/s	Flows Delay
✓	NetFlow Router	0.00	0.40	380 MB	2008-10-28 13:55:49	🟨	LAN Interface	977	3.5k/3.0k	29.0M/11.4M	0.3k	133 seconds
						🟪	WAN Interface	568	6.6k/6.9k	39.8M/29.2M	0.4k	

WANGuard Sensor: All WANGuard Sensors

Data Unit: Bits

Refresh Interval: 5 seconds

The refreshing of tables can be stopped by clicking the <Pause> button. When the <Pause> button is clicked it will change into a <Resume> button that will resume the refreshing of tables, when clicked.

The Systems View page includes Active Systems tables and two tabs: WANGuard Sensor Live Graphs Tab and Events Tab. Each of those elements is explained in the following sections.

Active WANGuard Sniff Systems Table

The Active WANGuard Sniff Systems table displays the latest system information collected from active WANGuard Sniff systems. If there are no WANGuard Sniff systems configured then this table is not displayed. The table has the following format:

Status	If the active WANGuard Sniff system is functioning properly then a green “checked” arrow is displayed. If WANGuard Console cannot manage or reach the WANGuard Sniff system then a red “X” icon is displayed. In this case make sure that WANGuard Sniff is configured correctly, read the Events Log and make sure that the *WANGuardController* daemon is running on all systems.
WANGuard Sniff	Displays the description of the WANGuard Sniff system and a colored box with the Graph Color Inbound as defined in the configuration.
Load	The load of the operating system for the last 5 minutes.
CPU%	The CPU percent used by the WANGuard Sniff process.
Mem	The amount of memory used by the WANGuard Sniff process.
Started	The time and date when the WANGuard Sniff process started.
IPs	The number of unique IP addresses detected making traffic. Only your network's IP addresses are counted.
Pkts/s (Inbound / Outbound)	The packets/second throughput after validation and filtering.
Bits/s (Inbound / Outbound)	The bits/second throughput after validation and filtering.
Received Pkts/s	The rate of received packets before validation and filtering.
Dropped Pkts/s	It represents the rate of packets dropped in the capturing process. When the number is high it indicates a performance problem located in the network card, in the network card's driver, or in the CPU. It may also mean a bad WANGuard Sniff installation.

Active WANGuard Flow Systems Table

The Active WANGuard Flow Systems table displays the latest system information collected from the active WANGuard Flow systems. If there are no WANGuard Flow systems configured then this table is not displayed. The table has the following format:

Status	If the active WANGuard Flow system is functioning properly then a green “checked” arrow is displayed. If WANGuard Console cannot manage or reach the WANGuard Flow system then a red “X” icon is displayed. In this case make sure that WANGuard Flow is configured correctly, read the Events Log and make sure that the *WANGuardController* daemon is running on all systems.
WANGuard Flow	Displays the description of the WANGuard Flow system.
Load	The load of the operating system for the last 5 minutes.
CPU%	The CPU percent used by the WANGuard Flow process.
Mem	The amount of memory used by the WANGuard Flow process.
Started	The time and date when the WANGuard Flow process started.
Interface	The interface description and a colored box with the Graph Color Inbound configured for the interface.
IPs	The number of unique IP addresses detected making traffic through the interface. Only your network's IP addresses are counted.
Pkts/s (Inbound/Outbound)	The packets/second throughput after validation and filtering. Only the traffic passing the interface is analyzed.
Bits/s (Inbound/Outbound)	The bits/second throughput after validation and filtering. Only the traffic passing the interface is analyzed.
Flows/s	The rate of flows that contain traffic passing the interface.
Flows Delay	Because traffic data must be aggregated, NetFlow devices export flows with a certain configured delay. Some devices export flows much later than the configured delays, and this field contains the maximum flows delay detected by WANGuard Flow. WANGuard Flow cannot run with delays over 5 minutes. To minimize the RAM usage and the performance of the WANGuard Flow process, the flows must be exported as soon as possible.

WANGuard Sensor Live Graphs Tab

The WANGuard Sensor Graphs Tab provides an animated, dynamic graph that illustrates trends over time of various traffic parameters collected from WANGuard Sensor systems.

The right side of the tab contains three selections lists that configure the graph:

- **WANGuard Sensor**

  Select the WANGuard Sensor system you're interested in.

- **Data Unit**

  Select the traffic parameter the graph will represent:

  - *Bits* - The bits/second throughput recorded by WANGuard Sensor.
  - *Bytes* - The bytes/second throughput recorded by WANGuard Sensor.
  - *Packets* - The packets/second throughput recorded by WANGuard Sensor.
  - *IPs* - The number of unique IP addresses detected making traffic. Usually a spike in the graph means that an IP class scan was performed. Only your network's IP addresses are counted.
  - *Received packets or flows* - For WANGuard Sniff it represents the rate of received packets before validation or filtering occurs. For WANGuard Flow it represents the rate of received flows before validation or filtering occurs.
  - *Dropped packets or flows* - For WANGuard Sniff it represents the rate of packets dropped in the capturing process. When the number is high it indicates a performance problem located in the network card, in the network card's driver, or in the CPU. It may also mean a bad WANGuard Sniff installation. For WANGuard Flow it represents the rate of flows dropped in the flow receiving process. When the number is high, it indicates a network problem between the flow exporter and the WANGuard Flow system, or a bad WANGuard Flow installation.
  - *Unknown packets or flows* - For WANGuard Sniff it represents the rate of discarded packets caused by validation or filtering. For WANGuard Flow it represents the rate of discarded flows caused by validation or filtering.

- **Refresh Interval**

  Select the interval between consecutive refreshes of the graph. The graph will update itself flicker-free, but it's best to keep the refresh interval big for low-bandwidth monitoring stations.

Events Tab

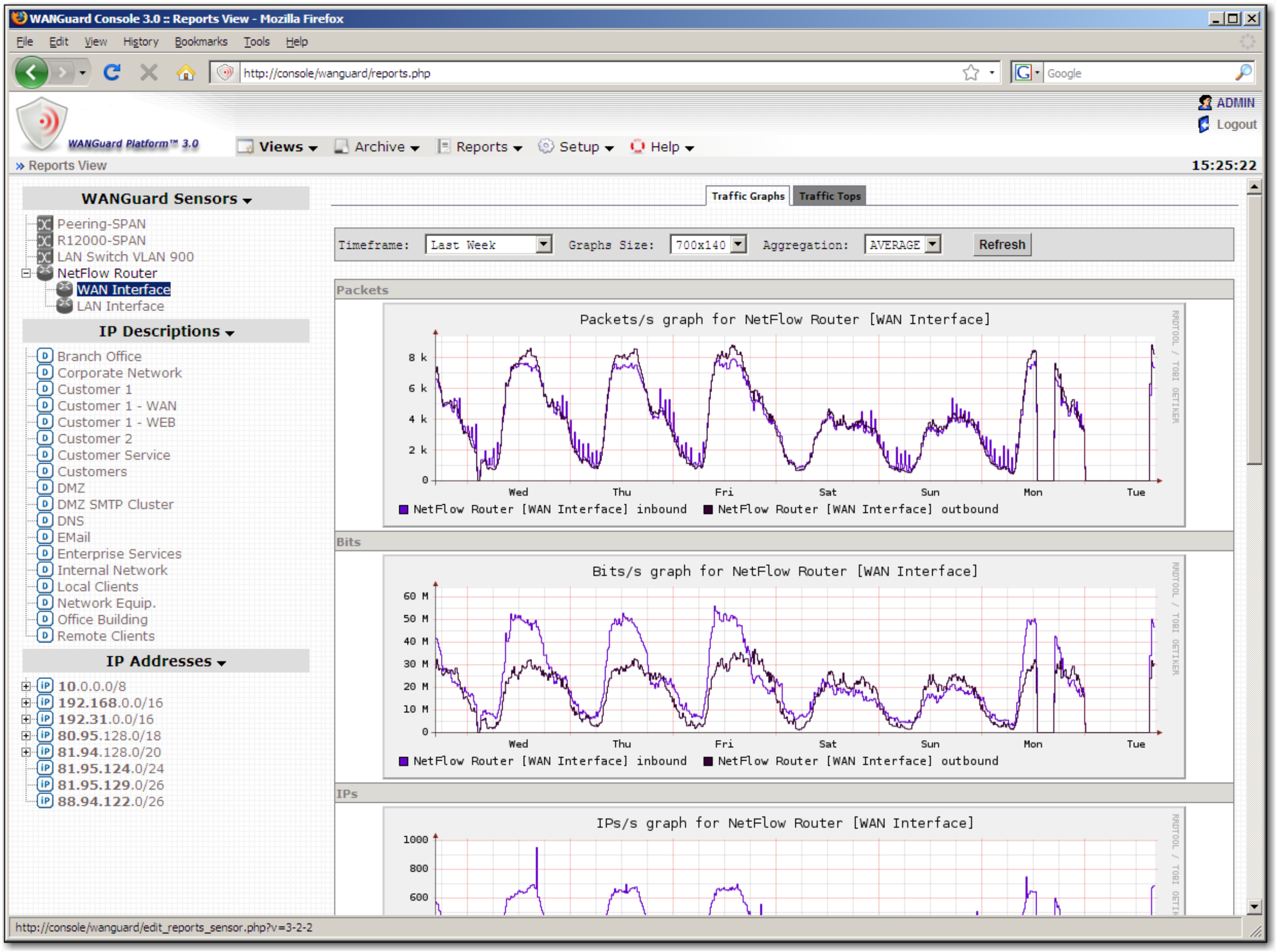
The Events Tab provides a list with the latest events recorded in the Events Log. Every field is explained in the Events Log section of the Archive chapter (Page 53).

Reports View

The Reports View provides easy access to live and historical information about monitored hosts, networks and network interfaces. The Reports View is split vertically in two sides. The left side contains three sections: WANGuard Sensors, IP Descriptions and IP Addresses. To prevent clutter you can click each section's header to minimize or maximize the section.

WANGuard Sensors Section

When you click a WANGuard Sensor description or interface, the right side of the Reports View will contain two tabbed areas, as you can see in the screenshot below. The **Traffic Graphs** area displays graphs containing traffic parameters generated by the selected WANGuard Sensor.



Timeframe: Last Week Graphs Size: 700x140 Aggregation: AVERAGE

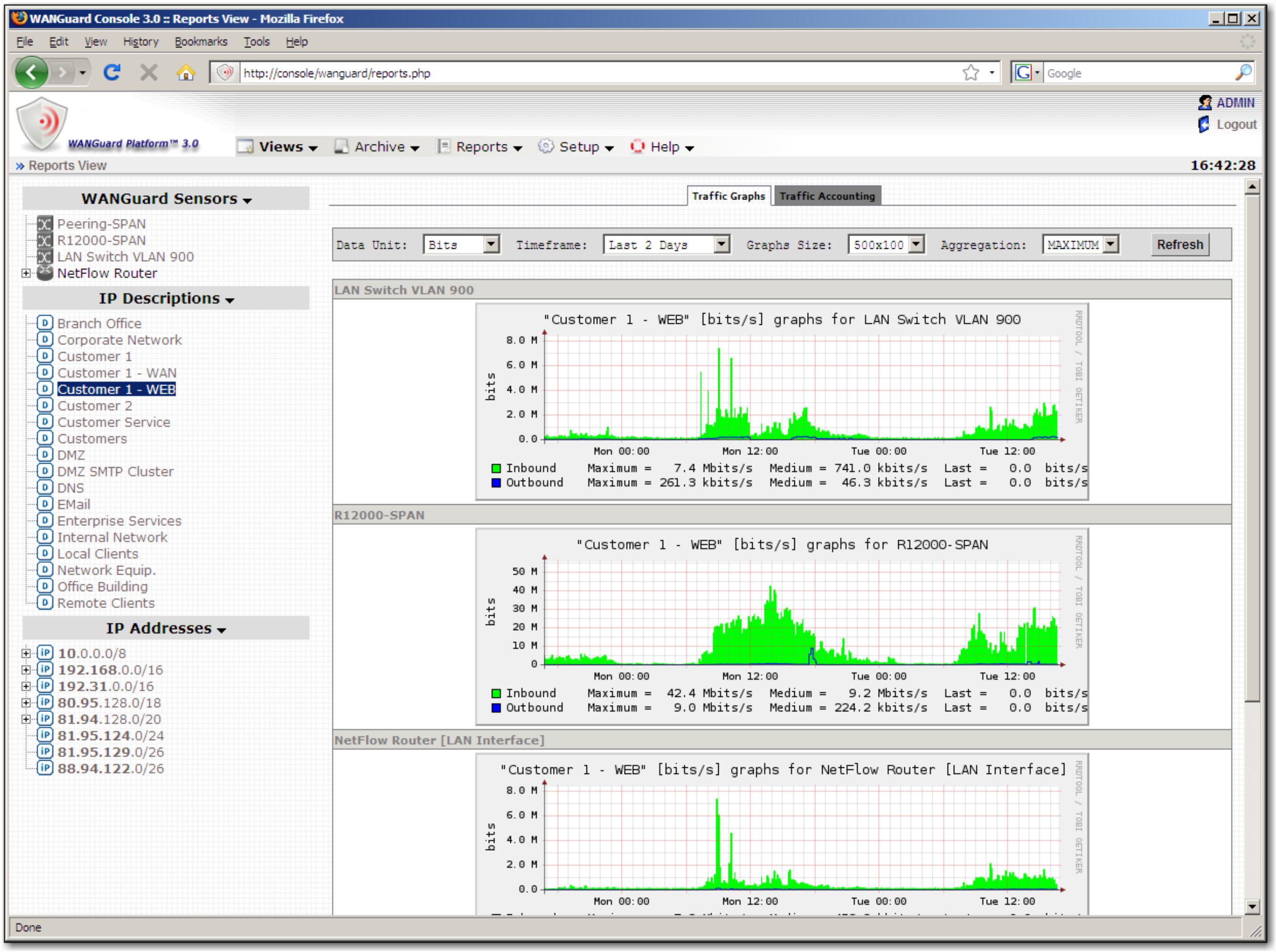
http://console/wanguard/edit_reports_sensor.php?v=3-2-2

The **Traffic Tops** area provides live statistics about top hosts (“talkers”), top TCP ports, top UDP ports, top IP protocols and top AS Numbers (only when NetFlow is used). This tab is not available if the selected WANGuard Sensor does not have the “Top” option activated in its configuration.

IP Descriptions Section

This section contains IP Description fields extracted from all existing IP Zones. When you click an IP Description, the right side of the Reports View will contain two tabbed areas, as you can see in the screenshot below. The **Traffic Graphs** area contains graphs with traffic parameters generated for all hosts or networks that have the selected IP Description.

The **Traffic Accounting** area contains a traffic accounting report generated for the hosts or networks that have the selected IP Description.



Data Unit: Bits Timeframe: Last 2 Days Graphs Size: 500x100 Aggregation: MAXIMUM

"Customer 1 - WEB" [bits/s] graphs for LAN Switch VLAN 900

```
Inbound    Maximum =   7.4 Mbits/s   Medium = 741.0 kbits/s   Last =   0.0  bits/s
Outbound   Maximum = 261.3 kbits/s   Medium =  46.3 kbits/s   Last =   0.0  bits/s
```

"Customer 1 - WEB" [bits/s] graphs for R12000-SPAN

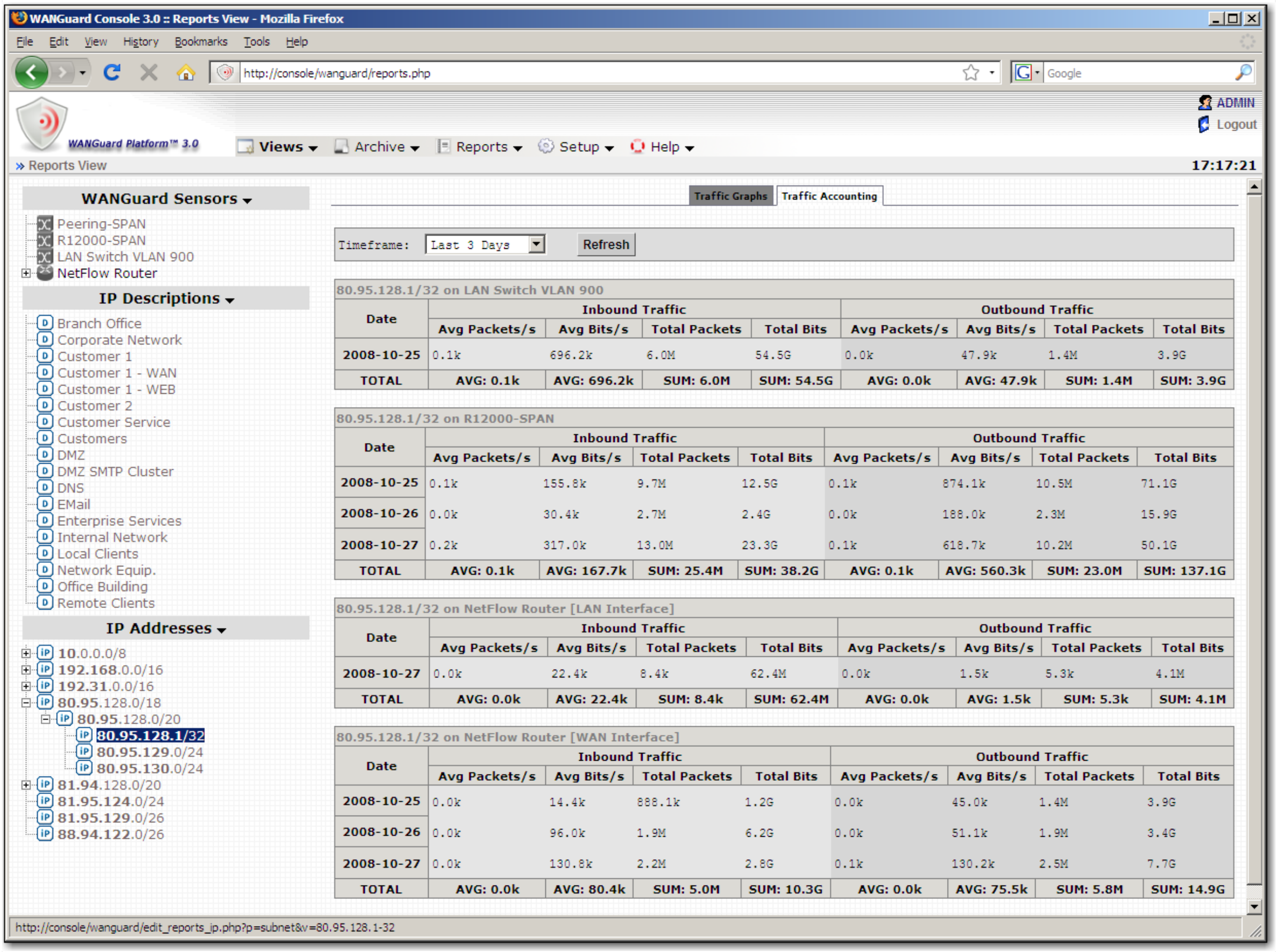
```
Inbound    Maximum =  42.4 Mbits/s   Medium =   9.2 Mbits/s   Last =   0.0  bits/s
Outbound   Maximum =   9.0 Mbits/s   Medium = 224.2 kbits/s   Last =   0.0  bits/s
```

"Customer 1 - WEB" [bits/s] graphs for NetFlow Router [LAN Interface]

IP Addresses Section

This section provides an IP tree that contains all IP classes extracted from existing IP Zones. When you click an IP class, the right side of the Reports View will contain two tabbed areas, as you can see in the screenshot below. The **Traffic Graphs** area contains graphs with traffic parameters generated for the selected host or network.

The **Traffic Accounting** area contains a traffic accounting report generated for the selected host or network.



Timeframe: Last 3 Days

80.95.128.1/32 on LAN Switch VLAN 900

Date	Inbound Traffic				Outbound Traffic			
	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits
2008-10-25	0.1k	696.2k	6.0M	54.5G	0.0k	47.9k	1.4M	3.9G
TOTAL	AVG: 0.1k	AVG: 696.2k	SUM: 6.0M	SUM: 54.5G	AVG: 0.0k	AVG: 47.9k	SUM: 1.4M	SUM: 3.9G

80.95.128.1/32 on R12000-SPAN

Date	Inbound Traffic				Outbound Traffic			
	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits
2008-10-25	0.1k	155.8k	9.7M	12.5G	0.1k	874.1k	10.5M	71.1G
2008-10-26	0.0k	30.4k	2.7M	2.4G	0.0k	188.0k	2.3M	15.9G
2008-10-27	0.2k	317.0k	13.0M	23.3G	0.1k	618.7k	10.2M	50.1G
TOTAL	AVG: 0.1k	AVG: 167.7k	SUM: 25.4M	SUM: 38.2G	AVG: 0.1k	AVG: 560.3k	SUM: 23.0M	SUM: 137.1G

80.95.128.1/32 on NetFlow Router [LAN Interface]

Date	Inbound Traffic				Outbound Traffic			
	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits
2008-10-27	0.0k	22.4k	8.4k	62.4M	0.0k	1.5k	5.3k	4.1M
TOTAL	AVG: 0.0k	AVG: 22.4k	SUM: 8.4k	SUM: 62.4M	AVG: 0.0k	AVG: 1.5k	SUM: 5.3k	SUM: 4.1M

80.95.128.1/32 on NetFlow Router [WAN Interface]

Date	Inbound Traffic				Outbound Traffic			
	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits	Avg Packets/s	Avg Bits/s	Total Packets	Total Bits
2008-10-25	0.0k	14.4k	888.1k	1.2G	0.0k	45.0k	1.4M	3.9G
2008-10-26	0.0k	96.0k	1.9M	6.2G	0.0k	51.1k	1.9M	3.4G
2008-10-27	0.0k	130.8k	2.2M	2.8G	0.1k	130.2k	2.5M	7.7G
TOTAL	AVG: 0.0k	AVG: 80.4k	SUM: 5.0M	SUM: 10.3G	AVG: 0.0k	AVG: 75.5k	SUM: 5.8M	SUM: 14.9G

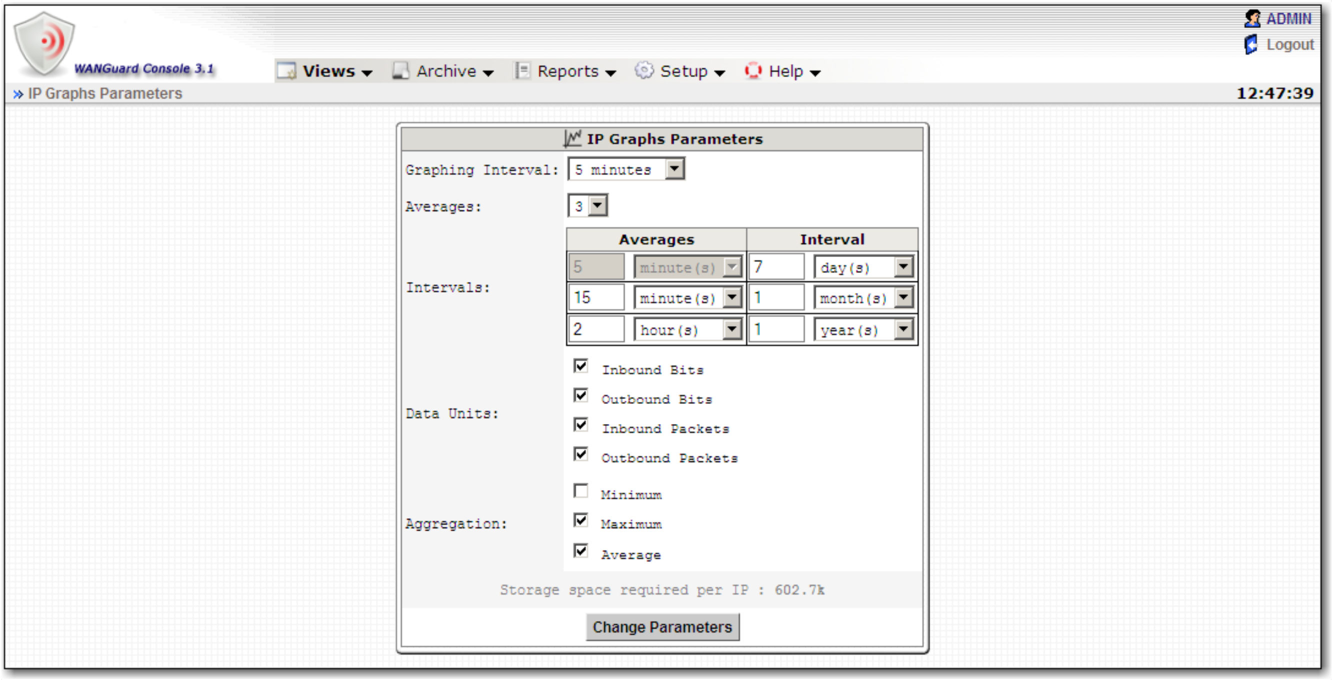
http://console/wanguard/edit_reports_ip.php?p=subnet&v=80.95.128.1-32

Traffic Accounting and Graphing

This chapter describes how to generate **advanced** traffic graphs and traffic accounting reports from data collected by WANGuard Sensor systems. For an **easier** but more limited access to traffic graphs and accounting reports, you can use the Reports View (Page 41).

IP Traffic Graphs Setup

To configure IP traffic graphs parameters select IP Graphs from the Setup menu.



IP Graphs Parameters

Graphing Interval: 5 minutes

Averages: 3

Intervals:

Averages		Interval	
5	minute(s)	7	day(s)
15	minute(s)	1	month(s)
2	hour(s)	1	year(s)

Data Units:
☑ Inbound Bits
☑ Outbound Bits
☑ Inbound Packets
☑ Outbound Packets

Aggregation:
☐ Minimum
☑ Maximum
☑ Average

Storage space required per IP : 602.7k

By default, every WANGuard Sensor stores IP graphing data with 5 minutes averages for 7 days, 15 minutes averages for 1 month, and 2 hours averages for 1 year. The default graphing interval is 5 minutes. If you do not change the default parameters, every IP for which you enabled graphing will require 603 kbytes of storage on the WANGuard Console's file system.

The **Graphing Interval** specifies the granularity of the graphs. The highest available granularity value is 5 seconds and the lowest is 5 minutes. When using WANGuard Flow, do not set the Graphing Interval to a lower value than the Accuracy parameter.

When granularity is very high, WANGuard Sensor uses more CPU, the WANGuard Console system becomes more loaded, and the network traffic between WANGuard Sensor and WANGuard Console is increased if the components are not installed on the same server.

The **Averages** and **Intervals** values specify the granularity for old data and for how long do you want the data to be stored.

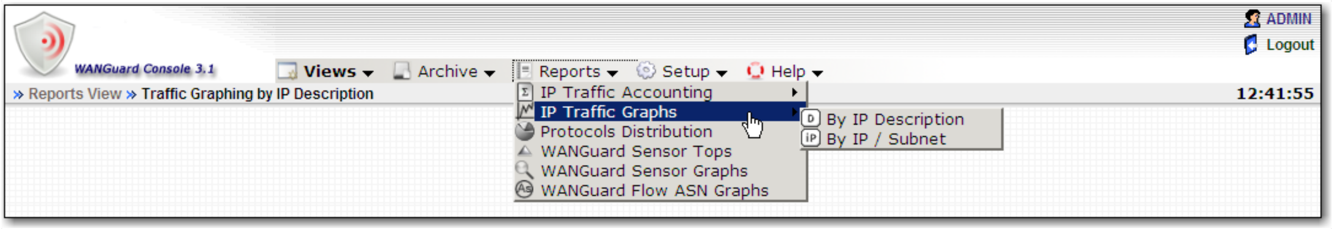
The **Data Units** options lets you select the traffic parameters that will be stored.

The **Aggregation** options lets you select how do you want the average values to be consolidated. If you are interested in traffic spikes, select the *MAXIMUM* aggregation type. If you are interested in average values, select the *AVERAGE* aggregation type. If you are interested in low traffic values, select the *MINIMUM* aggregation type.

All the above options have a direct impact on the storage space required on the WANGuard Console file system. The *storage space required per IP* will be updated when you click the <Change Parameters> button. If you change the graphs parameters, make sure you delete old data from the paths defined in WANGuard Sensor configurations.

IP Traffic Graphs

WANGuard Console can generate on-demand MRTG-style graphs for every hosts, IP class or IP classes sharing the same IP Description. The time-frame must be included in the biggest interval value configured in IP Traffic Graphs Setup. To generate IP traffic graphs select IP Traffic Graphs from the Reports menu, and then select one of the two available options.



The first option generates traffic graphs for IPs or IP classes that have the IP Description you select. The second option generates traffic graphs for the entered IP address or IP class.

The following fields are common for both options:

- **From / Until**

  Enter the desired time-frame.

- **WANGuard Sensor(s)**

  Contains all configured WANGuard Sensor systems. Select the WANGuard Sensor that captured the traffic you're interested in. Multiple selections can be made by holding the Control / Ctrl key.

- **Sum Multiple Sensors**

  If unchecked, each WANGuard Sensor generates a different traffic graph. If checked, all selected WANGuard Sensors generate a single traffic graph that contains the summed traffic data.

- **Data Unit**

  Enter the data unit for the traffic graph: *packets/second, bits/second* or *bytes/second*. If some data units are missing, see the IP Traffic Graphs configuration (Page 44).

- **Graph Size**

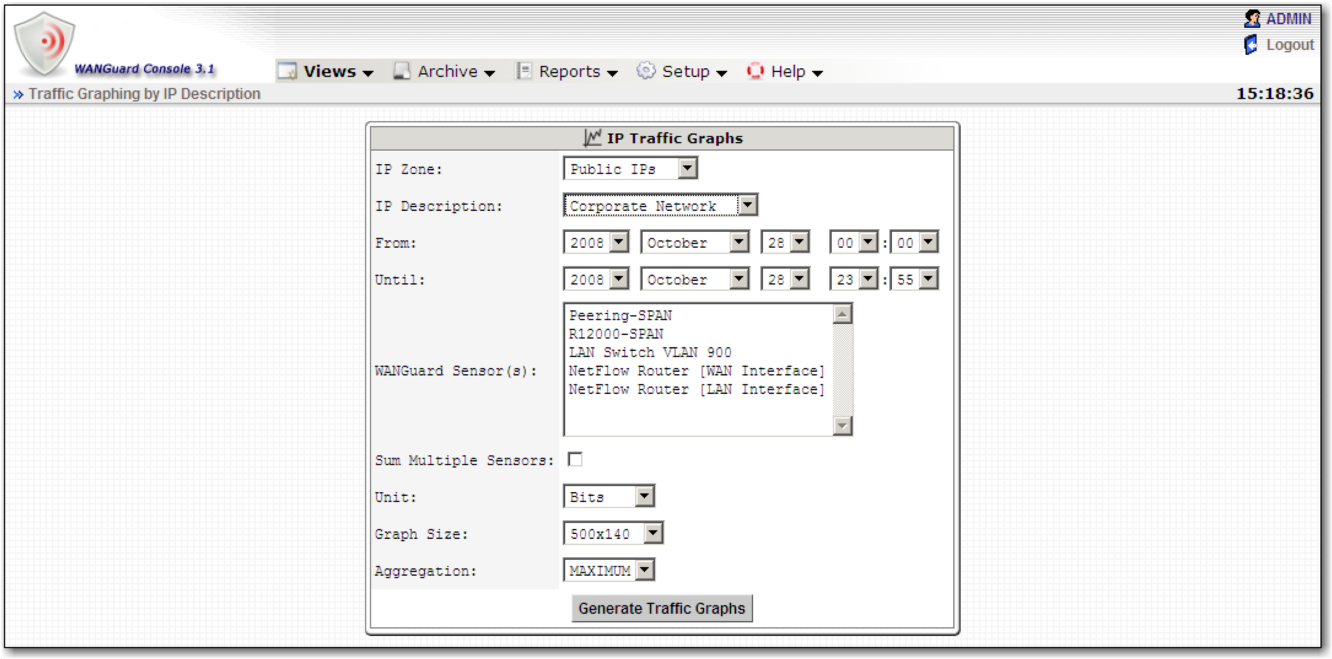
  Select the graph size.

- **Aggregation**

  Select the aggregation procedure for the graph: *MINIMUM*, *MAXIMUM* or *AVERAGE*. If some aggregation types are missing, see the IP Traffic Graphs configuration (Page 44).

By IP Description

By selecting this option you can generate traffic graphs for IPs or IP classes that share the selected IP Description. To generate traffic graphs using IP Descriptions, fill the form displayed below.



IP Zone: Public IPs

IP Description: Corporate Network

From: 2008 October 28 00:00

Until: 2008 October 28 23:55

WANGuard Sensor(s):
Peering-SPAN
R12000-SPAN
LAN Switch VLAN 900
NetFlow Router [WAN Interface]
NetFlow Router [LAN Interface]

Sum Multiple Sensors: □

Unit: Bits

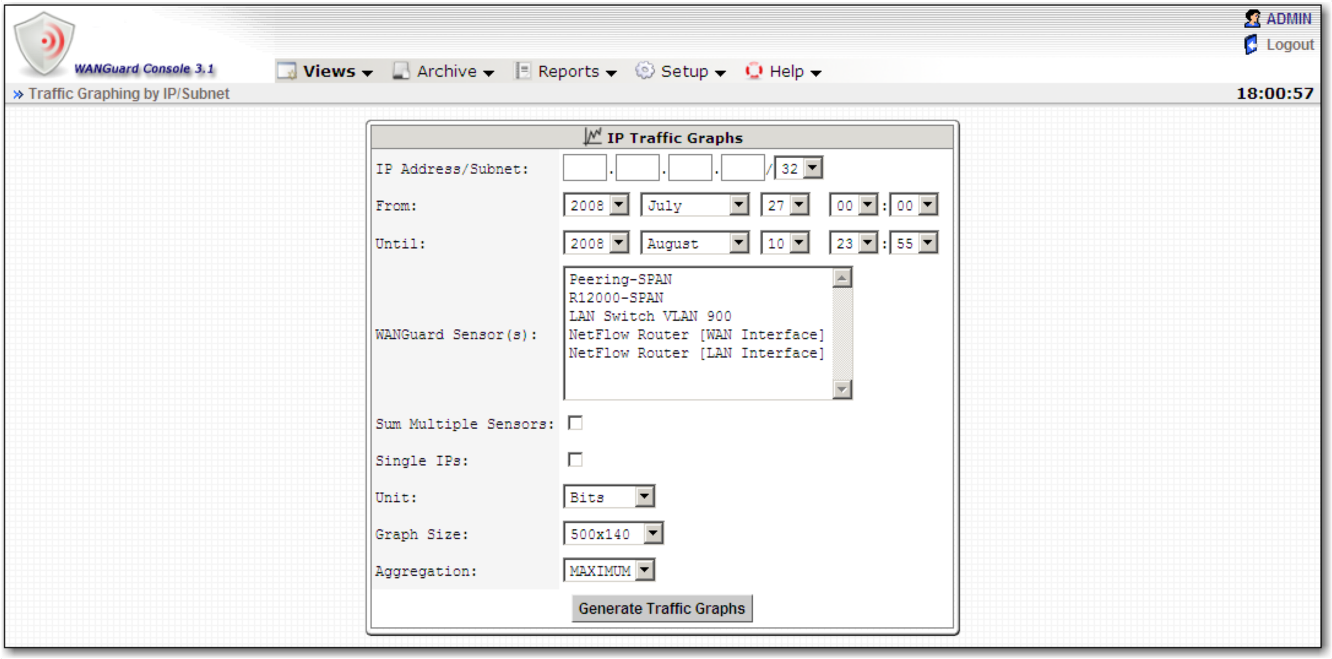
Graph Size: 500x140

Aggregation: MAXIMUM

Most fields are explained in the beginning of this section. To generate IP traffic graphs using this option, first select an **IP Zone** and then select an **IP Description** included in the selected IP Zone. WANGuard Console will search for IP addresses and IP classes that match the selected IP Description and will generate IP traffic graphs accordingly. By using this option you can easily generate traffic graphs for clients, departments etc. with multiple allocated IP classes.

By IP Address / Subnet

To generate traffic graphs for an IP address or IP class, fill the form displayed below.



IP Traffic Graphs

IP Address/Subnet: ___ . ___ . ___ . ___ / 32

From: 2008 July 27 00 : 00

Until: 2008 August 10 23 : 55

WANGuard Sensor(s): Peering-SPAN, R12000-SPAN, LAN Switch VLAN 900, NetFlow Router [WAN Interface], NetFlow Router [LAN Interface]

Sum Multiple Sensors: □

Single IPs: □

Unit: Bits

Graph Size: 500x140

Aggregation: MAXIMUM

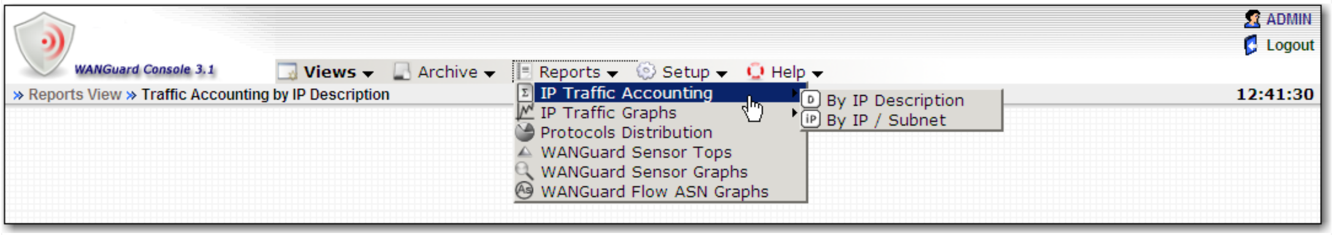
Most fields are explained on the beginning of this section. For the **IP Address / Subnet** fields use the CIDR notation. To generate traffic graphs for hosts - not networks, select the /32 CIDR. For more information about CIDR consult the Network Basics You Should Be Aware Of chapter (Page 13).

Check the **Single IPs** option if you want a different traffic graph displayed for every IP address contained in the selected subnet. For example, when this option is used with a /24 CIDR then 256 traffic graphs are displayed, one for each IP address in the "C" class.

If the traffic graphs are not displayed, check if the entered IP Address / Subnet is included in the selected WANGuard Sensor's IP Zone and that the "Graphing" parameter for that IP class is set to *Yes*.

IP Traffic Accounting

WANGuard Console can generate on-demand IP traffic accounting reports for every host, IP class or IP classes that share the same IP Description, for any time-frame. To generate an IP traffic accounting report, select IP Traffic Accounting from the Reports menu, and then select one of the two available options.



The first option generates IP traffic accounting reports for IP addresses or IP classes that have the IP Description you select. The second option generates IP traffic accounting reports for the entered IP address or IP class.

The following fields are common for both options:

- **From / Until**

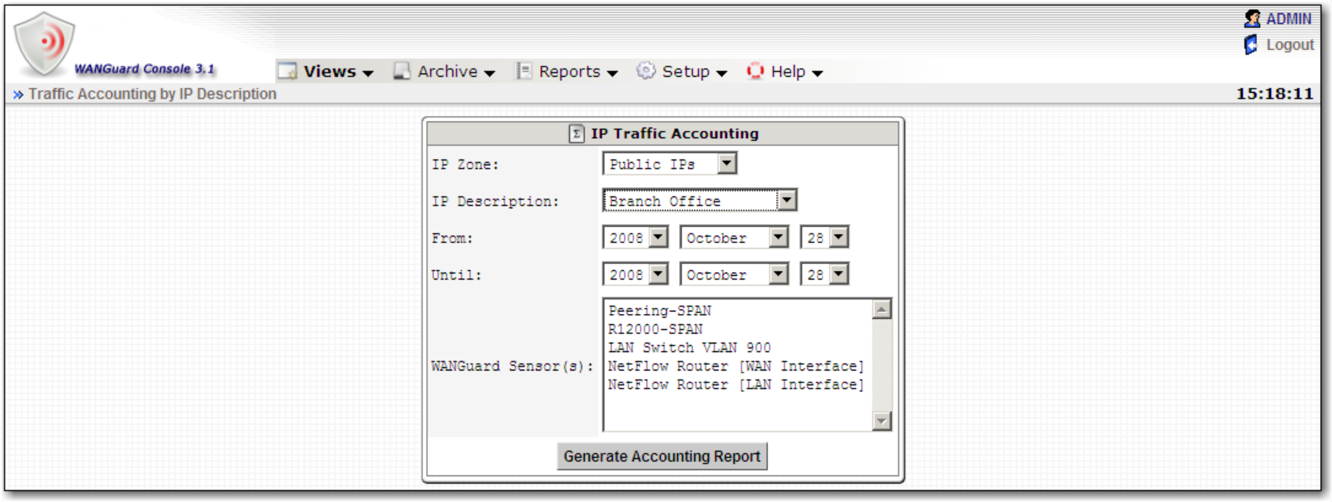
  Enter the desired time-frame.

- **WANGuard Sensor(s)**

  Contains all configured WANGuard Sensor systems. Select the WANGuard Sensor that captured the traffic you're interested in. Multiple selections can be made by holding the Control key.

By IP Description

By selecting this option you can generate traffic accounting reports for IP addresses or IP classes that have the selected IP Description.



IP Traffic Accounting

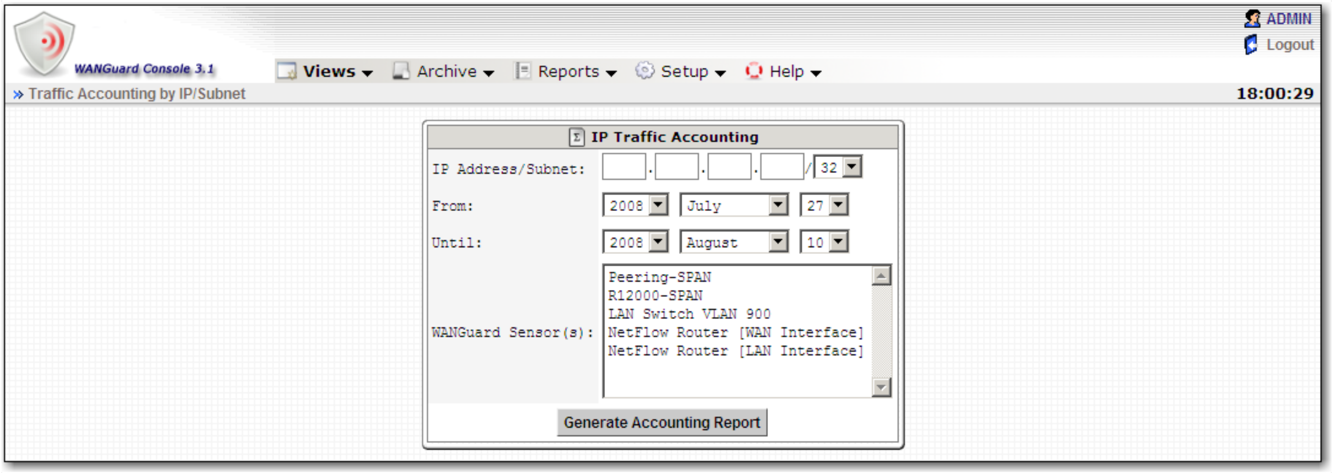
IP Zone:	Public IPs
IP Description:	Branch Office
From:	2008 October 28
Until:	2008 October 28
WANGuard Sensor(s):	Peering-SPAN R12000-SPAN LAN Switch VLAN 900 NetFlow Router [WAN Interface] NetFlow Router [LAN Interface]

The **From**, **Until** and **WANGuard Sensor(s)** fields are explained in the beginning of this section.

To generate traffic accounting reports using this option, first select an **IP Zone** and then select an **IP Description** included in the selected IP Zone. WANGuard Console will search for IP addresses and IP classes that match the selected IP Description and will generate a traffic accounting report for them. By using this option you can easily generate IP traffic accounting reports for clients, departments etc. with multiple allocated IP classes.

By IP Address / Subnet

To generate a traffic accounting report for an IP address or IP class, fill the form displayed below.



IP Traffic Accounting

IP Address/Subnet:	. . . / 32
From:	2008 July 27
Until:	2008 August 10
WANGuard Sensor(s):	Peering-SPAN R12000-SPAN LAN Switch VLAN 900 NetFlow Router [WAN Interface] NetFlow Router [LAN Interface]

The **From**, **Until** and **WANGuard Sensor(s)** fields are explained in the beginning of this section.

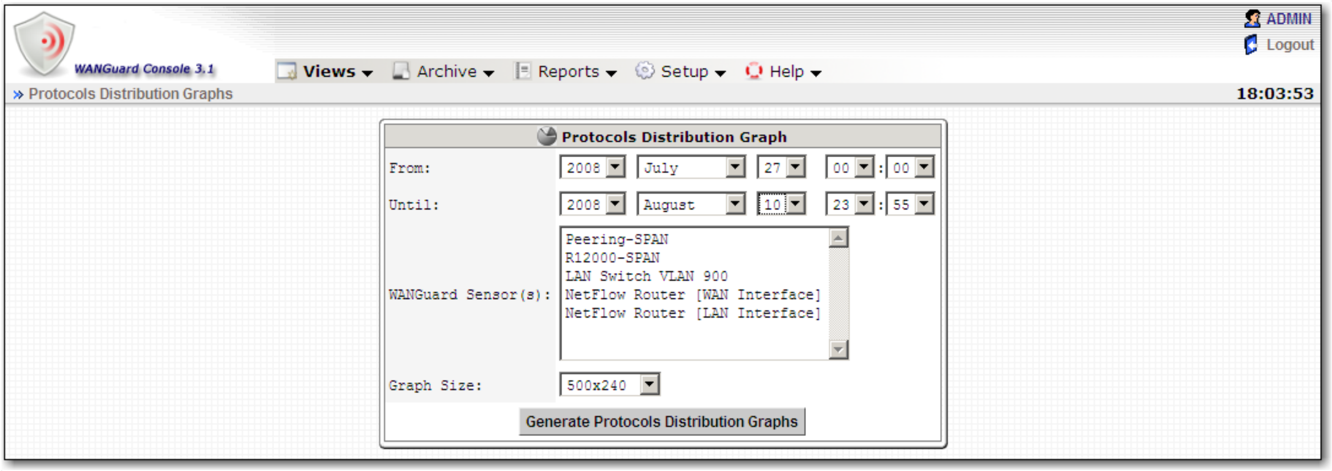
For the **IP Address / Subnet** fields use the CIDR notation. To generate traffic accounting reports for hosts - not networks, select the /32 CIDR. For more information about CIDR consult the Network Basics You Should Be Aware Of chapter (Page 13).

If the traffic accounting report is empty, check if the entered IP Address / Subnet is included in the selected WANGuard Sensor's IP Zone and that the “Accounting” parameter for that IP class is set to *Yes*.

Protocols Distribution Graphs

WANGuard Sensor systems configured with the “Top” option collect protocols distribution data. You can view this data by selecting Protocols Distribution from the Reports menu.

To generate Protocols Distribution graphs fill the following form.


WANGuard Console 3.1
Views
Archive
Reports
Setup
Help
ADMIN
Logout
» Protocols Distribution Graphs
18:03:53
Generate Protocols Distribution Graphs

Protocols Distribution Graph

From: 2008 July 27 00 : 00

Until: 2008 August 10 23 : 55

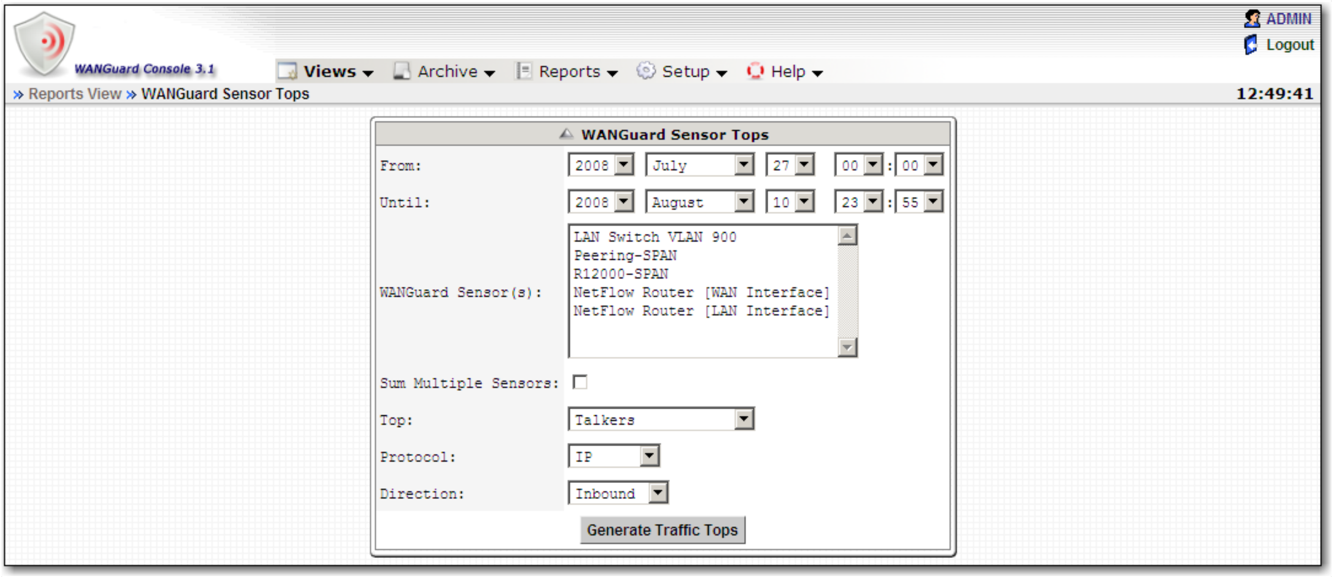
WANGuard Sensor(s): Peering-SPAN
R12000-SPAN
LAN Switch VLAN 900
NetFlow Router [WAN Interface]
NetFlow Router [LAN Interface]

Graph Size: 500x240

All fields are explained in the previous sections. Currently supported protocols are: SNMP, FTP, SSH, TELNET, SMTP, HTTP, POP3, IMAP, SQL, NETBIOS, IRC, DIRECTCONNECT, TORRENT, DNS, ICMP. Protocol detection is less reliable for applications that use non-standard, randomized source or destination ports.

WANGuard Sensor Tops

WANGuard Sensor systems configured with the "Top" option collect data that can be used to generate top statistics for any selected time-frame. Available statistics are: top hosts ("talkers"), top TCP ports, top UDP ports, top IP protocols and top AS Numbers (only when NetFlow is used). Top generation for large time-frames may take minutes. In this case edit the *max_execution_time* parameter from *php.ini* accordingly.



WANGuard Sensor Tops

From: 2008 July 27 00 : 00

Until: 2008 August 10 23 : 55

WANGuard Sensor(s): LAN Switch VLAN 900
Peering-SPAN
R12000-SPAN
NetFlow Router [WAN Interface]
NetFlow Router [LAN Interface]

Sum Multiple Sensors: □

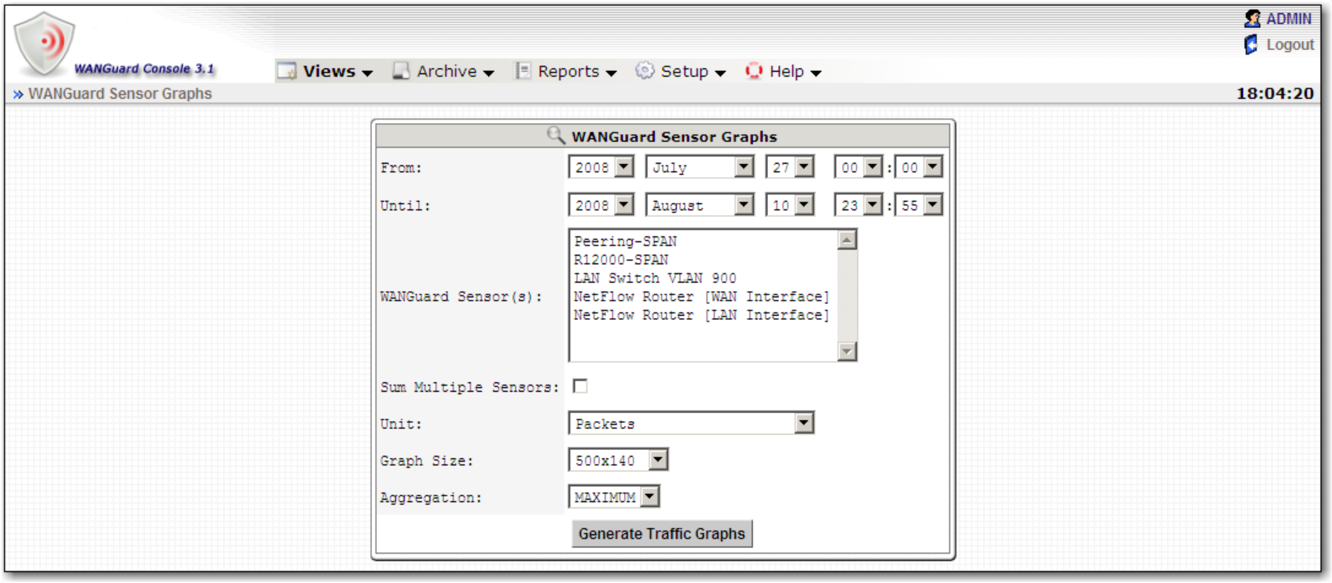
Top: Talkers

Protocol: IP

Direction: Inbound

WANGuard Sensor Graphs

WANGuard Console can generate on-demand MRTG-style graphs for WANGuard Sensor traffic parameters, for the selected time-frame. To generate WANGuard Sensor graphs you must fill the form below after selecting WANGuard Sensor Graphs from the Reports menu.



WANGuard Sensor Graphs

From:	2008 July 27 00 : 00
Until:	2008 August 10 23 : 55
WANGuard Sensor(s):	Peering-SPAN R12000-SPAN LAN Switch VLAN 900 NetFlow Router [WAN Interface] NetFlow Router [LAN Interface]
Sum Multiple Sensors:	□
Unit:	Packets
Graph Size:	500x140
Aggregation:	MAXIMUM

The WANGuard Sensor Graphs form fields:

- **From / Until**

  Enter the desired time-frame.

- **WANGuard Sensor(s)**

  Contains all configured WANGuard Sensor systems. Select the WANGuard Sensor that captured the traffic you're interested in. Multiple selections can be made by holding the Control key.

- **Sum Multiple Sensors**

  If unchecked, each WANGuard Sensor generates a different traffic graph. If checked, all selected WANGuard Sensors generate a single traffic graph that contains all traffic data.

- **Data Unit**

  Select the traffic parameter the graph will represent:

  - *Bits* - The bits/second throughput recorded by WANGuard Sensor.
  - *Bytes* - The bytes/second throughput recorded by WANGuard Sensor.

  - *Packets* - The packets/second throughput recorded by WANGuard Sensor.
  - *IPs* - The number of unique IP addresses detected making traffic. Usually a spike in the graph means that an IP class scan was performed. Only your network's IP addresses are counted.
  - *Received packets or flows* - For WANGuard Sniff it represents the rate of received packets before validation or filtering occurs. For WANGuard Flow it represents the rate of received flows before validation or filtering occurs.
  - *Dropped packets or flows* - For WANGuard Sniff it represents the rate of packets dropped in the capturing process. When the number is high it indicates a performance problem located in the network card, in the network card's driver, or in the CPU. It may also mean a bad WANGuard Sniff installation. For WANGuard Flow it represents the rate of flows dropped in the flow receiving process. When the number is high, it indicates a network problem between the flow exporter and the WANGuard Flow system, or a bad WANGuard Flow installation.
  - *Unknown packets or flows* - For WANGuard Sniff it represents the rate of discarded packets caused by validation or filtering. For WANGuard Flow it represents the rate of discarded flows caused by validation or filtering.

- **Graph Size**

  Select the size of the graph.

- **Aggregation**

  Select the aggregation procedure for the graph: *MINIMUM*, *MAXIMUM* or *AVERAGE*. If you are interested in traffic spikes, select the MAXIMUM aggregation type. If you are interested in average values, select the AVERAGE aggregation type. If you are interested in low traffic values, select the MINIMUM aggregation type.

WANGuard Flow ASN Graphs

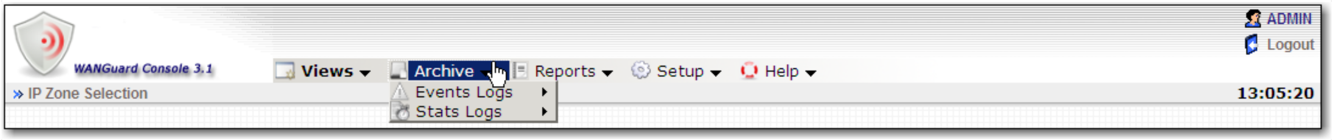
The WANGuard Flow ASN Graphs page will not be accessible through the Menu if there is no previously configured WANGuard Flow system.

WANGuard Flow systems configured with the “Top” option collect data that can be used to generate very accurate Autonomous System graphs for every detected Autonomous System Number. To use this option your flow exporter must be configured to include AS information in the exported flows.

You can generate graphs by ASN by entering one or more Autonomous System Numbers. If more then one ASN is entered, delimited by space, and if you check the **Sum Multiple ASNs** option, then a single graph will be generated containing data from all ASNs.

Archive

All WANGuard Lite components store traffic and operational details in a MySQL database located on the WANGuard Console server. You can view the contents of the database by selecting the tables from the Archive menu.



Events Logs

Events Logs contain all events generated by WANGuard Lite components. Each component that generates events is listed in a sub-menu. Each record has the following format:

System	The name or description of the WANGuard Lite component that generated the event.
Module	The module or internal function that generated the event.
Severity	Events are tagged with a severity value that describes the importance of the event. Severity levels descriptions are listed in the Managing Users chapter (Page 18).
Event	The text of the event.
Details	Some modules provide additional information in this field.
Date	The date and time when the notification was generated.

Stats Logs

Statistics Logs contain traffic statistics recorded by WANGuard Lite components. New rows are inserted every 5 seconds so expect lots of records. These logs are used only for debugging purposes and are not documented in this manual.

Help Menu

Contextual Help

The Contextual Help provides direct access to the WANGuard Lite User Guide. Depending on the context, the User Guide will open at the chapter describing the active window. If the Contextual Help does not work, please install Adobe PDF Reader on your computer.

AS Information

The AS Information windows provide access to an on-line ASN database (RIPE, ARIN, APNIC) and to a local ASN database.

IP Information

The IP Information windows provides details about IP addresses and domains, as well as web-based access to *ping*, *whois*, *traceroute* and *telnet* commands. IP information is contained in an internal database that contains IP ranges, Country codes and Autonomous System information.

IP Protocols

The IP Protocols window provides access to a table that contains descriptions for all available IPv4 protocols.

Subnet Calculator

The Subnet Calculator lets you see and calculate network masks, CIDR, broadcast addresses, number of hosts and IP ranges for subnets.

TCP&UDP Ports

The TCP&UDP Ports window provides access to a table that contains name, description, service, common servers and common clients for well known TCP and UDP port numbers.

About...

The About window provides information about the WANGuard version and license. The license key can be changed from this window.

Appendix 1 – 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 Cisco 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 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 linecards 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 your WANGuard Flow server and the configured listening port. UDP port 2000 is used as an example. WANGuard Flow is using NetFlow version 5. 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. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

```
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 your WANGuard Flow server 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. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

```
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 then 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. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

```
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:

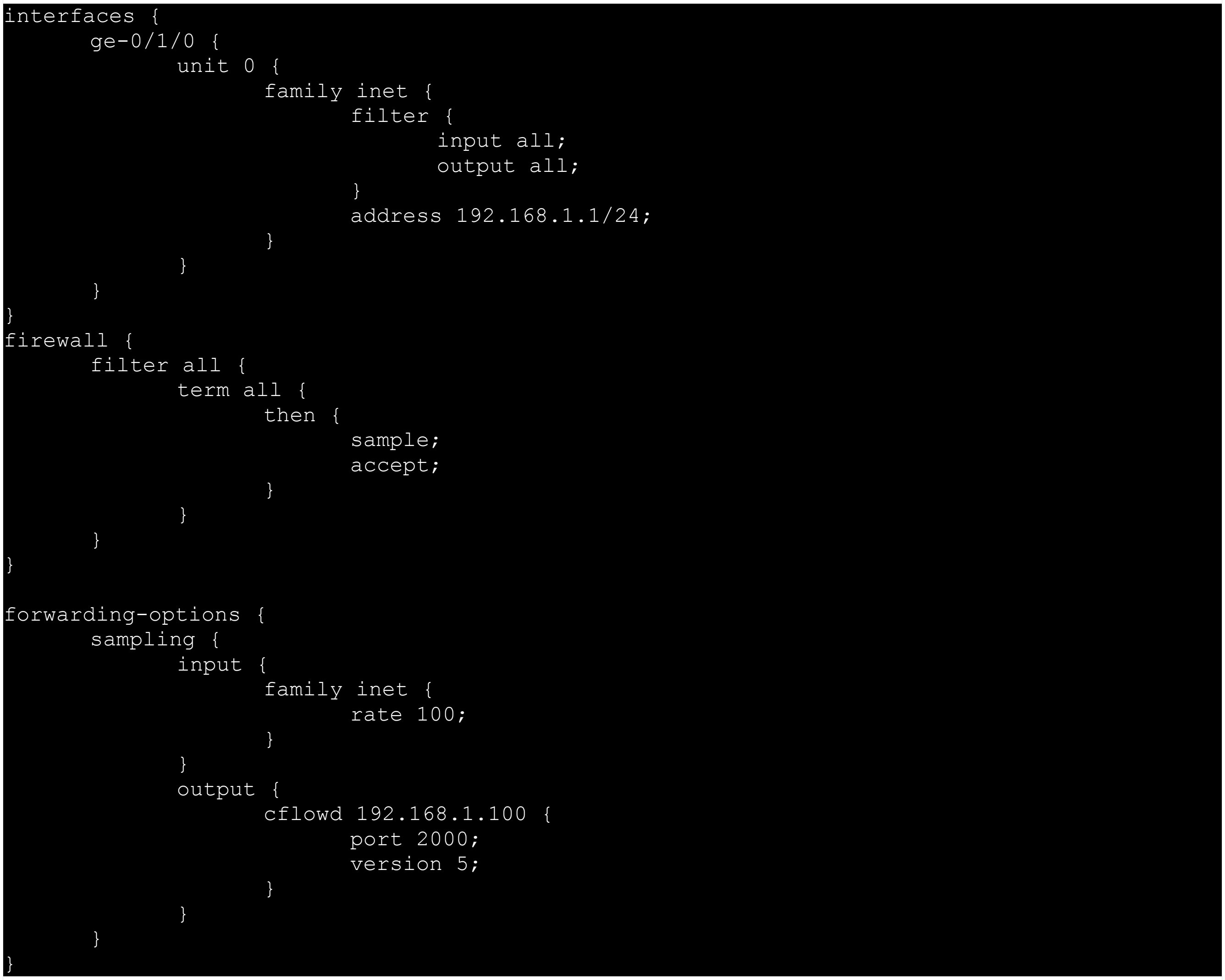
```
switch(config)# mls flow ip interface-full
switch(config)# mls nde interface
```

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

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;
                        }
                }
        }
}
```