



WANGuard Platform 3.1

User Manual

WANGuard Console + WANGuard Sensor + WANGuard Filter

Copyright & trademark notices

This edition applies to version 3.1 of the licensed program WANGuard Platform 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

© ANDRISOFT S.R.L. 2008. All rights reserved.

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

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

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

© Copyright ANDRISOFT S.R.L. 2008. All rights reserved.

Table of Contents

1. Traffic Monitoring & Accounting, DoS / DDoS Detection & Protection with WANGuard™ Platform.....	5
Why WANGuard™ Platform Is Important.....	5
What WANGuard™ Platform Can Do For You.....	5
WANGuard™ Platform Components.....	6
WANGuard Sensor.....	6
WANGuard Filter.....	7
WANGuard Console.....	8
2. How To Choose A Method Of Traffic Capturing.....	9
Supported Traffic Capturing Methods.....	9
Port Mirroring (Switched Port Analyzer - SPAN, Roving Analysis Port), Network TAP, In-line deployment.....	9
How Port Mirroring, Network TAP, In-line Deployment works	10
Reasons to choose Port Mirroring, Network TAP, In-line Deployment.....	10
NetFlow® Monitoring.....	10
How NetFlow® Monitoring Works.....	10
Reasons to choose NetFlow® Monitoring	11
Comparison between Packet Sniffing and NetFlow® Monitoring.....	11
3. Installation.....	12
System Requirements.....	12
WANGuard Sensor System Requirements for 1 Gigabit Network Interface.....	12
WANGuard Filter System Requirements for 1 Gigabit Network Interface.....	13
WANGuard Console System Requirements for < 5 WANGuard Sensors and WANGuard Filters.....	14
Download	14
Software Installation.....	15
4. Network Basics You Should Be Aware Of.....	16
Who Should Read This Section.....	16
A Short Introduction To IP Addresses & Classes.....	16
IP Addresses.....	16
IP Classes.....	17
Subnet CIDR Notation.....	18
5. Getting Started with WANGuard™ Platform.....	19
Basic Concepts.....	19
Menu Bar.....	19
Views.....	19
Tables.....	20
IP Zones	20
Actions.....	20
Opening WANGuard Console for the first time.....	20
A First Look at the Systems View.....	21
Managing WANGuard Console Users.....	22
6. Actions Setup.....	25
Understanding Actions.....	25
Adding New Action.....	25
Action Renaming & Deleting.....	26
Adding New Action Modules.....	27
Action Modules Common Fields, Conditional & Dynamic Parameters	27
WANGuard Filter Enabler Action Module.....	28
BGP Announcement Action Module.....	28

WANGuard Sensor Email Action Module.....	29
WANGuard Sensor Script Action Module.....	30
WANGuard Sensor Syslog Action Module.....	30
WANGuard Filter Email Action Module.....	31
WANGuard Filter Script Action Module.....	32
WANGuard Filter Syslog Action Module.....	33
7. IP Zones Setup.....	35
Understanding IP Zones.....	35
Inheritance.....	36
IP Zone Selection.....	36
Adding a new IP Zone.....	37
Changing Description, Copying & Deleting IP Zones.....	37
IP Zone Configuration.....	38
Inbound and Outbound Traffic Thresholds.....	39
Accounting.....	40
Graphing.....	40
Concurrency	41
Description.....	41
Thresholds Templates.....	41
IP Zone Configuration Example.....	42
8. WANGuard Sensor Setup.....	46
WANGuard Sniff Configuration.....	46
WANGuard Flow Configuration.....	50
9. WANGuard Filter Setup.....	55
WANGuard Filter Configuration.....	55
WANGuard Filter Whitelists.....	59
10. BGP Router Setup.....	61
BGP Router Selection.....	61
BGP Router Configuration.....	62
11. Views.....	64
Systems View.....	64
Active WANGuard Sniff Systems Table.....	65
Active WANGuard Flow Systems Table.....	66
Active WANGuard Filter Systems Table.....	67
WANGuard Sensor Live Graphs Tab.....	68
Events Tab.....	68
Reports View.....	69
WANGuard Sensors Section.....	69
IP Descriptions Section.....	70
IP Addresses Section.....	71
Security View.....	72
Current Traffic Anomalies.....	73
Past Traffic Anomalies.....	74
BGP Operations.....	75
12. Traffic Accounting and Graphing.....	77
IP Traffic Graphs Setup.....	77
IP Traffic Graphs.....	78
By IP Description.....	79
By IP Address / Subnet.....	80
IP Traffic Accounting.....	80

By IP Description.....	81
By IP Address / Subnet.....	82
Protocols Distribution Graphs.....	82
WANGuard Sensor Tops	83
WANGuard Sensor Graphs	84
WANGuard Flow ASN Graphs	85
13. Archive	86
Anomaly Logs.....	86
BGP Logs.....	87
Events Logs.....	88
Filter Logs.....	88
Attacks Patterns.....	89
WANGuard Filters.....	90
Stats Logs.....	90
14.Help Menu.....	91
Contextual Help.....	91
AS Information	91
IP Information.....	91
IP Protocols.....	91
Subnet Calculator.....	91
TCP&UDP Ports.....	91
About.....	91
15.Appendix 1 – Configuring NetFlow Data Export.....	92
Configuring NDE on an IOS Device.....	92
Configuring NDE on a CatOS Device.....	93
Configuring NDE on a Native IOS Device.....	94
Configuring NDE on a 4000 Series Switch.....	94
Configuring NDE on a Juniper Router.....	94
16.Appendix 2 – Conditional & Dynamic Parameters.....	96
17.Appendix 3 – Configuring Traffic Diversion.....	99
Understanding the BGP Diversion Method.....	99
BGP Configuration Guidelines.....	100
WANGuard Filter System BGP Configuration.....	100
WANGuard Filter System BGP Configuration Example.....	102
Cisco Router BGP Configuration.....	102
Cisco Router BGP Configuration Example.....	103
Understanding Traffic Forwarding Methods.....	103
Static Routing – Layer 2 Forwarding Method.....	104
GRE / IP over IP Tunneling – Layer 3 Forwarding Method.....	104
Configuring Static Routing – Layer 2 Forwarding Method.....	104
Configuring GRE / IP over IP Tunneling – Layer 3 Forwarding Method.....	104

Traffic Monitoring & Accounting, DoS / DDoS Detection & Protection with WANGuard™ Platform

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

What WANGuard™ Platform Can Do For You

Andrisoft WANGuard Platform is an easy to use software platform that provides network traffic monitoring, network traffic accounting and network protection against DoS, DDoS and DrDoS attacks.

It allows you to quickly and easily set up and run monitoring and filtering 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.)
- Historic and real-time recordings about the sources and destinations that use bandwidth above the acceptable limits
- Per endpoint insightful report analytics and audit trail analysis for detected traffic anomalies
- Historic and real-time information about DoS, DDoS and DrDoS attacks in your network

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™ Platform Components

The WANGuard Platform has three main components:

WANGuard Sensor

WANGuard Sensor is an advanced Linux-based software created to do both incoming and outgoing traffic monitoring and analysis. 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 Sensor also has traffic anomalies detection and reaction capabilities, and when used together with WANGuard Filter it can provide complete network protection against DoS,DDoS and DrDoS attacks.

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
- Detects traffic anomalies and provides per endpoint flexible threat management tools and an easy to use API for configuring the reaction to traffic anomalies:
 - activate WANGuard Filter for DoS / DDoS / DrDoS mitigation or additional threat information
 - alert the NOC Staff by email using user-defined email templates
 - send custom syslog messages to remote log servers
 - send BGP announcements for blackholing targeted endpoints
 - execute custom scripts that extend the built-in capabilities, such as:

- configure ACLs or execute PIX "shun" commands to drop traffic towards targeted endpoints
- send SNMP TRAP messages to SNMP monitoring stations
- display the routers that are being transited by the anomalous traffic
- Includes a very flexible billing system for bandwidth based billing
- Easy and non-disruptive installation on common server hardware
- The most cost-effective traffic monitoring and analysis solution on the market

WANGuard Filter

WANGuard Filter is an advanced Linux-based software designed to protect organizations from internal and external threats (availability attacks on DNS, VoIP, Mail and similar services, unauthorized traffic resulting in network congestion), botnet-based attacks, zero-day worm and virus outbreaks. WANGuard Filter includes sophisticated traffic analysis algorithms that are able to detect and filter the attack patterns contained in the malicious traffic, while re-injecting the cleaned traffic back into the network.

WANGuard Filter Features and Benefits:

- Quickly see detailed live and historical information about traffic anomalies in your network from any location by accessing WANGuard Console with your web browser
- Defends against known, unknown and evolving attack patterns
- Recognizes and filters malicious traffic in under 5 seconds
- Does not block / blacklist valid customer traffic
- WANGuard Filter can be deployed in-line or out-of-line by diverting the malicious traffic towards the server running it. The cleaned traffic can be re-injected back to the network using Static Routing or GRE / IPIP tunneling
- Provides per endpoint flexible threat management tools and an easy to use API for configuring the reaction to attack patterns:
 - alert the NOC Staff by email using user-defined email templates
 - alert the ISPs of the attackers via email using user-defined email templates
 - send custom syslog messages to remote log servers
 - execute custom scripts that extend the built-in capabilities, such as:
 - configure ACLs or execute PIX "shun" commands to filter attack patterns
 - filter attacking IP addresses by executing "route blackhole" commands
 - send SNMP TRAP messages to SNMP monitoring stations

- Does not require network baseline training and operator intervention after the initial setup
- Easy and non-disruptive installation on common server hardware
- The most cost-effective DoS / DDoS / DrDoS protection and traffic policy enforcement 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 network protection. 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 and WANGuard Filter systems deployed within the network.

WANGuard Console Features and Benefits:

- Consolidated, real-time WANGuard Sensor and WANGuard Filter 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 analysis, **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 want the quickest reaction to traffic anomalies (under 5 seconds) and 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 Anomalies Detection Time	< 5 seconds	< flow export time + 5 seconds
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 Platform 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 Platform 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 and protected immediately. No baseline data gathering is required.

System Requirements

WANGuard Platform 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 Platform architecture is completely **scalable**. By installing the software on better hardware, the number of monitored and protected endpoints and networks increases. All WANGuard Platform 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 92).

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 Filter System Requirements for 1 Gigabit Network Interface

Architecture	x86 (32 or 64 bit)
CPU	1 x Xeon 2.5 GHz or 1 x Opteron 1.8 GHz
Memory	500 MBytes
Network Cards	2 x Gigabit Ethernet (NAPI support strongly recommended)
Operating System	Linux kernel 2.6.x
Installed Packages	perl 5.x quagga or zebra Net::Telnet iptables mysql 5.x perl-DBD-MySQL tcpdump WANGuard-Filter 3.1 WANGuard-BGPSupport 3.1 WANGuard-Controller 3.1
Disk Space	5GB (including OS)

WANGuard Filter can be deployed in-line or it must have access to an BGP router that can be used to divert the malicious traffic towards the server running it. For sending BGP announcements WANGuard Filter uses the free, open-source quagga or zebra routing software. For more information about configuring quagga or zebra and your network devices for traffic diversion please consult Appendix 3 – Configuring Traffic Diversion (page 99).

Having a dedicated filtering server for each monitored link is not always required. You can deploy a single filtering server that will protect multiple links, as long as you can re-route the traffic towards it and re-inject the cleaned traffic to a downstream router. For very large networks, a dedicated filtering server for each upstream link is highly recommended.

WANGuard Console System Requirements for < 5 WANGuard Sensors and WANGuard Filters

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

Binary WANGuard Platform 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 Platform 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 Platform 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™ Platform

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 Platform 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 four different types of Views:

- **Security View**

Displays the latest traffic anomalies detected by WANGuard Sensor systems, and live information about DoS,DDoS and DrDoS attacks mitigated by WANGuard Filter systems. On the bottom section it displays tabbed live traffic graphs, events, WANGuard Sensor and WANGuard Filter information.

- **Systems View**

Displays a table with live information about all running WANGuard Sensor and WANGuard Filter 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.

- **BGP Operations**

BGP Operations lets you manage iBGP and eBGP announcements. Manual removal of BGP announcements is only available to Administrator accounts.

More information about Views is available on the Views chapter (page 64).

Tables

All WANGuard Platform 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, inbound and outbound traffic thresholds, and what Action should be activated when an inbound or outbound traffic anomaly is detected.

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

Actions

Actions provide an unique and powerful way to automate reaction to traffic anomalies and attack patterns. An Action contains a collection of Action Modules that WANGuard Sensor and WANGuard Filter execute during the reaction phase of a traffic anomaly or DoS / DDoS / DrDoS attack.

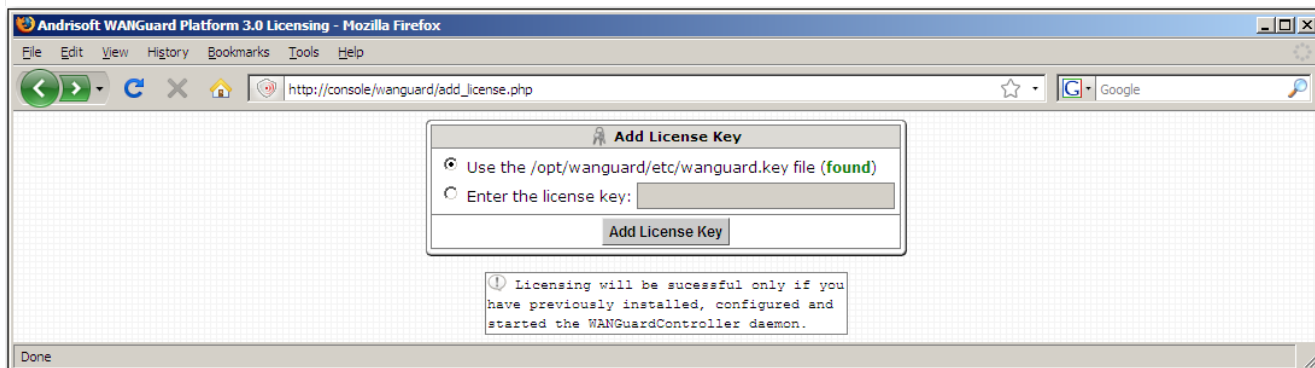
Every IP class monitored and defined in the current IP Zone, may have it's own Action configured. If a traffic threshold for an IP address is reached then the defined Action for that IP's IP class is triggered.

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 14) 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.

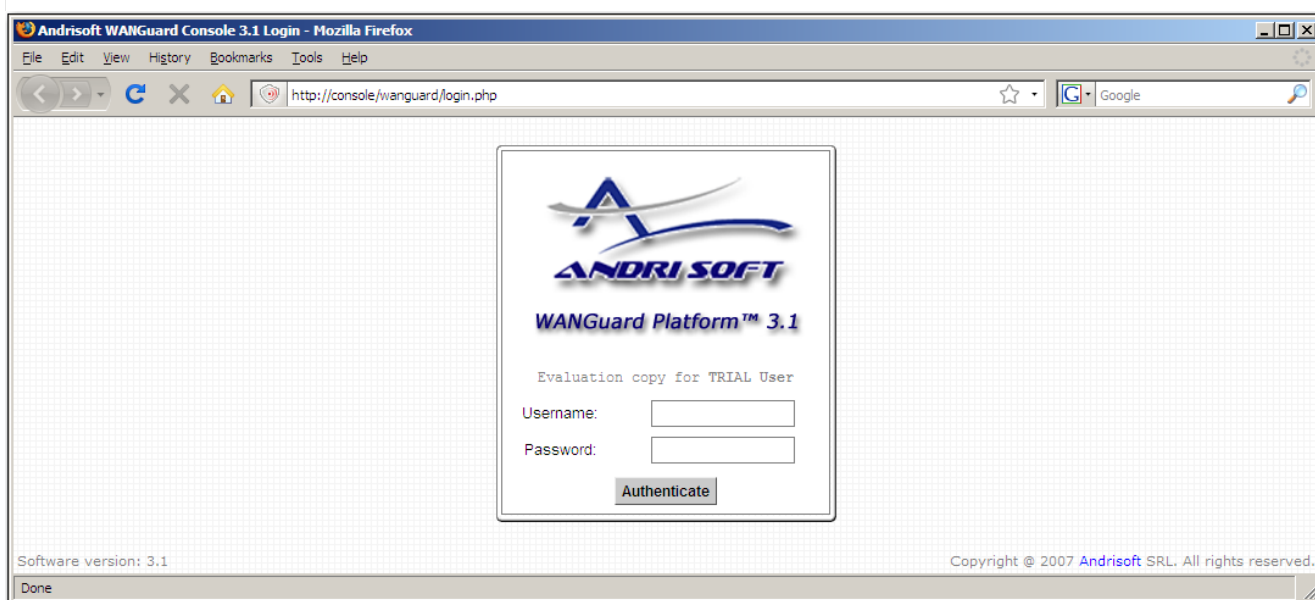
If you haven't licensed WANGuard Platform yet, you will be asked to do so:



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**.



A First Look at the Systems View

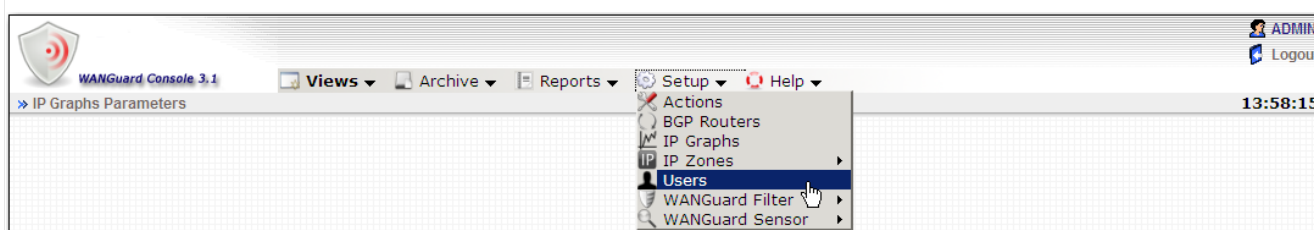
Immediately after logging into WANGuard Console, the layout of the Systems View will be displayed.

You can change the default View by editing your User preferences.

Because no WANGuard Sensor or WANGuard Filter 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 64).

You can navigate throughout WANGuard Console using the drop-down menu located in the upper side of every page.

Managing WANGuard Console Users

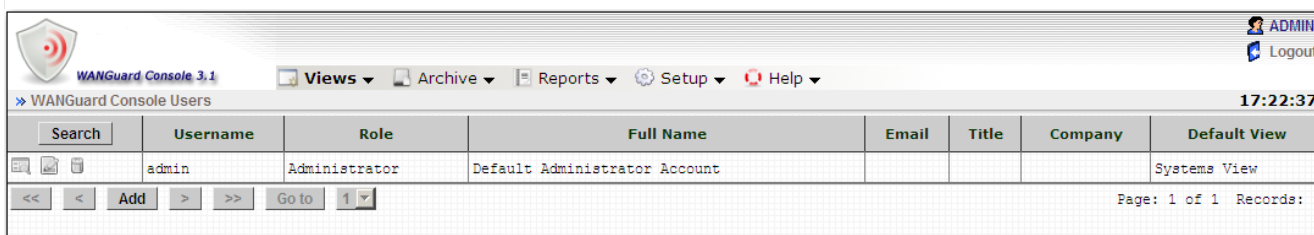


If you install WANGuard Console on a publicly available server, you should immediately change the default password for the **admin** user, and eventually add new users. To manage WANGuard Console users you must select Users from the Setup menu. A list of existing users will be displayed.

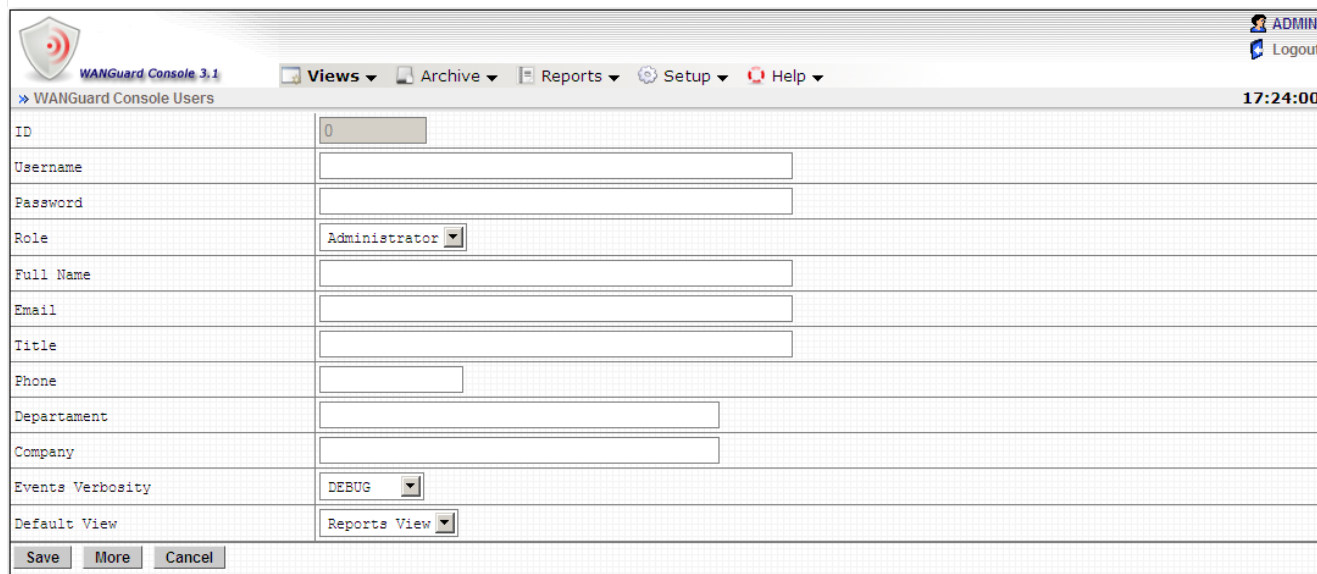
To **view** additional information about a user you must click the first icon in the first column.

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.



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



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 and WANGuard Filter configurations nor can it add or delete BGP announcements and users.
- **Administrator** - The user has all privileges to view and manage WANGuard Platform 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 Security View and 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 Platform 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.
- *Security View* - recommended for IT security engineers.
- *BGP Operations* - recommended for BGP operators.

Actions Setup

Understanding Actions

Actions provide a unique and powerful way to automate the reaction to traffic anomalies and attack patterns. An Action is a collection of commands executed by WANGuard Sensor and WANGuard Filter during the reaction phase of a traffic anomaly or DoS / DDoS / DrDoS attack.

As explained in the Basic Concepts chapter, every IP class monitored and defined in the current IP Zone, may have its own Action configured. When a traffic threshold value defined for an IP is reached, the defined Action for the IP's IP class is executed by WANGuard Sensor and, if installed and activated, by WANGuard Filter.

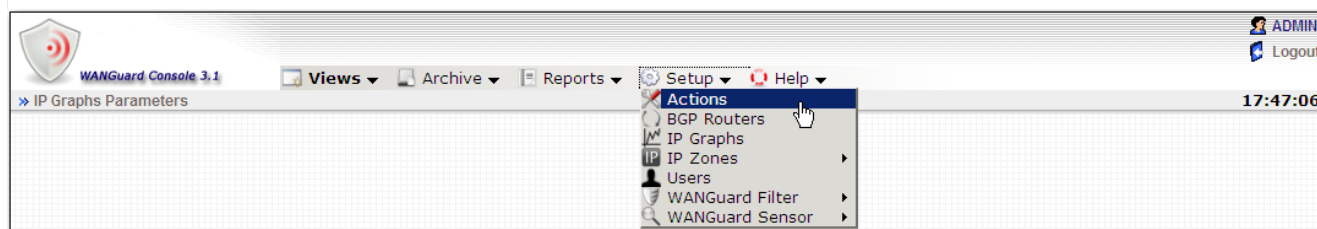
Every Action runs the contained Action Modules. Action Modules provide means to execute commands, send notifications, write logs and more. There are two types of Action Modules:

- **WANGuard Sensor Action Modules** are predefined commands that are executed by the WANGuard Sensor system that detected the traffic anomaly, while the traffic anomaly is active.
- **WANGuard Filter Action Modules** are predefined commands that are executed by the WANGuard Filter system activated to mitigate the traffic anomaly, while attack patterns are detected.

The Action Modules are executed in three situations, each having its own branch in the Action tree:

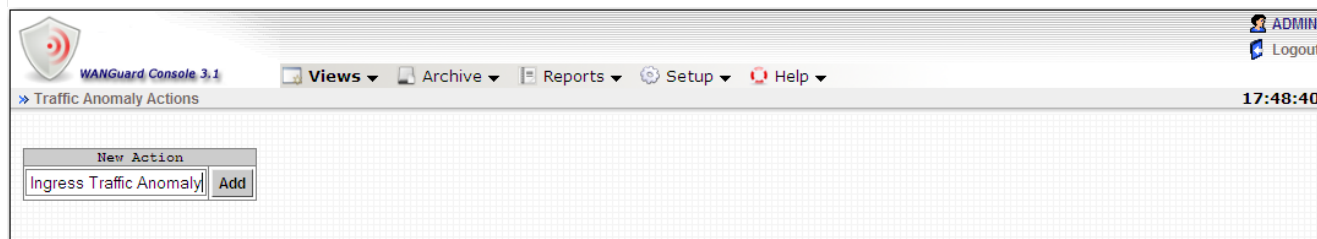
- **Beginning** - Action Modules added to this branch are executed once, immediately after the traffic anomaly or attack pattern has been detected.
- **Polling** - Action Modules added to this branch are executed periodically, every 5 seconds, while the traffic anomaly or attack pattern is active. A Polling Action Module can be configured to run only once, by checking the RunOnce checkbox, usually when used together with Preconditions.
- **Ending** - Action Modules added to this branch are executed once, after 5 minutes of traffic anomaly inactivity or after the attack pattern timeout occurs.

Adding New Action

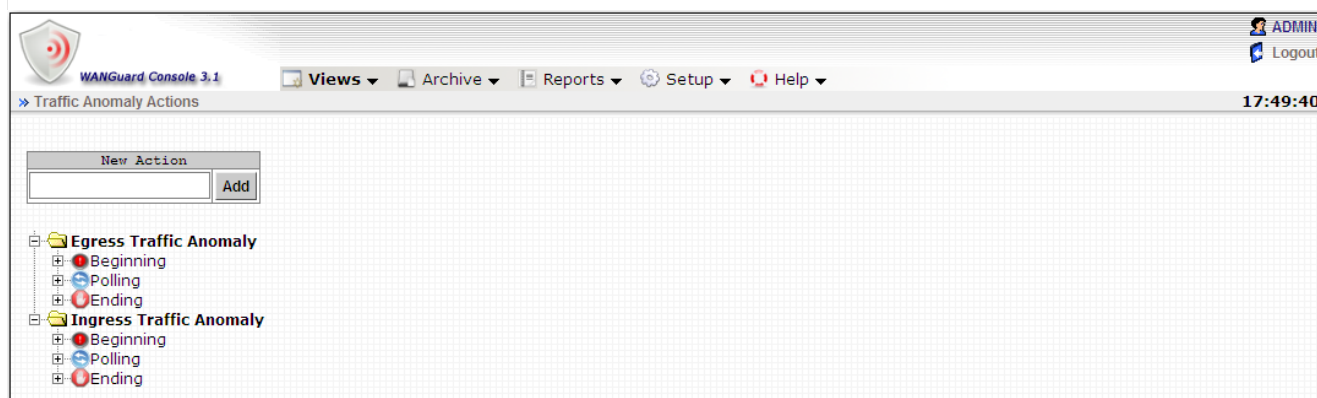


When you select Actions from the Setup menu, the Actions configuration window will be displayed. Existing Actions are listed in the left section of the window, in a hierarchical structure, where every Action has it's own Beginning, Polling and Ending branches (explained in the previous paragraph).

To add a new Action you must first enter a generic description in the New Action form found in the top left part of the window, and click <Add>.



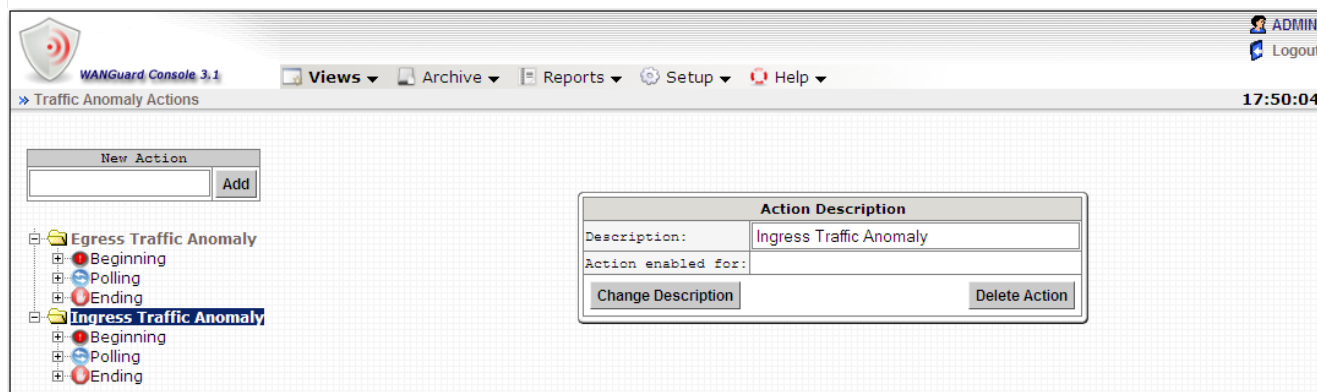
After the <Add> button is clicked, the left section will change to include the new Action. In the following example we added two Actions: "Ingress Traffic Anomaly" and "Egress Traffic Anomaly".



Action Renaming & Deleting

To delete or rename an Action you must select the Action name in the left section.

On the right side you will see what IP Zones and IP classes are currently configured to use the selected Action. The left arrow indicates that the Action was defined for Outbound traffic anomalies and the right arrow indicates that the Action was defined for Inbound traffic anomalies.



Adding New Action Modules

To add a new Action Module, you must first decide whether you want the Action Module to be executed at the beginning, during, or at the end of a traffic anomaly or attack pattern. Then expand the corresponding branch and click Add.

If WANGuard Filter is not installed or the existing licensing option does not include it, the WANGuard Filter Action Modules will not be available.

Action Modules Common Fields, Conditional & Dynamic Parameters

All Action Modules have the following common fields:

- *Active* – selects if the Action Module is enabled or disabled.
- *Priority* – selects the order of execution relative to the other Action Modules that are defined within the same branch. Lower numerical values correspond to increased priority.
- *Description* – a generic description of the Action Module.
- *Preconditions* – let's the user define the rules that must be validated before the Action Module is executed.

Preconditions provide a way for Conditional Parameters to be validated against user defined values. If the validation is unsuccessful then the Action Module is not executed.

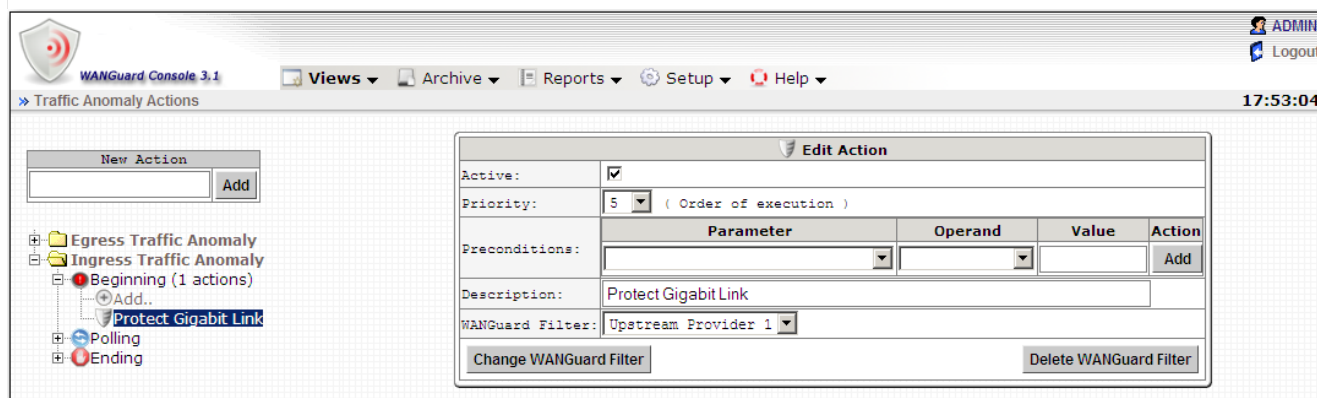
Conditional Parameters are dynamic, internal parameters that are updated every 5 seconds by WANGuard Sensor and WANGuard Filter systems. A complete list of Conditional Parameters is available in Appendix 2 – Conditional & Dynamic Parameters (Page 96).

Dynamic Parameters are parameters defined within curly brackets - { and } that can be included in the body of most Action Modules. Every Conditional Parameter has a correspondence with a Dynamic Parameter.

One very special type of Conditional Parameter is called Unique Dynamic Parameter. Basically what Unique Dynamic Parameters do, is to check if no other WANGuard Sensor exports the same Unique Dynamic Parameters. Using this property, it becomes possible to resolve conflicts between WANGuard Sensor systems when two or more WANGuard Sensors systems analyze some common traffic, especially in redundant configurations.

WANGuard Filter Enabler Action Module

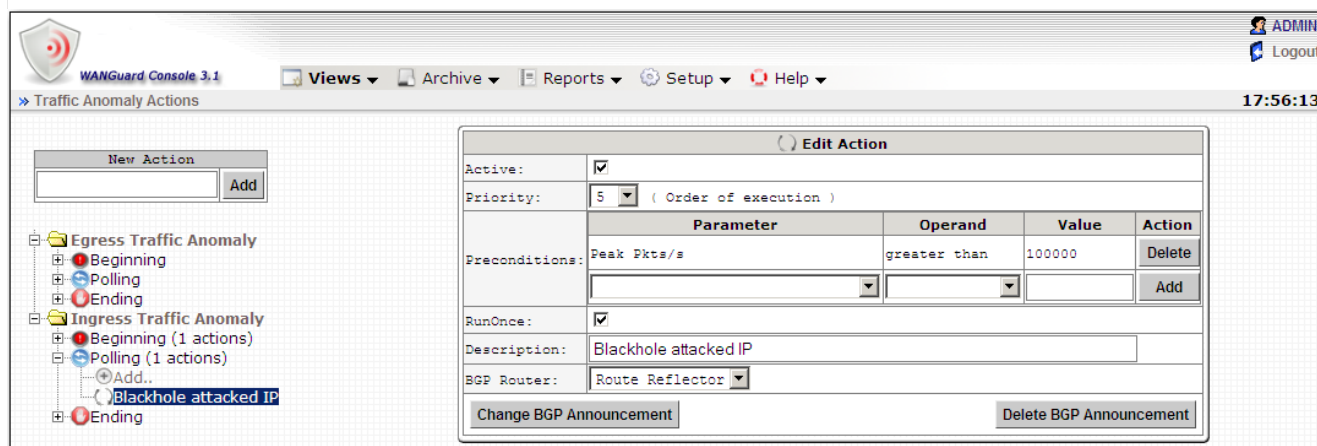
The WANGuard Filter Enabler Action Module is used by WANGuard Sensor to activate a WANGuard Filter for mitigation purposes. This module should be activated at the beginning of a traffic anomaly, or while polling the traffic anomaly if you check the *RunOnce* checkbox and use Preconditions (to check if the traffic anomaly's severity is big enough for example).



The screenshot shows the WANGuard Console 3.1 interface. On the left, a tree view shows 'Ingress Traffic Anomaly' with 'Beginning (1 actions)' and 'Polling'. The 'Edit Action' module is active, showing the following details:

- Active:** ☒
- Priority:** 5 (Order of execution)
- Preconditions:** A table with columns: Parameter, Operand, Value, Action. The first row is empty, and the second row has 'Add' in the Action column.
- Description:** Protect Gigabit Link
- WANGuard Filter:** Upstream Provider 1
- Buttons:** Change WANGuard Filter, Delete WANGuard Filter

BGP Announcement Action Module



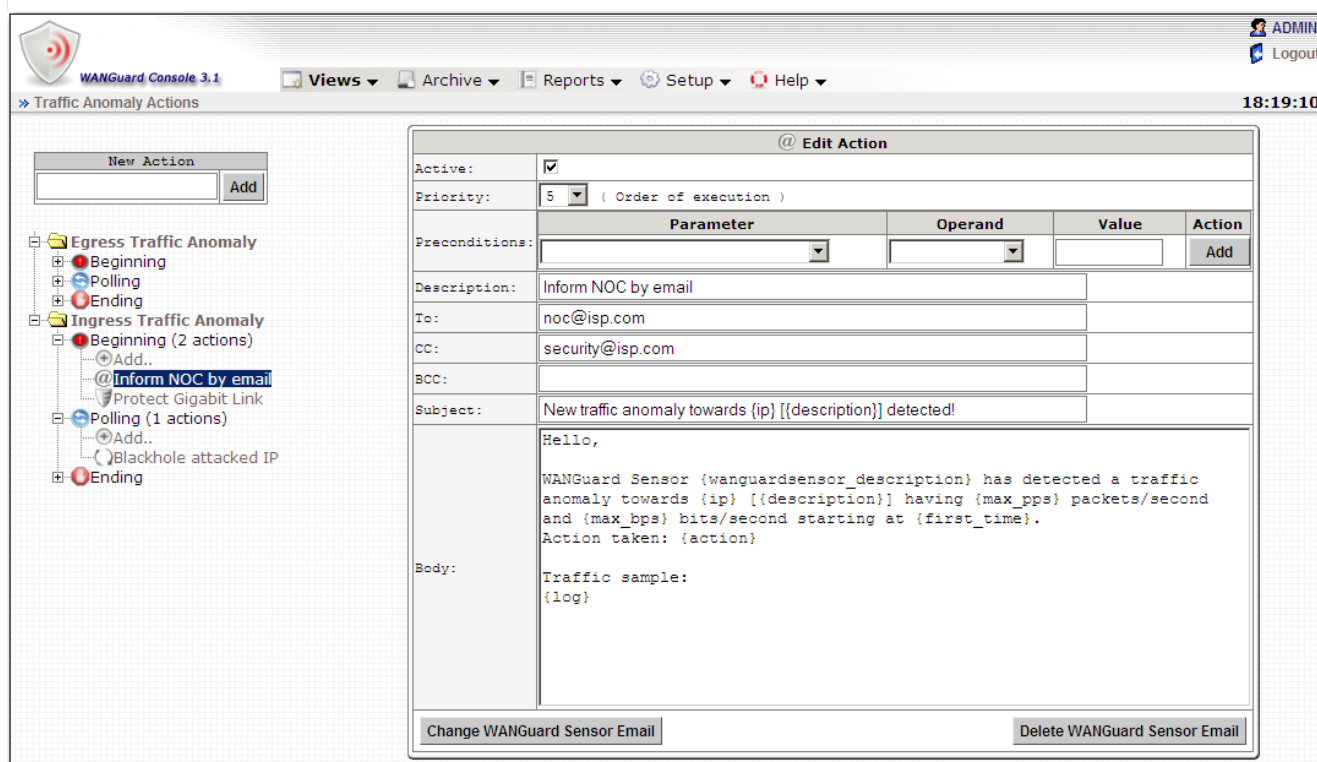
The screenshot shows the WANGuard Console 3.1 interface. On the left, a tree view shows 'Ingress Traffic Anomaly' with 'Beginning (1 actions)', 'Polling (1 actions)', and 'Blackhole attacked IP'. The 'Edit Action' module is active, showing the following details:

- Active:** ☒
- Priority:** 5 (Order of execution)
- Preconditions:** A table with columns: Parameter, Operand, Value, Action. The first row has 'Peak Pkts/s', 'greater than', '100000', and 'Delete'. The second row has 'Add' in the Action column.
- RunOnce:** ☒
- Description:** Blackhole attacked IP
- BGP Router:** Route Reflector
- Buttons:** Change BGP Announcement, Delete BGP Announcement

This module is used by WANGuard Sensor to send a BGP announcement with the traffic anomaly's IP address. The BGP announcement will be automatically removed at the end of the traffic anomaly. More information can be found in the BGP Router Setup chapter (Page 61).

WANGuard Sensor Email Action Module

This module is used by WANGuard Sensor to send notification emails at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of a traffic anomaly.



The screenshot shows the WANGuard Console 3.1 interface. On the left, a tree view shows the configuration structure under 'Traffic Anomaly Actions', including 'Egress Traffic Anomaly' and 'Ingress Traffic Anomaly'. The 'Ingress Traffic Anomaly' section is expanded, showing 'Beginning (2 actions)', 'Polling (1 actions)', and 'Ending'. The 'Beginning' branch is selected, and the 'Inform NOC by email' action is highlighted.

The main area displays the 'Edit Action' configuration for the selected action. The configuration includes the following fields:

- Active:** ☒
- Priority:** 5 (Order of execution)
- Preconditions:** A table with columns: Parameter, Operand, Value, and Action. The 'Add' button is visible.
- Description:** Inform NOC by email
- To:** noc@isp.com
- CC:** security@isp.com
- BCC:**
- Subject:** New traffic anomaly towards {ip} [{description}] detected!
- Body:**

```

Hello,

WANGuard Sensor {wanguardsensor_description} has detected a traffic
anomaly towards {ip} [{description}] having {max_pps} packets/second
and {max_bps} bits/second starting at {first_time}.
Action taken: {action}

Traffic sample:
{log}

```

At the bottom, there are two buttons: 'Change WANGuard Sensor Email' and 'Delete WANGuard Sensor Email'.

The *Subject* and *Body* fields can contain any number of WANGuard Sensor Dynamic Parameters. Dynamic Parameters are explained at the beginning of the chapter. A complete list of Dynamic Parameters available can be found on Appendix 2 – Conditional & Dynamic Parameters (Page 96).

The emails are sent through the local SMTP server (sendmail, postfix, qmail etc.) of the WANGuard Console system using the perl Mail::Send module. By default, the sender will be <WANGuard@localhost.localdomain>. For sender customizations (From field) please consult your SMTP server documentation.

Every email sent by this module is recorded in the Anomaly Logs (Page 86).

WANGuard Sensor Script Action Module

This module is used by WANGuard Sensor to execute custom scripts written in any Linux compatible scripting languages such as bash, perl, ruby, python etc. C and C++ programs or Linux commands can also be executed. The scripts can be executed at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of a traffic anomaly.

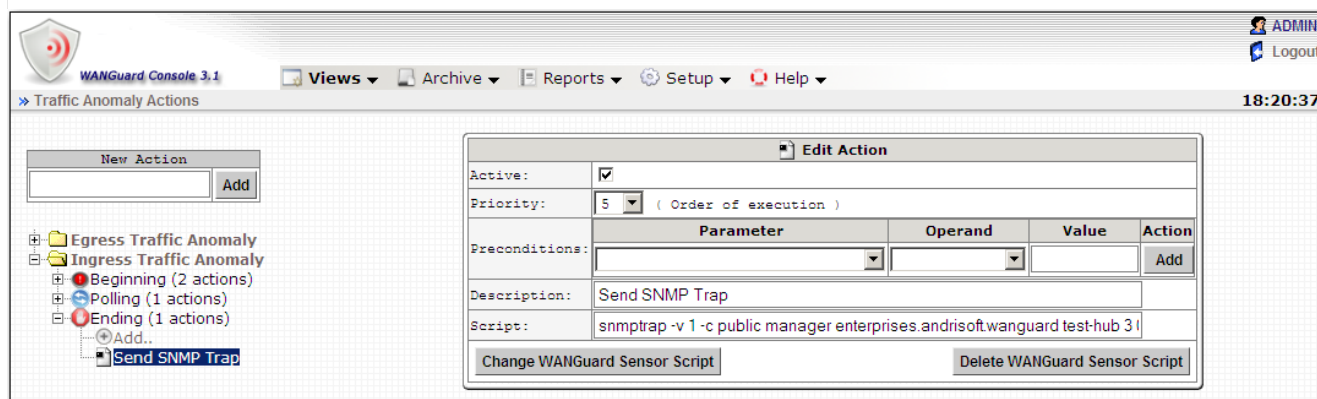
Scripts can access WANGuard Sensor Dynamic Parameters through command-line parameters / options. The scripts are executed locally on each WANGuard Sensor system that uses Actions that include this module. Multiple commands can be executed using the “;” separator.

Scripts executed through the WANGuard Sensor Action Module have the user privileges of the “wanguard” system account. To elevate privileges for your scripts you should use the *sudo* prefix, after editing the */etc/sudoers* file.

Some possible uses of this module:

- configure ACLs or execute PIX "shun" commands to drop traffic towards attacked IPs
- send SNMP TRAP messages to SNMP monitoring stations
- display the routers that are being transited by the anomalous traffic using third-party software

The image below shows a simple module configuration used to send SNMP TRAP messages to a SNMP monitoring station.



The screenshot displays the WANGuard Console 3.1 interface. On the left, a tree view shows the configuration structure: Egress Traffic Anomaly, Ingress Traffic Anomaly, Beginning (2 actions), Polling (1 actions), and Ending (1 actions). The 'Send SNMP Trap' action is selected under the 'Ending' branch. The main area shows the 'Edit Action' configuration for this action.

Parameter	Operand	Value	Action
Active:	<input checked="" type="checkbox"/>		
Priority:	5	(Order of execution)	
Preconditions:			Add
Description:	Send SNMP Trap		
Script:	snmptrap -v 1 -c public manager enterprises.andrisoft.wanguard test-hub 3 l		

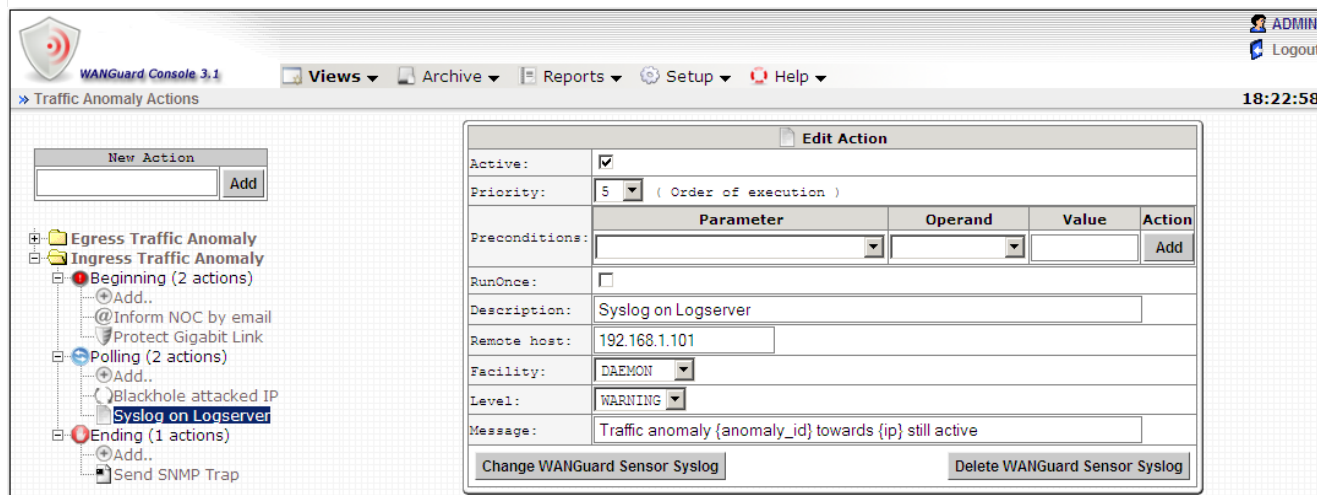
Buttons at the bottom: Change WANGuard Sensor Script, Delete WANGuard Sensor Script

WANGuard Sensor Syslog Action Module

This module is used by WANGuard Sensor to send syslog messages locally, or to remote syslog monitoring stations. To send syslog messages you must enter the IP address of the syslog server (127.0.0.1 for localhost), select the desired facility, severity level and message content. Syslog messages can be sent at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of a traffic anomaly.

The message field can contain any number of WANGuard Sensor Dynamic Parameters.

A configuration example of this module is shown in the image below.



WANGuard Filter Email Action Module

This module is used by WANGuard Filter to send notification emails at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of an attack pattern.

The *Subject* and *Body* fields can contain any number of WANGuard Sensor and WANGuard Filter Dynamic Parameters. Dynamic Parameters are explained at the beginning of the chapter. A complete list of Dynamic Parameters available can be found in Appendix 2 – Conditional & Dynamic Parameters (Page 96).

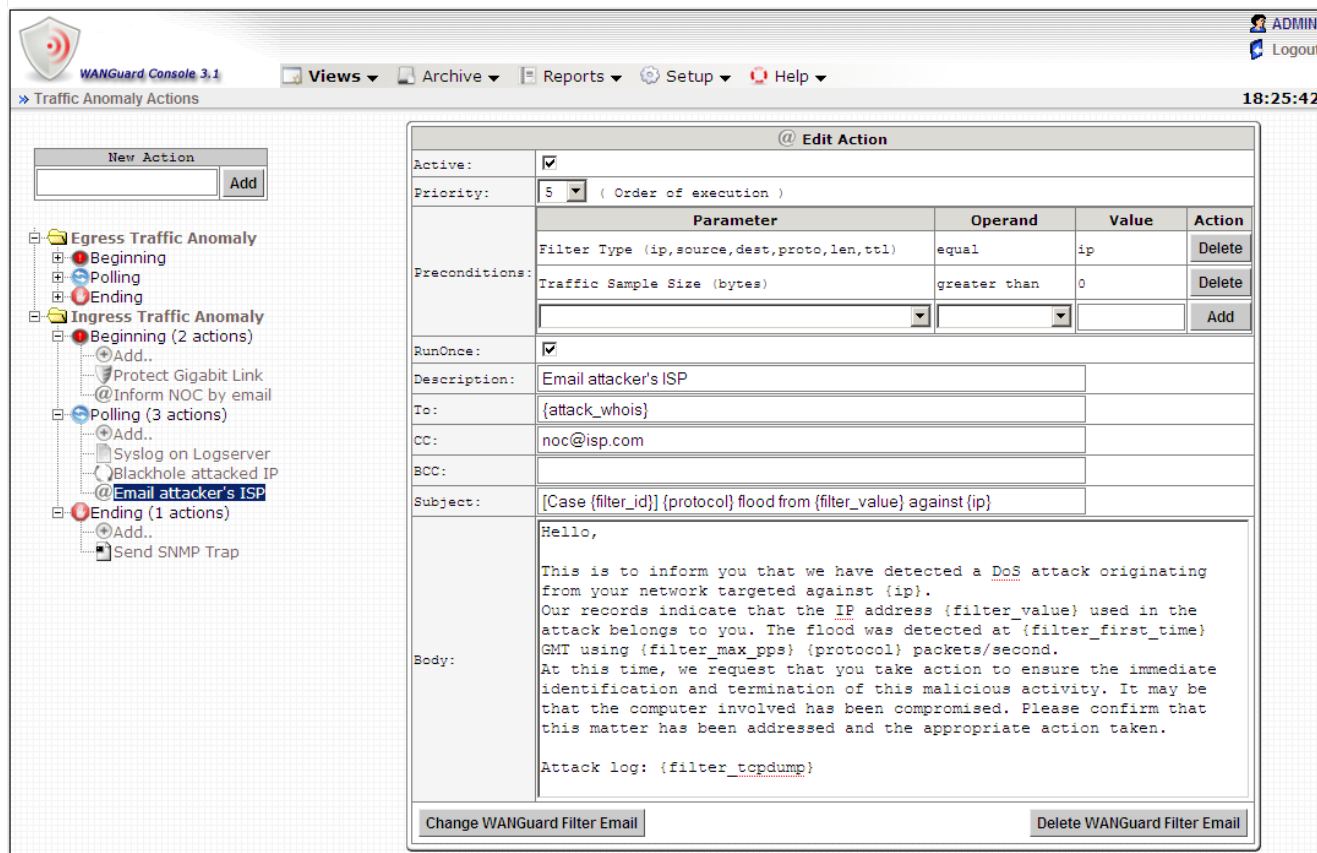
The *To* field can contain any number of email addresses (separated by comma) where notification emails will be sent. The “To” field can also contain the {attacker_whois} Dynamic Parameter. The {attacker_whois} parameter will be replaced with the ISP contact email addresses of the attacker, extracted from the whois database (RIPE, ARIN, APNIC, AfriNic, LacNIC). To use the {attacker_whois} parameter correctly you must first ensure that the attack pattern has the “ip” type, by using Conditional Parameters to check if “Filter type” equals “ip”. In case of spoofed attacks, the “Filter type” parameter will be different and the Module will not be executed.

WANGuard Filter generates a traffic sample log for every attack pattern it detects. Sometimes attack patterns are not active enough for the traffic sample log to be generated. To prevent sending emails that don't include a full traffic sample log, you must do the following:

- Send the notification emails in the Polling branch instead of the Beginning branch.
- Use Preconditions to verify that the traffic sample log has been generated by checking if “Filter Traffic Sample Size” is bigger than zero.

- Select the RunOnce checkbox to only allow the module to be executed one time per attack pattern. If you do not check this checkbox, emails will be sent every 5 seconds.

A configuration example of this module is shown in the image below. Emails are automatically sent towards attackers ISPs, if the attack is not spoofed (first Precondition) and if a traffic sample has been generated (second Precondition).



The screenshot shows the WANGuard Console 3.1 interface. On the left, a tree view shows the configuration structure under 'Traffic Anomaly Actions'. The main panel displays the configuration for the '@Email attacker's ISP' action.

@ Edit Action

Active: ☒
Priority: 5 (Order of execution)

Parameter	Operand	Value	Action
Filter Type (ip,source,dest,proto,len,ttl)	equal	ip	Delete
Traffic Sample Size (bytes)	greater than	0	Delete
			Add

RunOnce: ☒
Description: Email attacker's ISP
To: {attack_whois}
CC: noc@isp.com
BCC:
Subject: [Case {filter_id}] {protocol} flood from {filter_value} against {ip}

Body:

```

Hello,

This is to inform you that we have detected a DoS attack originating
from your network targeted against {ip}.
Our records indicate that the IP address {filter_value} used in the
attack belongs to you. The flood was detected at {filter_first_time}
GMT using {filter_max_pps} {protocol} packets/second.
At this time, we request that you take action to ensure the immediate
identification and termination of this malicious activity. It may be
that the computer involved has been compromised. Please confirm that
this matter has been addressed and the appropriate action taken.

Attack log: {filter_topdump}

```

Buttons: Change WANGuard Filter Email, Delete WANGuard Filter Email

The emails are sent through the local SMTP server (sendmail, postfix, qmail etc.) of the WANGuard Console system using the perl Mail::Send module. By default, the sender will be <WANGuard@localhost.localdomain>. For sender customizations (From field) please consult your SMTP server documentation.

Emails sent by this module are recorded in the Attack Patterns Log (Page 89).

WANGuard Filter Script Action Module

This module is used by WANGuard Filter to execute custom scripts written in any Linux compatible

scripting languages such as bash, perl, ruby, python etc. C and C++ programs or Linux commands can also be executed. The scripts can be executed at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of an attack pattern.

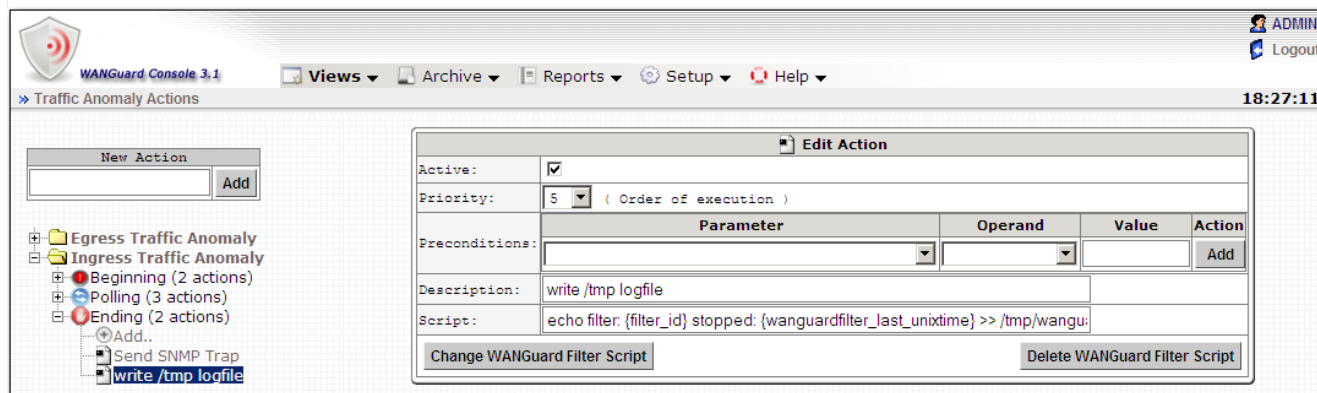
Scripts can access WANGuard Sensor and WANGuard Filter Dynamic Parameters through command-line parameters / options. Dynamic Parameters are explained at the beginning of the chapter. A complete list of Dynamic Parameters available can be found in Appendix 2 – Conditional & Dynamic Parameters (Page 96).

The scripts are executed locally on each WANGuard Filter system that uses Actions that include this module. Multiple commands can be executed using the “;” separator. Scripts executed through the WANGuard Filter Action Module have the user privileges of the “wanguard” system account. To elevate privileges for your scripts you should use the *sudo* prefix, after editing the */etc/sudoers* file.

Some possible uses of this module:

- configure ACLs or execute PIX "shun" commands to filter attacking IPs
- issue “route blackhole” commands on the attacked Linux servers to filter attacking IPs
- send SNMP TRAP messages to SNMP monitoring stations

The image below shows how to use this module to write a text file with logs of attack patterns that became inactive, using basic Linux commands.



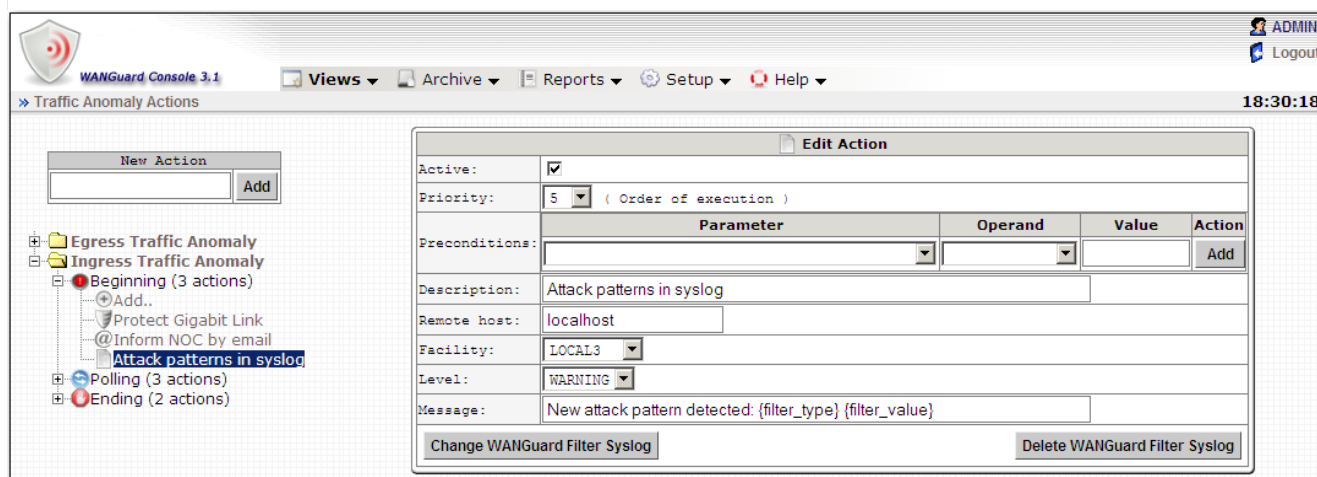
WANGuard Filter Syslog Action Module

This module is used by WANGuard Filter to send syslog messages locally, or to remote syslog monitoring hosts. To send syslog messages you must enter the IP address of the syslog server (127.0.0.1 for localhost), select the desired facility, severity level and message content. Syslog messages can be sent at the beginning (Beginning branch), during (Polling branch), or at the end (Ending branch) of an attack pattern.

The message field can contain any number of WANGuard Sensor and WANGuard Filter Dynamic

Parameters. Dynamic Parameters are explained at the beginning of the chapter. A complete list of Dynamic Parameters available can be found in Appendix 2 – Conditional & Dynamic Parameters (Page 96).

A configuration example of this module is shown below.



The screenshot shows the WANGuard Console 3.1 interface. The top menu bar includes 'Views', 'Archive', 'Reports', 'Setup', and 'Help'. The left sidebar shows a tree view of 'Traffic Anomaly Actions' with categories like 'Egress Traffic Anomaly', 'Ingress Traffic Anomaly', 'Beginning (3 actions)', 'Polling (3 actions)', and 'Ending (2 actions)'. The main area displays the 'Edit Action' configuration form.

Edit Action Configuration:

- Active:** ☒
- Priority:** 5 (Order of execution)
- Preconditions:** Table with columns: Parameter, Operand, Value, Action.

Parameter	Operand	Value	Action
			Add
- Description:** Attack patterns in syslog
- Remote host:** localhost
- Facility:** LOCAL3
- Level:** WARNING
- Message:** New attack pattern detected: {filter_type} {filter_value}

Buttons at the bottom: Change WANGuard Filter Syslog, Delete WANGuard Filter Syslog.

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
- inbound and outbound traffic thresholds used for traffic anomalies detection
- what Action should be activated when an inbound or outbound traffic anomaly is detected

When configuring a WANGuard Sensor (Page 46) 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 Platform 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 16).

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.

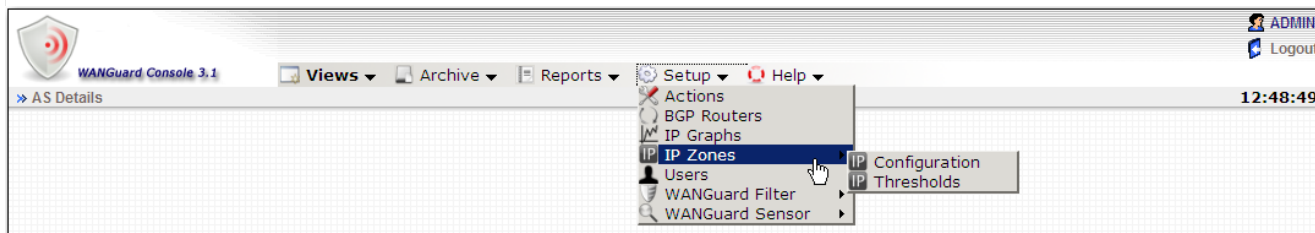
To ease the configuration of IP Zones, every new IP class that you define, inherits by default the properties of the closest (having the biggest CIDR) IP class that includes it. The only IP class that does not inherit any properties is the 0.0.0.0/0 IP class, because there is no other IP class that includes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

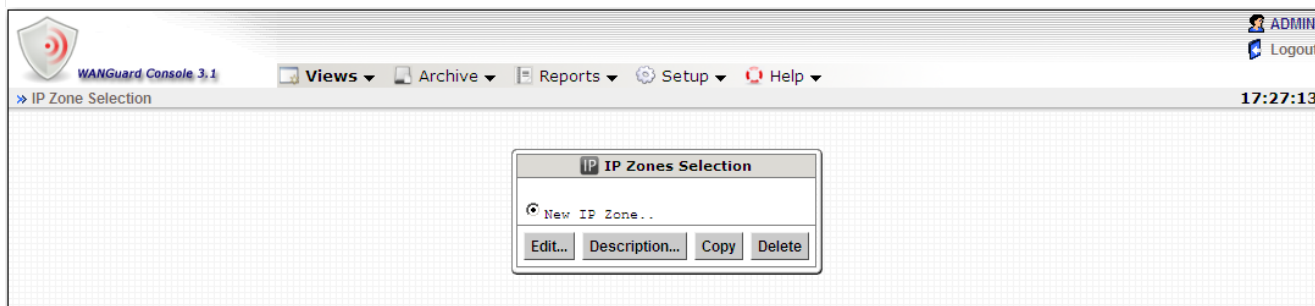
In the last section of this chapter you can see an example on how inheritance works.

IP Zone Selection

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

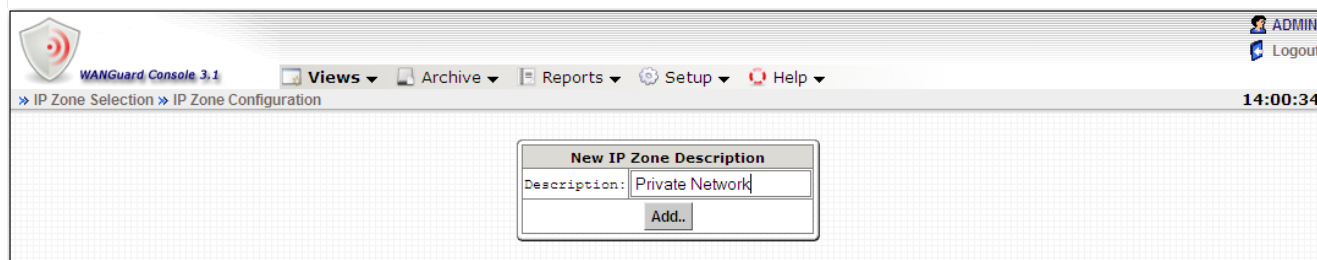


The IP Zones Selection window lets you select existing IP Zones to edit, change description, copy or delete. If no IP Zones were previously added, then the form will only have the option to add a new IP Zone.



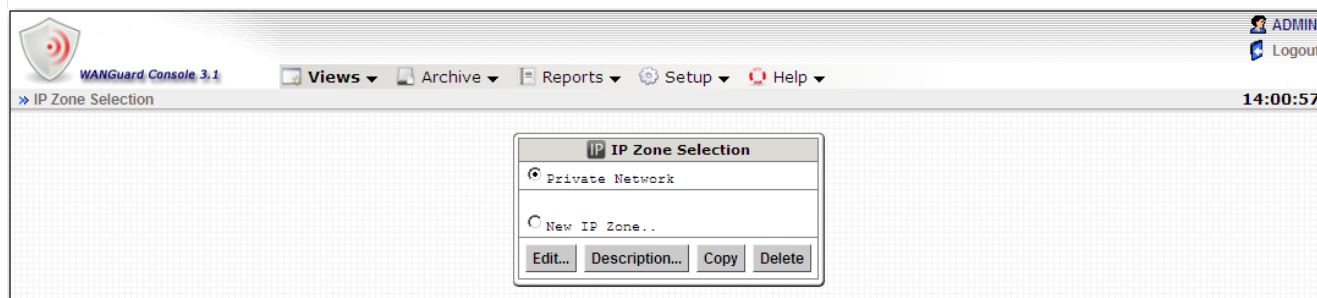
Adding a new IP Zone

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.



Changing Description, Copying & Deleting IP Zones

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

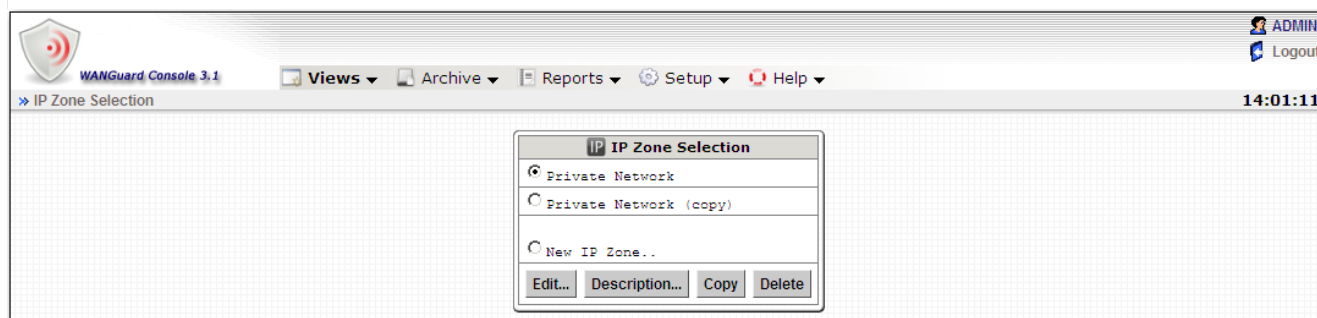


You can **configure** the selected IP Zone by clicking the <Edit...> button.

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

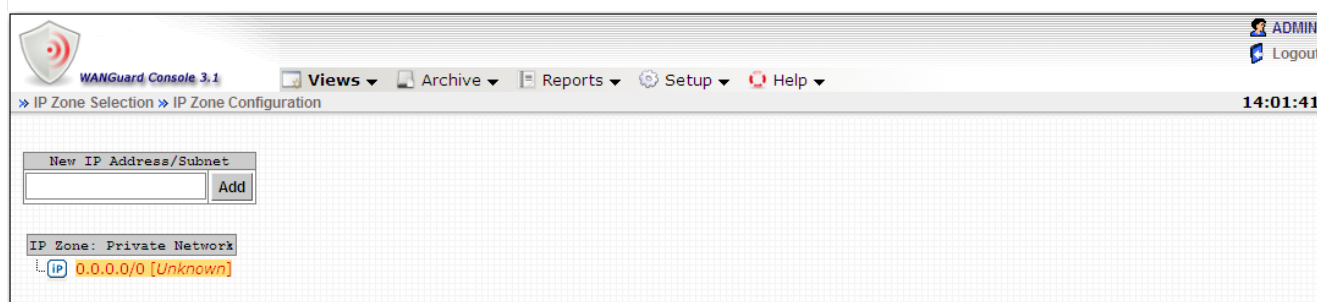
To **copy** the selected IP Zone you must click the <Copy> button. A new IP Zone will be created that will have the same information and the same description with the word “(copy)” attached. In some cases when you have multiple WANGuard Sensor systems, you may have to create multiple IP Zones that share 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.



WANGuard Console 3.1

Views ▾

Archive ▾

Reports ▾

Setup ▾

Help ▾

ADMIN

Logout

>> IP Zone Selection >> IP Zone Configuration

13:43:33

New IP Address/Subnet

Add

IP Zone: Private Network

IP

0.0.0.0/0 [Unknown]

Inbound traffic thresholds for 0.0.0.0/0			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
UDP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
ICMP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
OTHER	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
Action:		None	none
Outbound traffic thresholds for 0.0.0.0/0			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
UDP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
ICMP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
OTHER	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
Action:		None	none
Parameters for 0.0.0.0/0			
Parameter	Value	Inheritance	
Accounting:	No	none	
Graphing:	No	none	
Concurrency:	1	none	
Description:	Unknown	none	
Change Record		Delete Record	

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:

Inbound and Outbound Traffic Thresholds

Contains traffic thresholds for any IP address included in the selected IP class. When a traffic threshold

is reached then WANGuard Sensor generates a traffic anomaly alarm that is displayed in the Security View (Page 72), recorded in the Archive (Page 86), and the selected inbound or outbound Action is executed.

Inbound traffic describes the traffic coming towards your network, and outbound traffic describes traffic sent by your network.

WANGuard Sensor checks packets/second and bits/second threshold values for 5 types of traffic:

- **TCP** describes all traffic that uses the TCP protocol (HTTP, HTTPS, IMAP, POP3, FTP, SSH, etc.)
- **TCP + SYN** describes TCP packets with the SYN flag set and the ACK flag not set (useful for SYN flood detection)
- **UDP** describes all traffic that uses the UDP protocol (DNS, SNMP, TFTP etc.)
- **ICMP** describes all traffic that uses the ICMP protocol (PING, TRACEROUTE etc.)
- **OTHER** describes all other protocols (non-UDP, non-TCP and non-ICMP)

If you are not interested in checking traffic thresholds for an IP class, you can check the Unlimited checkbox from the right side of the threshold value field. To enter a threshold value, the Unlimited checkbox must be unchecked first. To inherit the value of the parent IP class you must leave the threshold value field empty and the Unlimited checkbox unchecked.

To ease the configuration of threshold values for many IP classes / addresses with the same properties, you can define a single **Thresholds Template** and then select it from the list. The thresholds template will override all existing thresholds values. Thresholds Templates management is described in-depth in the next section.

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.

Concurrency

This parameter is used by WANGuard Filter when doing source IP filtering. If the traffic thresholds are reached and the concurrency value is set to “1” then every single source IP that reaches that threshold will be filtered by WANGuard Filter. If the concurrency value is set to “3” then every single source IP that reaches a third of the destination's traffic threshold will be filtered by WANGuard Filter. If the parameter is empty, then the parameter will be inherited from the parent IP class. The default value for concurrency is “1”.

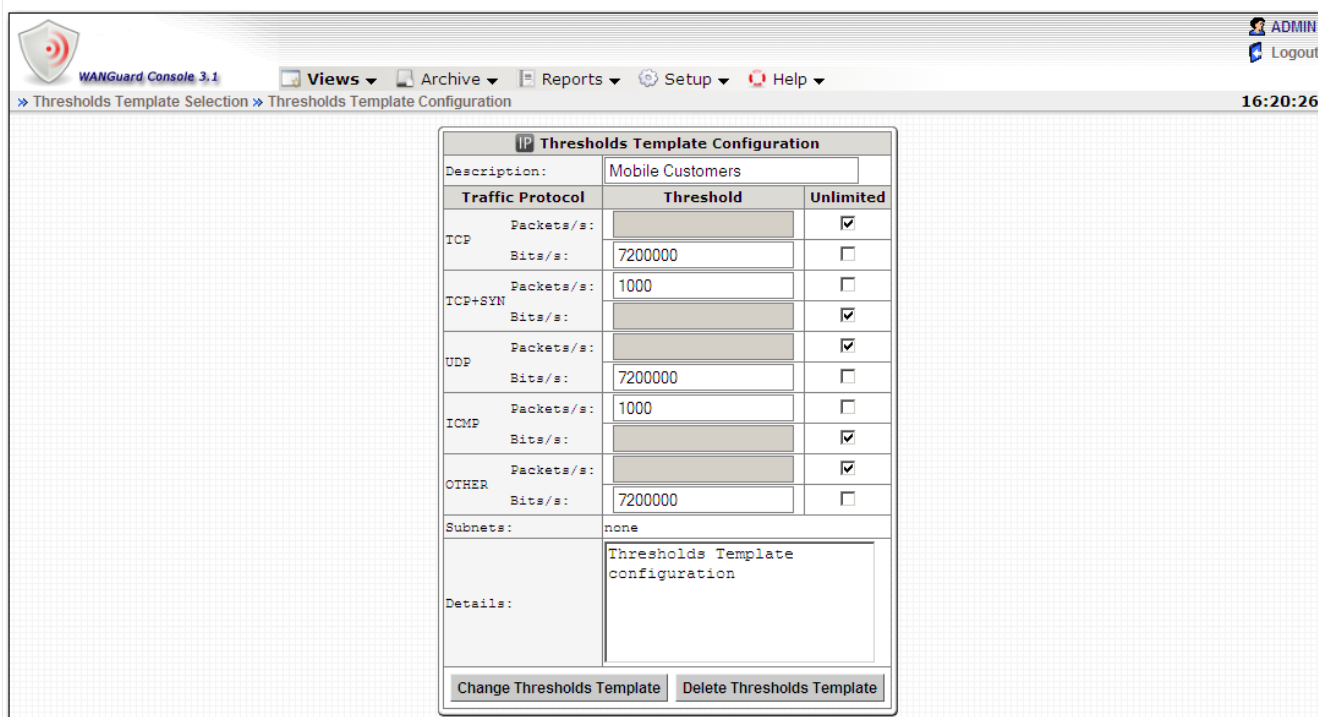
Description

This parameter should contain a short description for the selected IP class or IP address.

Thresholds Templates

To ease the addition of traffic thresholds with the same values, define a Thresholds Template first and then apply it on multiple IP classes. To manage Thresholds Templates you must first select IP Zones from Setup menu and then select Thresholds.

Most fields are explained in the Inbound and Outbound Traffic Thresholds section above. The subnets row displays the IP classes and IP Zones that are using the selected template. When you update a template, every record using it will be updated too. An example of a Thresholds Template configuration is shown below.



IP Thresholds Template Configuration

Description: Mobile Customers

Traffic Protocol	Threshold	Unlimited
TCP	Packets/s: 7200000	<input checked="" type="checkbox"/>
	Bits/s: 1000	<input type="checkbox"/>
TCP+SYN	Packets/s: 7200000	<input checked="" type="checkbox"/>
	Bits/s: 1000	<input checked="" type="checkbox"/>
UDP	Packets/s: 7200000	<input type="checkbox"/>
	Bits/s: 1000	<input type="checkbox"/>
ICMP	Packets/s: 7200000	<input checked="" type="checkbox"/>
	Bits/s: 1000	<input checked="" type="checkbox"/>
OTHER	Packets/s: 7200000	<input checked="" type="checkbox"/>
	Bits/s: 1000	<input type="checkbox"/>

Subnets: none

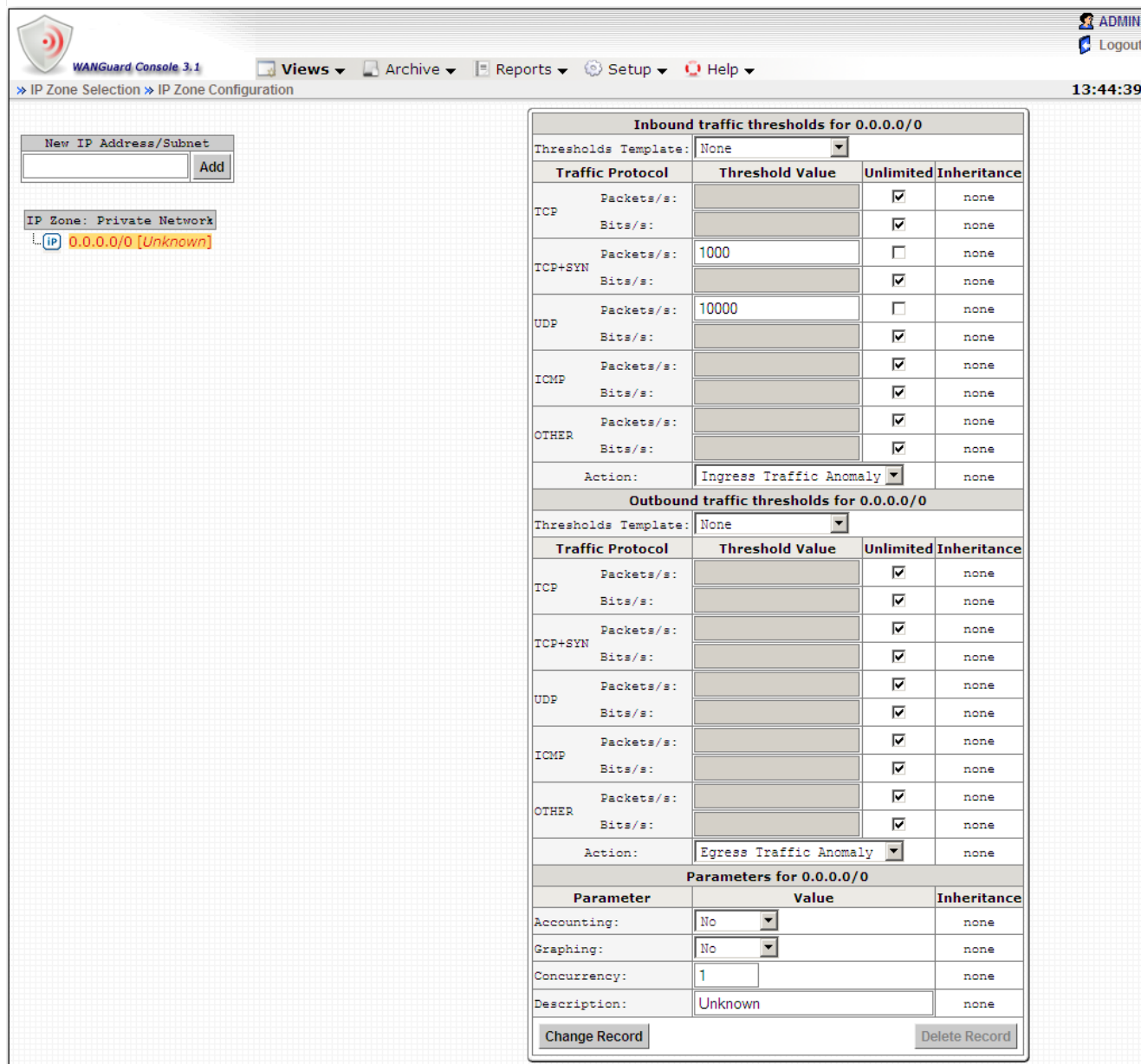
Details: Thresholds Template configuration

Change Thresholds Template Delete Thresholds Template

IP Zone Configuration Example

In the following images you can see how IP Zone inheritance works and how you can configure WANGuard Platform's features for various IP classes and IP addresses.

By default, the 0.0.0.0/0 IP class has all threshold values set to Unlimited, *Actions* set to None and *Accounting* and *Graphing* set to No. By unchecking the Unlimited checkbox we defined new values for *TCP+SYN Packets/second* and *UDP Packets/second*, and we defined new Inbound and Outbound *Actions*.



WANGuard Console 3.1 Views Archive Reports Setup Help 13:44:39

IP Zone Selection >> IP Zone Configuration

New IP Address/Subnet: Add

IP Zone: Private Network

IP 0.0.0.0/0 [Unknown]

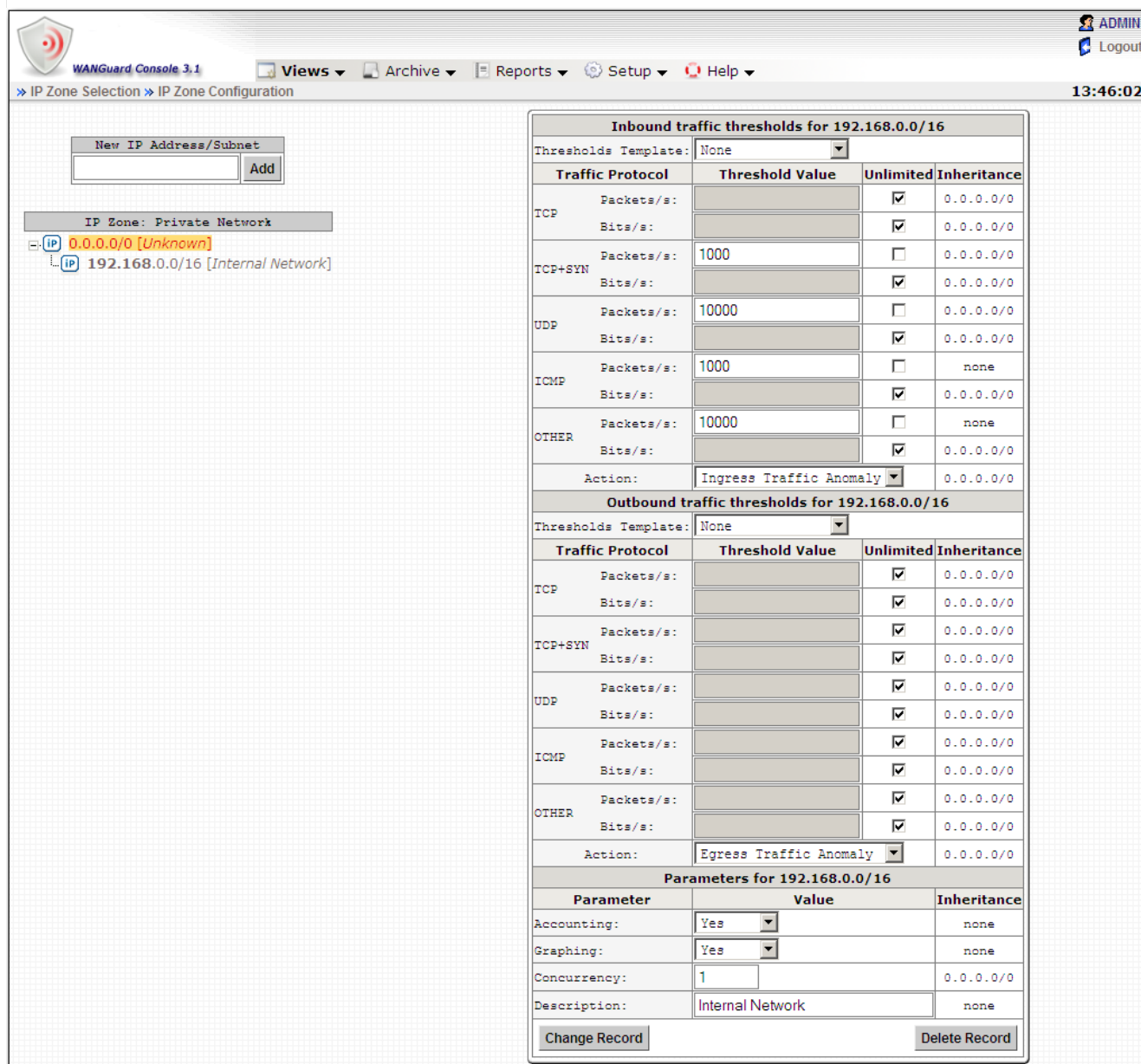
Inbound traffic thresholds for 0.0.0.0/0			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
TCP+SYN	Packets/s:	<input type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
UDP	Packets/s:	<input type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
ICMP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
OTHER	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
Action:		Ingress Traffic Anomaly	none

Outbound traffic thresholds for 0.0.0.0/0			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
UDP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
ICMP	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
OTHER	Packets/s:	<input checked="" type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	none
Action:		Egress Traffic Anomaly	none

Parameters for 0.0.0.0/0		
Parameter	Value	Inheritance
Accounting:	No	none
Graphing:	No	none
Concurrency:	1	none
Description:	Unknown	none

Change Record Delete Record

In the image above you can see that all the values are inherited from 0.0.0.0/0, except the following values: *ICMP Packets/second* (1000), *Other Packets/second* (10000), *Accounting* (YES), *Graphing* (YES) and *Description* (Internal Network).



WANGuard Console 3.1 Views Archive Reports Setup Help 13:46:02

IP Zone Selection >> IP Zone Configuration

New IP Address/Subnet Add

IP Zone: Private Network

- IP 0.0.0.0/0 [Unknown]
- IP 192.168.0.0/16 [Internal Network]

Inbound traffic thresholds for 192.168.0.0/16			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s:	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s:	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s:	<input type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s:	<input type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:		Ingress Traffic Anomaly	0.0.0.0/0

Outbound traffic thresholds for 192.168.0.0/16			
Thresholds Template: None			
Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:		Egress Traffic Anomaly	0.0.0.0/0

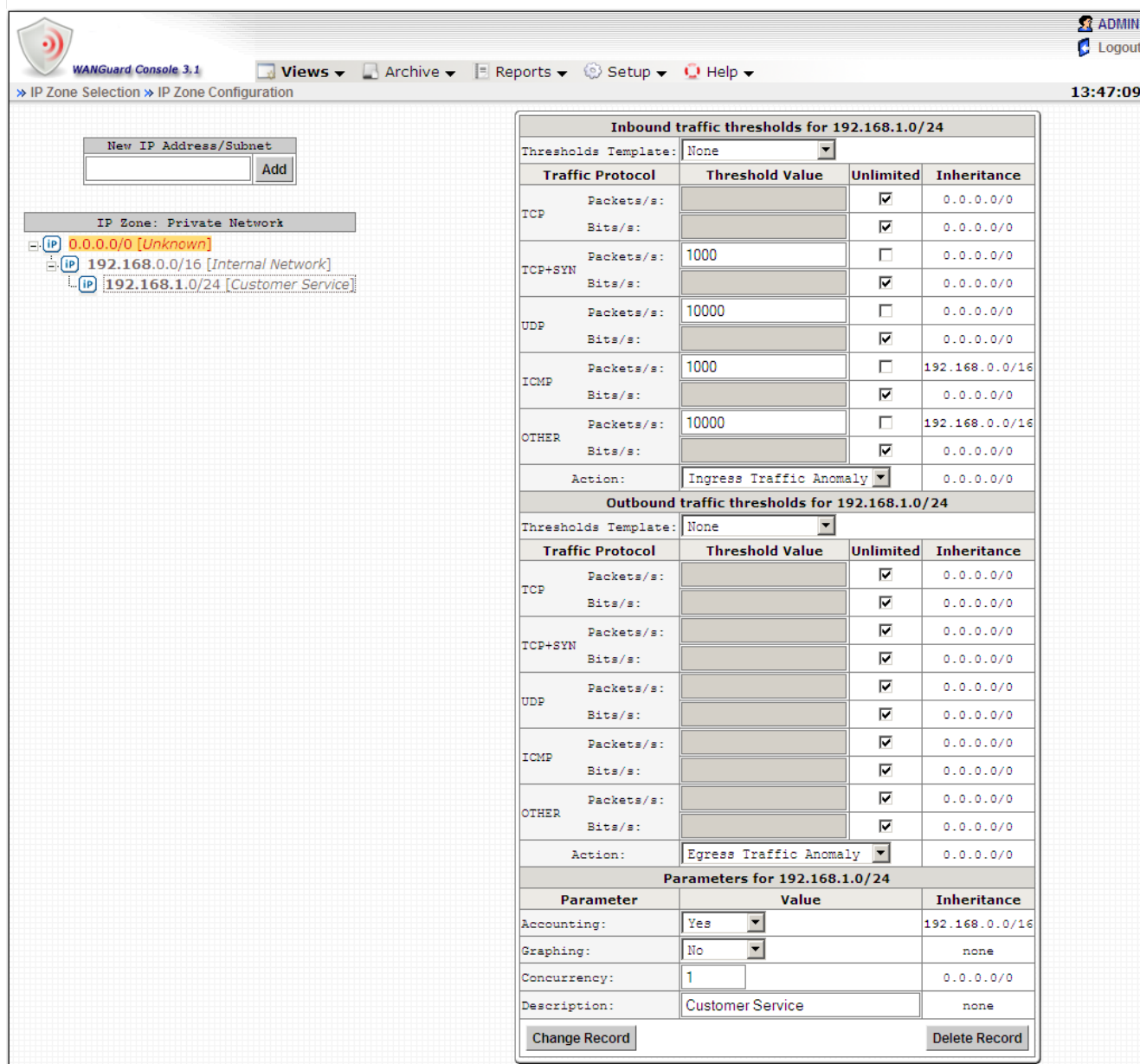
Parameters for 192.168.0.0/16		
Parameter	Value	Inheritance
Accounting:	Yes	none
Graphing:	Yes	none
Concurrency:	1	0.0.0.0/0
Description:	Internal Network	none

Change Record Delete Record

After adding the 192.168.0.0/16 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 below you can see that a new IP class called “Customer Service” was added, and only the *Description* and the *Graphing* values were changed. The other values are inherited from the direct parent 192.168.0.0/16, or from the parent's parent 0.0.0.0/0, if the direct parent didn't change those values.

Because the parent IP class has the *Graphing* parameter set to “Yes” and this IP class has the *Graphing* parameter set to “No”, WANGuard Sensor generates traffic graphs for all IP addresses contained in the “Internal Network” IP class that are not contained in the “Customer Service” IP class.



WANGuard Console 3.1 Views Archive Reports Setup Help

IP Zone Selection > IP Zone Configuration 13:47:09

New IP Address/Subnet Add

IP Zone: Private Network

- IP 0.0.0.0/0 [Unknown]
- IP 192.168.0.0/16 [Internal Network]
- IP 192.168.1.0/24 [Customer Service]

Inbound traffic thresholds for 192.168.1.0/24

Thresholds Template: None

Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s:	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s:	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s:	<input type="checkbox"/>	192.168.0.0/16
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s:	<input type="checkbox"/>	192.168.0.0/16
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:			Ingress Traffic Anomaly 0.0.0.0/0

Outbound traffic thresholds for 192.168.1.0/24

Thresholds Template: None

Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:			Egress Traffic Anomaly 0.0.0.0/0

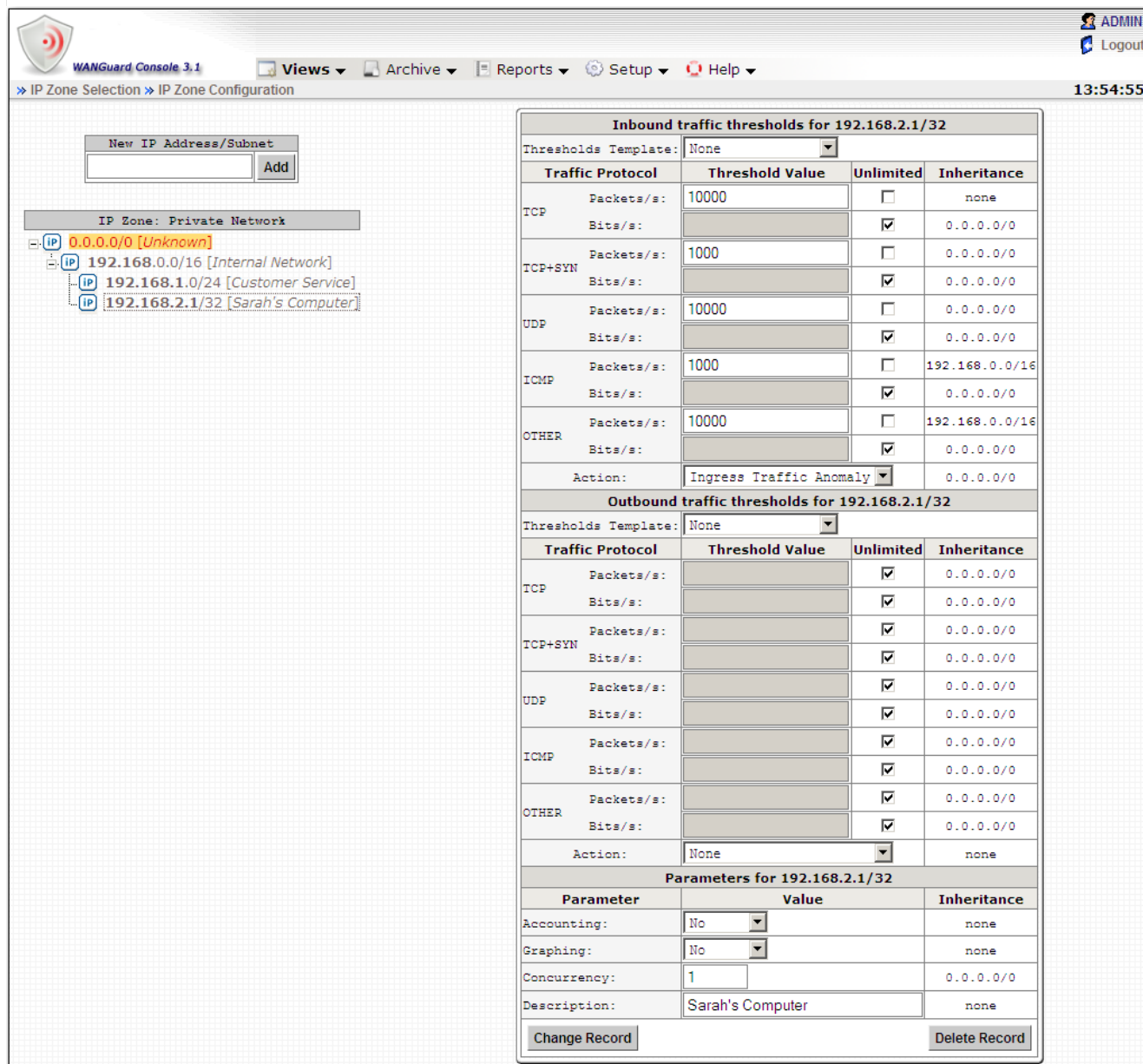
Parameters for 192.168.1.0/24

Parameter	Value	Inheritance
Accounting:	Yes	192.168.0.0/16
Graphing:	No	none
Concurrency:	1	0.0.0.0/0
Description:	Customer Service	none

Change Record Delete Record

In the image below you can see that a new IP address called “Sarah's Computer” is added, and only the *TCP Packets/second*, *Outbound Action*, *Accounting*, *Graphing* and *Description* values were changed. The rest of the values from “Internal Network” propagated to “Sarah's Computer” because they were not modified.

“Sarah's Computer” IP address is placed in the tree together with the “Customer Service” IP class because both are contained in the “Internal Network” IP class.



WANGuard Console 3.1 Views Archive Reports Setup Help

IP Zone Selection IP Zone Configuration 13:54:55

New IP Address/Subnet Add

IP Zone: Private Network

- IP 0.0.0.0/0 [Unknown]
- IP 192.168.0.0/16 [Internal Network]
 - IP 192.168.1.0/24 [Customer Service]
 - IP 192.168.2.1/32 [Sarah's Computer]

Inbound traffic thresholds for 192.168.2.1/32

Thresholds Template: None

Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s: 10000	<input type="checkbox"/>	none
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s: 1000	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s: 10000	<input type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s: 1000	<input type="checkbox"/>	192.168.0.0/16
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s: 10000	<input type="checkbox"/>	192.168.0.0/16
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:	Ingress Traffic Anomaly		0.0.0.0/0

Outbound traffic thresholds for 192.168.2.1/32

Thresholds Template: None

Traffic Protocol	Threshold Value	Unlimited	Inheritance
TCP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
TCP+SYN	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
UDP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
ICMP	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
OTHER	Packets/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
	Bits/s:	<input checked="" type="checkbox"/>	0.0.0.0/0
Action:	None		none

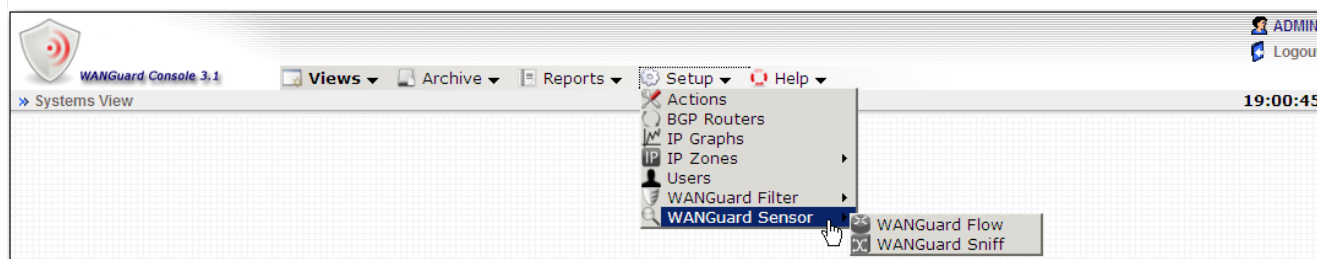
Parameters for 192.168.2.1/32

Parameter	Value	Inheritance
Accounting:	No	none
Graphing:	No	none
Concurrency:	1	0.0.0.0/0
Description:	Sarah's Computer	none

Change Record Delete Record

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.

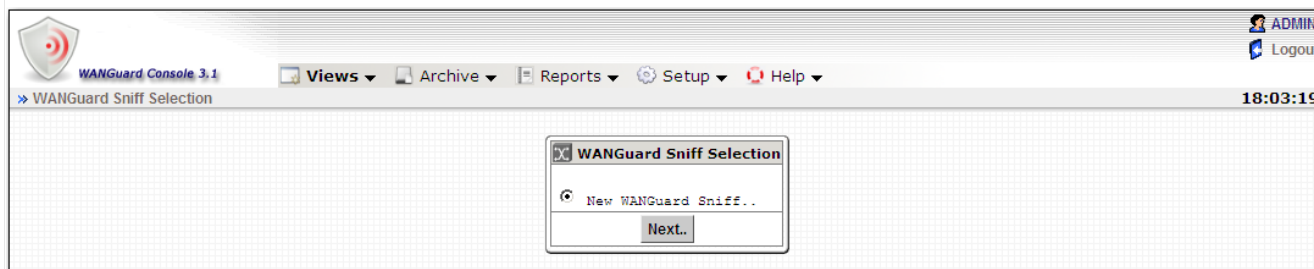


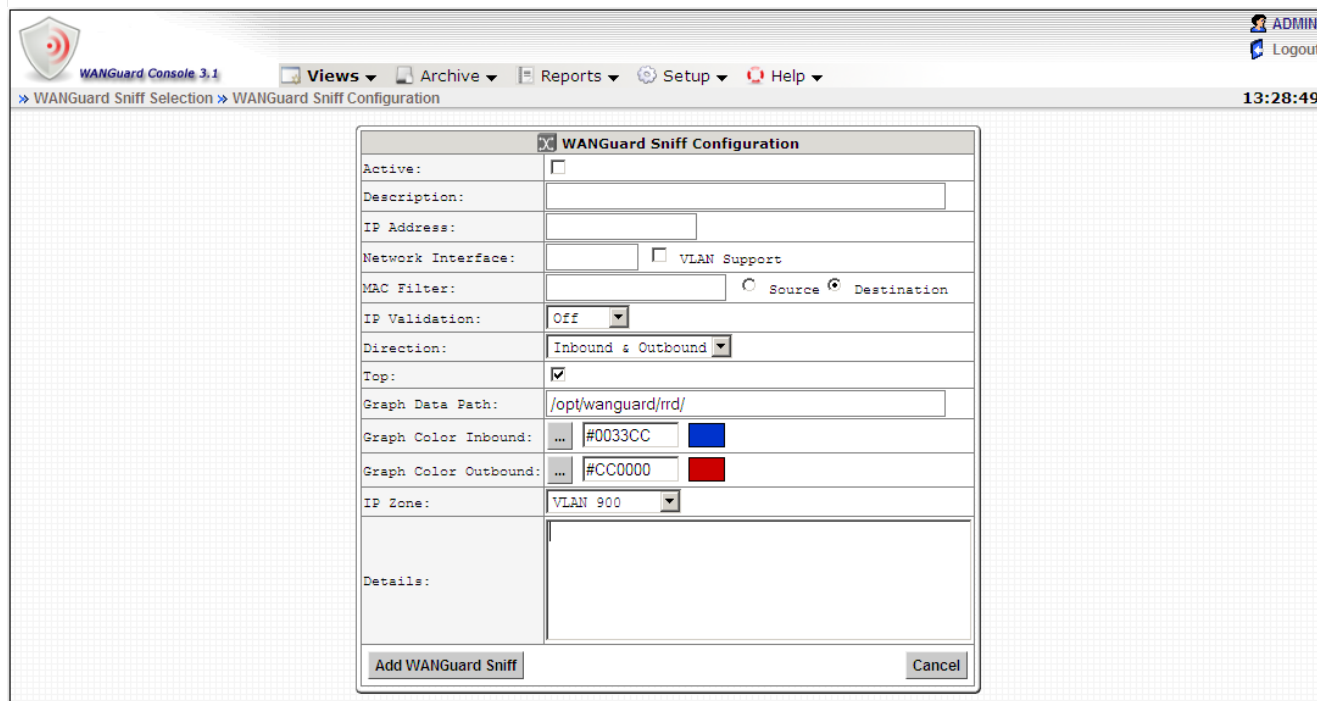
To learn more about the differences between the two types of WANGuard Sensor please consult Chapter 2 - How To Choose A Method Of Traffic Capturing (Page 9).

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.





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 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.

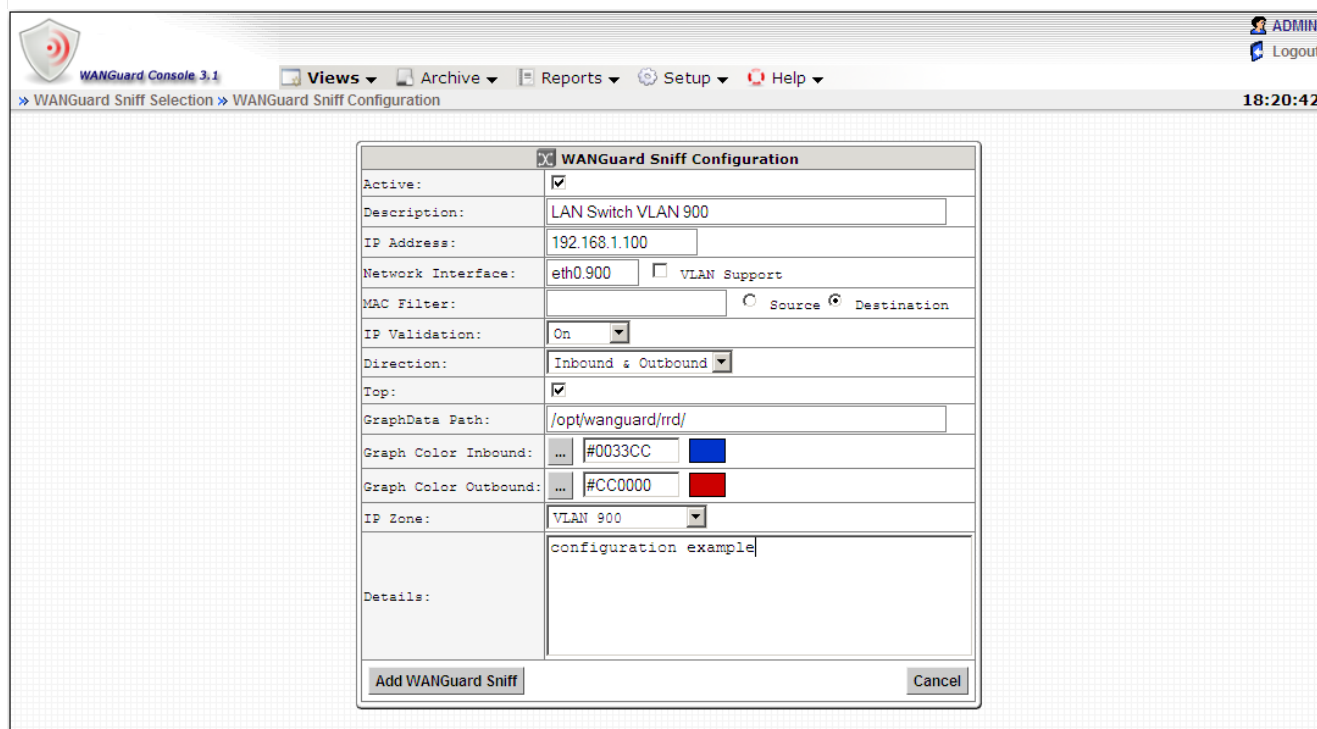
- **IP Zone**

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 Console 3.1 Views Archive Reports Setup Help

WANGuard Sniff Selection WANGuard Sniff Configuration 18:20:42

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

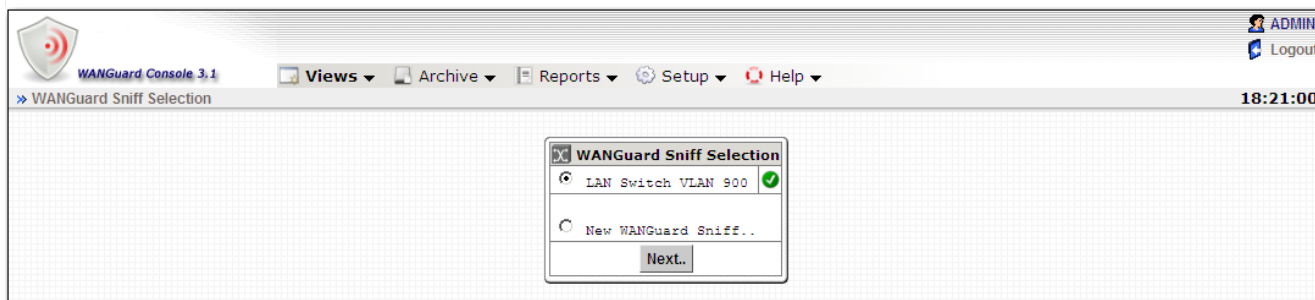
Details: configuration example

Add WANGuard Sniff Cancel

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.

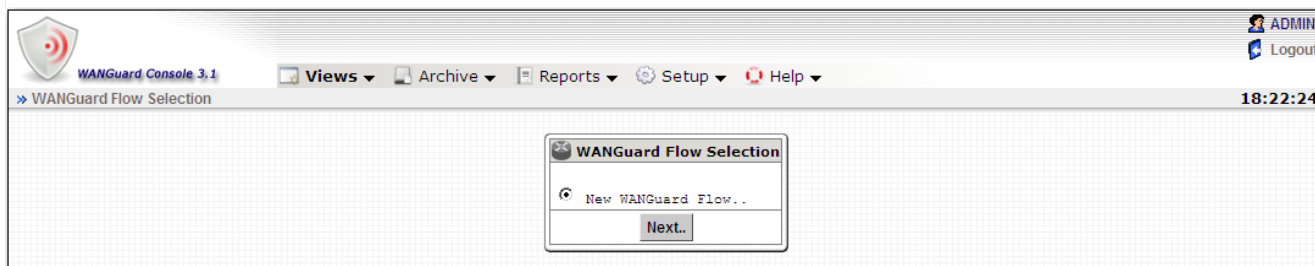
If you checked the Active switch but the WANGuard Sniff is still not running, you can find a description of the error in the WANGuard Sniff Events Logs (see Archive chapter – Page 88) or in the Events Tab (see Views chapter – Page 68) .

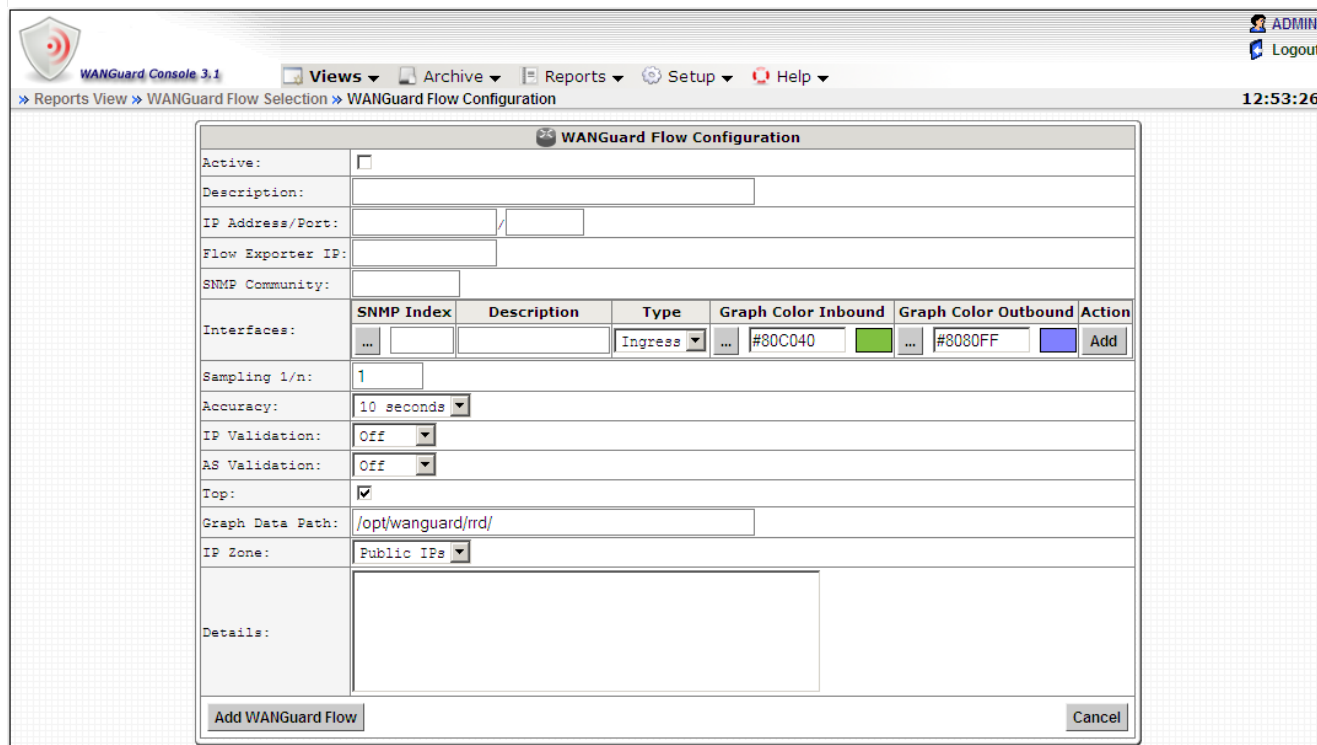


WANGuard Flow Configuration

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 92).

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.





WANGuard Flow Configuration

Active: ☐

Description:

IP Address/Port:

Flow Exporter IP:

SNMP Community:

SNMP Index	Description	Type	Graph Color Inbound	Graph Color Outbound	Action
...	<input type="text"/>	Ingress	#80C040	#8080FF	Add

Sampling 1/n:

Accuracy:

IP Validation:

AS Validation:

Top: ☒

Graph Data Path:

IP Zone:

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.

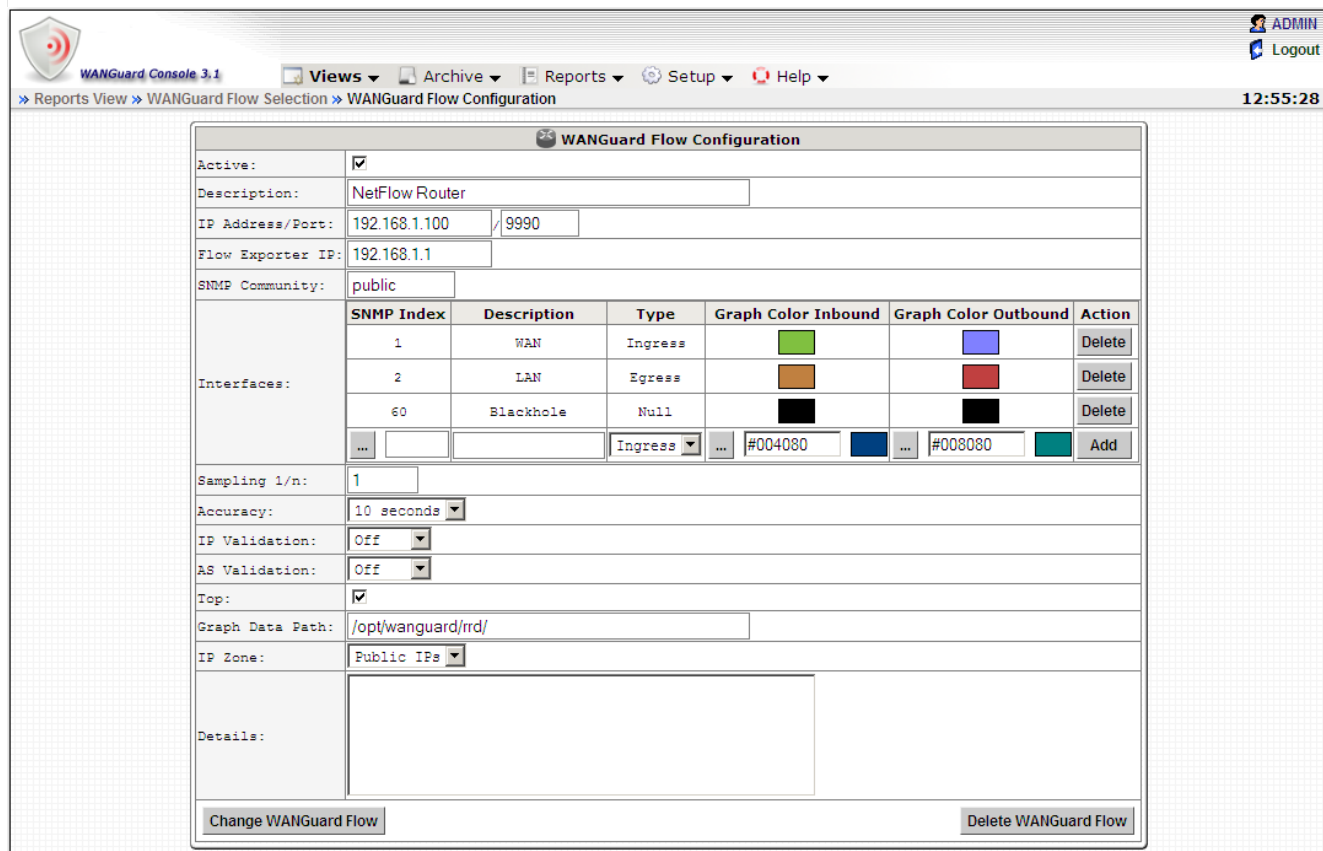
- **IP Zone**

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 | 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

SNMP Index	Description	Type	Graph Color Inbound	Graph Color Outbound	Action
1	WAN	Ingress			Delete
2	LAN	Egress			Delete
60	Blackhole	Null			Delete
...		Ingress			Add

Sampling 1/n: 1

Accuracy: 10 seconds

IP Validation: Off

AS Validation: Off

Top: ☒

Graph Data Path: /opt/wanguard/rdr/

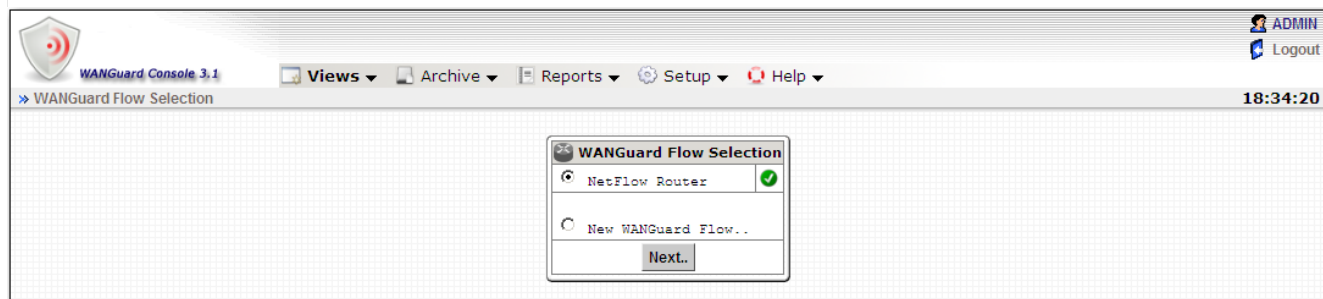
IP Zone: Public IPs

Details:

Change WANGuard Flow | Delete WANGuard Flow


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 88) or in the Events Tab (see Views chapter – Page 68) .



WANGuard Console 3.1 | Views | Archive | Reports | Setup | Help | ADMIN | Logout | 18:34:20

WANGuard Flow Selection

NetFlow Router 

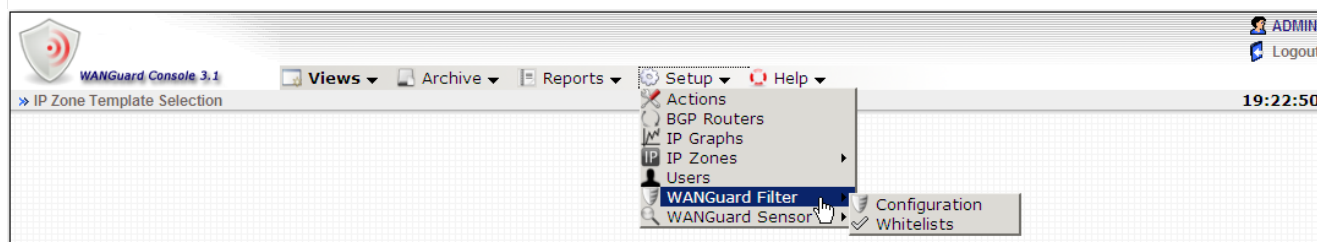
New WANGuard Flow..

Next..

WANGuard Filter Setup

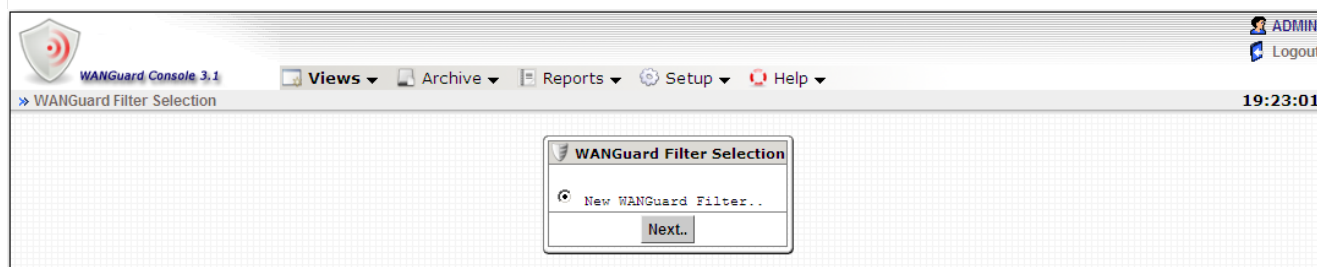
WANGuard Filter can be deployed in-line or it must have access to an iBGP router that can be used to divert the malicious traffic towards the server running it. For sending iBGP announcements WANGuard Filter uses the free, open-source quagga or zebra routing software. For more information about configuring quagga or zebra and your network devices for traffic diversion please consult Appendix 3 – Configuring Traffic Diversion (page 99). Keep in mind that our support team can help you with any configuration issues.

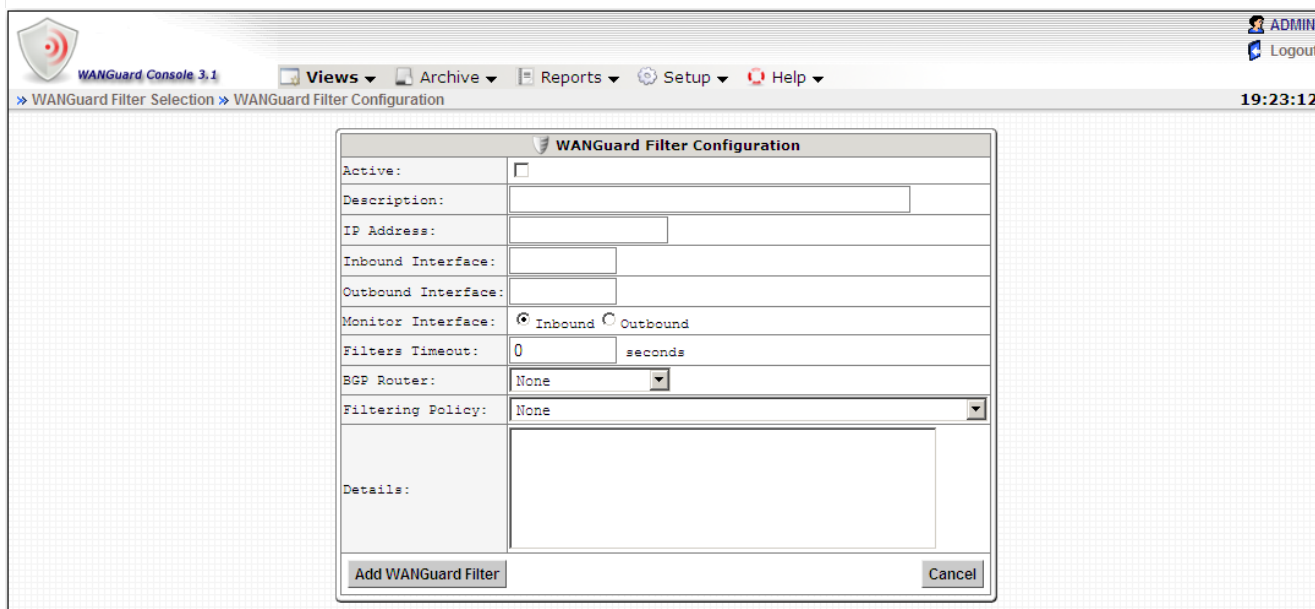
This chapter describes how to add, configure and delete WANGuard Filter systems through WANGuard Console. If you don't plan to use WANGuard Filter, you can skip this chapter.



WANGuard Filter Configuration

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





The screenshot shows the 'WANGuard Filter Configuration' window. It has a title bar with 'WANGuard Console 3.1' and a menu bar with 'Views', 'Archive', 'Reports', 'Setup', and 'Help'. The main area contains the following fields:

- Active:** A checkbox.
- Description:** A text input field.
- IP Address:** A text input field.
- Inbound Interface:** A text input field.
- Outbound Interface:** A text input field.
- Monitor Interface:** Radio buttons for 'Inbound' (selected) and 'Outbound'.
- Filters Timeout:** A text input field with '0' and a unit dropdown set to 'seconds'.
- BGP Router:** A dropdown menu with 'None' selected.
- Filtering Policy:** A dropdown menu with 'None' selected.
- Details:** A large text area.

At the bottom, there are two buttons: 'Add WANGuard Filter' and 'Cancel'.

The WANGuard Filter Configuration window contains the following fields:

- **Active**

If the Active checkbox is checked, WANGuard Filter can be activated by the WANGuard Filter Enabler Action Module.

- **Description**

A short, generic description that will help you to identify the WANGuard Filter system.

- **IP Address**

An IP address configured on the machine that must run the selected WANGuard Filter. This field is used only by the *WANGuardController* daemon for system identification.

- **Inbound Interface**

The network interface that receives the malicious traffic. If the WANGuard Filter system is deployed in-line then this is the interface that receives the traffic towards your network.

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. If VLANs are used then you should configure them first using the *vconfig* command.

- **Outbound Interface**

The cleaned traffic is sent to a downstream router through this network interface. The default gateway must be reachable through this interface.

If GRE or IP over IP tunneling is required then you must first configure a virtual network interface with the *ip* command, part of the *iproute2* package.

- **Monitor Interface**

This switch configures the interface monitored by WANGuard Filter.

- *Inbound* - WANGuard Filter analyzes the traffic passing the inbound interface. The advantage is that the generated statistics are accurate because WANGuard Filter analyzes all traffic. The disadvantage is that CPU usage is higher because WANGuard Filter continuously inspects malicious packets even if they are being filtered.
- *Outbound* - WANGuard Filter analyzes the traffic passing the outbound interface. The advantage is that the CPU usage is lower because malicious packets are not forwarded through the outbound interface, and are not being analyzed. The disadvantage is that the attack statistics are not entirely accurate.

- **Filters Timeout**

This field contains the number of seconds of inactivity required for the deletion of an attack pattern. If set to 0 then every attack pattern detected is not being deleted until the attack stops and WANGuard Filter becomes inactive. Usually, an attack pattern is associated with a filter (see Filtering Policy below).

- **BGP Router**

The BGP Router field provides a selection of currently defined BGP Routers that may be used for traffic diversion. When activated, WANGuard Filter sends a BGP announcement through the selected BGP router. The WANGuard Filter system will then become next-hop for the attacked IP address. When the attack ends, WANGuard Filter automatically deletes the BGP announcement and the traffic towards the IP address will be routed normally.

For more information about defining BGP Routers please consult the BGP Router Setup chapter (Page 61). If the WANGuard Filter system is deployed in-line, or you don't plan to use traffic diversion, you can leave the Router field set to None.

- **Filtering Policy**

The Filtering Policy lets you select what actions WANGuard Filter will take when it detects an attack pattern. An attack pattern is formed by malicious packets that share some common Layer 3, Layer 4 or Layer 5 fields. When an attack comes from a non-spoofed IP address, the attack pattern is the source IP address of the attacker. In case of a spoofed attack, the attack pattern could be the source TCP or UDP port, the destination TCP or UDP port, IP protocol number, packets size, TTL etc.

WANGuard Filter does inbound traffic filtering and packet rate limiting using the Linux 2.6.x Netfilter framework.

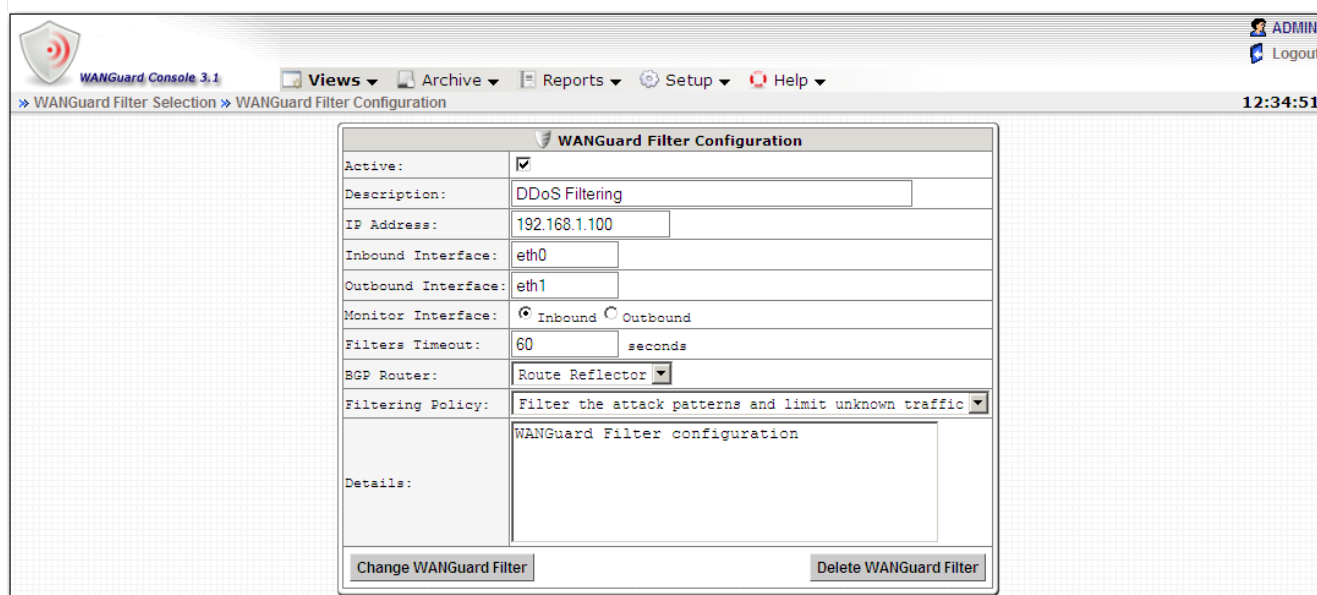
Available Filtering Policies are:

- *None* - WANGuard Filter only detects and reports attack patterns. The Linux firewall API is not used.

- *Filter the attack patterns* - WANGuard Filter detects, reports and filters the attack patterns. If an attack pattern is not whitelisted then all the traffic matched by the attack pattern is dropped.
 - *Filter the attack patterns and limit unknown traffic* - WANGuard Filter detects, reports and filters the attack patterns and limits the unknown traffic. If an attack pattern is not whitelisted then all the traffic matched by the attack pattern is dropped. Also, the WANGuard Filter system will not forward traffic that exceeds the anomaly's traffic type packets/second threshold value for the attacked IP address recorded in the WANGuard Sensor's IP Zone.
 - *Limit the attack patterns* - WANGuard Filter detects, reports and limits the attack patterns. The WANGuard Filter only forwards attack patterns traffic that does not exceed the anomaly's traffic type packets/second threshold value for the attacked IP address recorded in the WANGuard Sensor's IP Zone.
 - *Apply default forwarding policy* - WANGuard Filter detects and reports the attack patterns, and the default Netfilter forwarding policy is applied. Netfilter is still being used, but all the rules have the "RETURN" target. This is mostly used for debugging Netfilter rules.
- **Details**

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

In the following configuration example when the WANGuard Filter is activated by the WANGuard Filter Enabler Action Module, a BGP announcement will be sent through the "Route Reflector" BGP Router. The WANGuard Filter system will then receive the traffic towards the attacked IP, it will analyze the traffic coming through the "eth0" interface and will update the Security View (Views chapter – Page 72) with the latest information about the detected attack patterns. The malicious traffic will be dropped, while the cleaned traffic will be forwarded through the eth1 interface and injected back into the network.



WANGuard Filter Configuration

Active: ☒

Description: DDoS Filtering

IP Address: 192.168.1.100

Inbound Interface: eth0

Outbound Interface: eth1

Monitor Interface: ☒ Inbound ☐ Outbound

Filters Timeout: 60 seconds

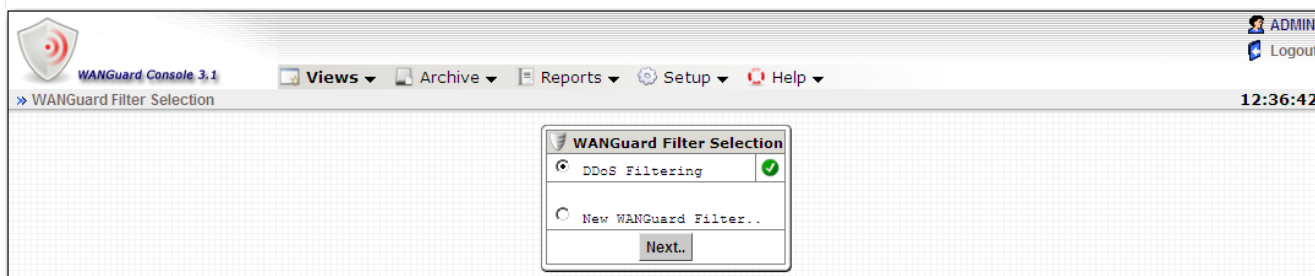
BGP Router: Route Reflector

Filtering Policy: Filter the attack patterns and limit unknown traffic

Details: WANGuard Filter configuration

Change WANGuard Filter Delete WANGuard Filter

After a new WANGuard Filter system is added, the WANGuard Filter Selection window is updated. If there is a green “OK” sign on the right of the WANGuard Filter then the WANGuard Filter system can be used. If there is a “X” red sign instead, then the WANGuard Filter is inactive.

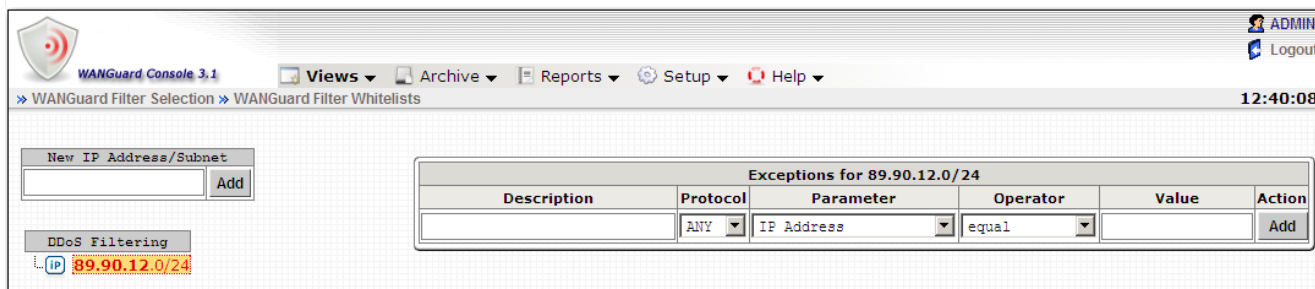


WANGuard Filter Whitelists

A WANGuard Filter Whitelist is a collection of user-created rules that prevents the filtering of critical traffic types. If the filtering policy permits, WANGuard Filter may filter attack patterns that should not be filtered.

WANGuard Filter filters destination ports and destination IP addresses only in worst-case scenarios, when no other attack pattern is detected. In some cases, it's best to let the malicious traffic enter the network than to filter some critical destination IPs and destination ports. For example, if your DNS server is being attacked by spoofed addresses on port 53 UDP, then WANGuard Filter might filter port 53 UDP traffic towards your DNS server making your DNS partially unreachable. In this case it's best to configure a Whitelist that will prevent this behavior.

To configure WANGuard Filter Whitelists you must first select the WANGuard Filter from the WANGuard Filter Selection window and then add IP classes using the New IP Address / Subnet form. The mode of operation is very similar with the one used in IP Zones configuration.



To add a new rule to the Whitelist you must enter the following fields:

- **Description**

Add a description, explanation or comment for the exception.

- **Protocol**

You can choose what type of traffic the rule will match: *ANY, TCP, UDP, ICMP*.

- **Parameter**

Which traffic parameter should be compared: *IP Address, Source Port, Destination Port, Packet Length, IP Packet TimeToLive, IP Protocol Type*.

- **Operator**

Operators for strings and numbers: *equal, non-equal*. Operators for numbers: *less than, greater than*.

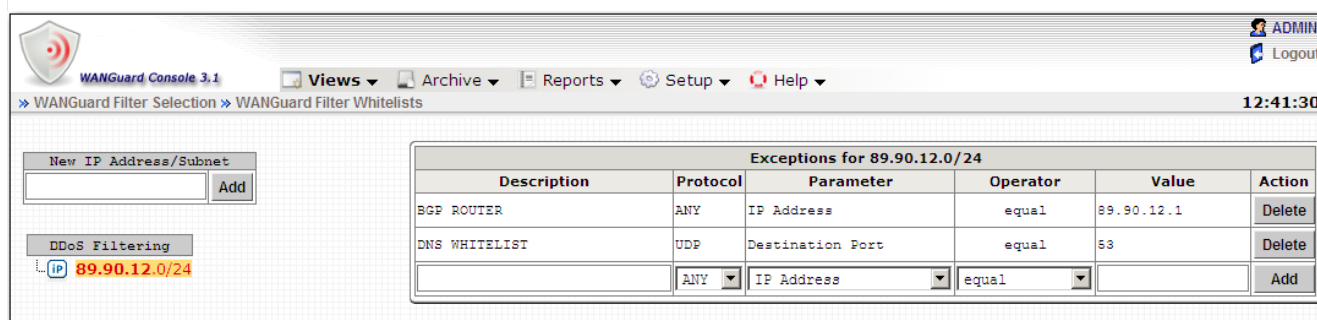
- **Value**

The user-defined value that should be compared.

- **Action**

- *Add* - To add the new rule to the Whitelist.
- *Delete* - To delete an existing rule.

In the following configuration example, when the “DDoS Filtering” WANGuard Filter is activated to protect an IP from 89.90.12.0/24, it will not filter destination IP 89.90.12.1 and destination port 53/UDP.



The screenshot shows the WANGuard Console 3.1 interface. The top menu bar includes Views, Archive, Reports, Setup, and Help. The main window displays the 'WANGuard Filter Selection' and 'WANGuard Filter Whitelists' section. On the left, there is a 'New IP Address/Subnet' input field with an 'Add' button. Below this, the 'DDoS Filtering' section is active, showing a red exclamation point icon and the IP range '89.90.12.0/24'. On the right, a table titled 'Exceptions for 89.90.12.0/24' lists the following rules:

Description	Protocol	Parameter	Operator	Value	Action
BCP ROUTER	ANY	IP Address	equal	89.90.12.1	Delete
DNS WHITELIST	UDP	Destination Port	equal	53	Delete
	ANY	IP Address	equal		Add

When an attack pattern cannot be filtered because it conflicts with the WANGuard Filter's Whitelist then the attack pattern is reported in the Security View with a red exclamation point and is recorded in the Archive with the Whitelist field set to 1.

BGP Router Setup

Users can view, send and withdraw BGP announcements from WANGuard Console through the BGP Operations window (Page 75). All records about BGP announcements are stored in the Archive (Page 87).

WANGuard Sensor and WANGuard Filter can be configured to send and withdraw BGP announcements automatically, in the following cases:

- To protect networks by announcing upstream providers using a special BGP community, that your side does not route the attacked addresses anymore, or that they should null-route the announced addresses. This network protection technique is called black-holing.
- To divert DoS, DDoS and DrDoS traffic through a WANGuard Filter system that will filter the malicious traffic.

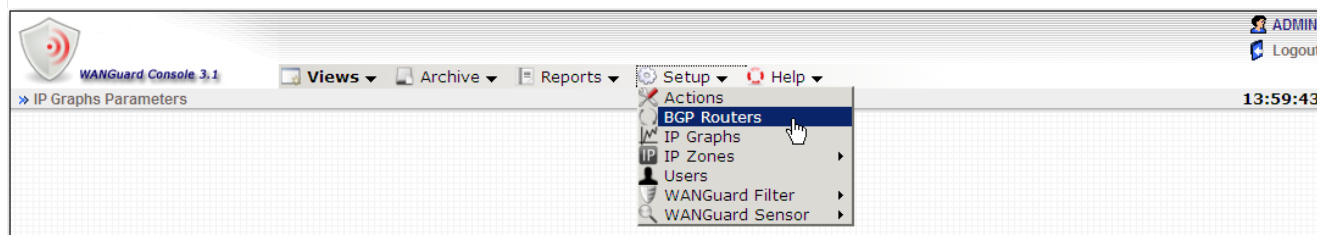
If you do not need any of those features you can safely skip this chapter. Keep in mind that our support team can help you with any configuration issues.

WANGuard Sensor and WANGuard Filter can make use of BGP only if you have previously installed and configured the bgpd daemon included in zebra (<http://www.zebra.org>) or quagga (<http://www.quagga.net>) packages. Bgpd configuration steps are found on Appendix 3 – Configuring Traffic Diversion (Page 99).

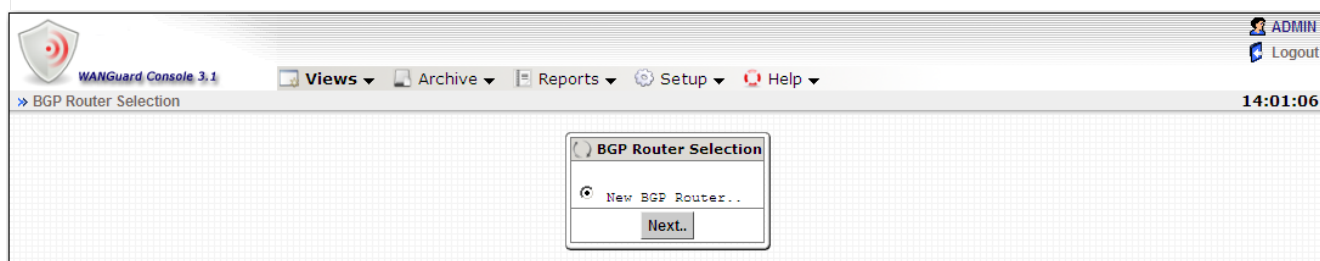
After you have configured bgpd, you must define the BGP router(s) in WANGuard Console. BGP announcements are sent automatically by WANGuard Sensor when a BGP Announcement Action Module (Page 28) is executed. BGP announcements are sent automatically by WANGuard Filter when a BGP router is selected in the WANGuard Filter's configuration (Page 55).

BGP Router Selection

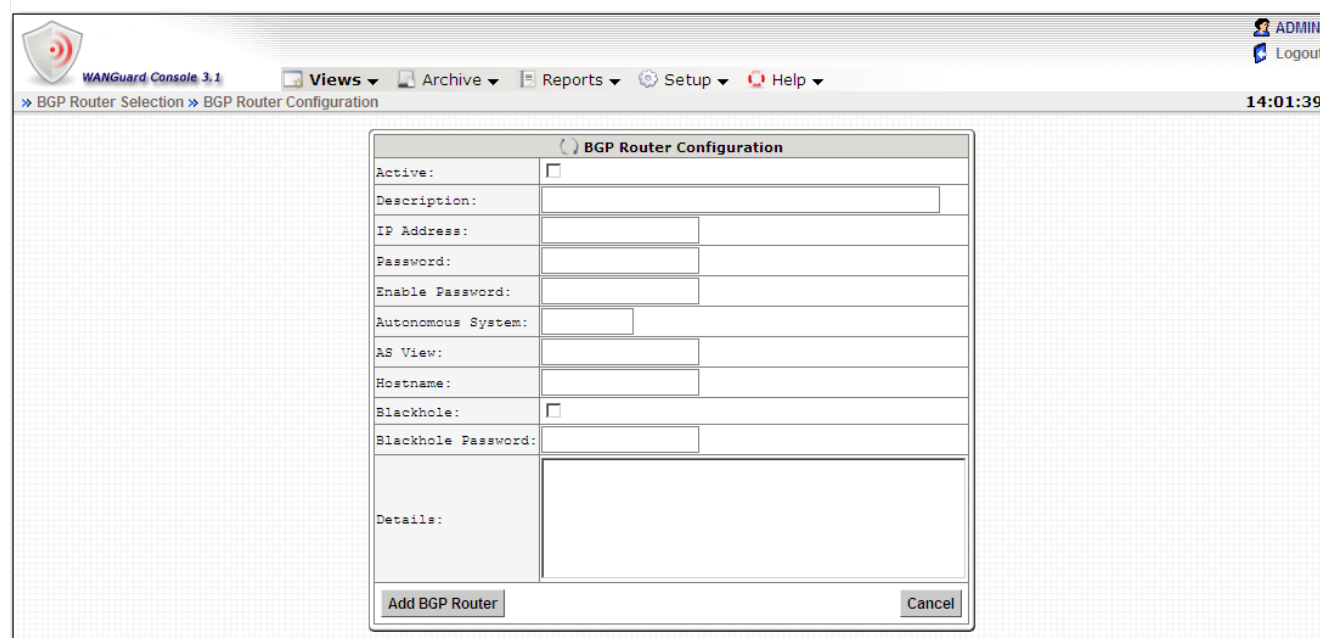
To enter the BGP Router Selection window select BGP Routers from the Setup menu.



If no BGP router was previously configured, the BGP Router Selection window will be displayed empty, with the only option available being to add a new BGP router.



BGP Router Configuration



The BGP Router Configuration window contains the following fields:

- **Active**

The BGP router will be used only if this checkbox is checked.

- **Description**

A short generic description of the BGP router.

- **IP Address**

The IP address of the bgpd host. The *WANGuardController* daemon must be running on the host.

- **Password**

The password required when connecting to the bgpd daemon.

- **Enable Password**

Configuration mode password of the bgpd daemon.

- **Autonomous System**

Autonomous System number used in the bgpd configuration.

- **AS View**

If multiple AS views are defined in the bgpd configuration then you must enter which view do you want to use for this configuration. It can be left empty if no AS views are used.

- **Hostname**

The hostname of the bgpd host. The hostname field must be identical with the hostname defined in the *bgpd.conf* file.

- **Blackhole**

Check if you need the black-hole feature in quagga or zebra.

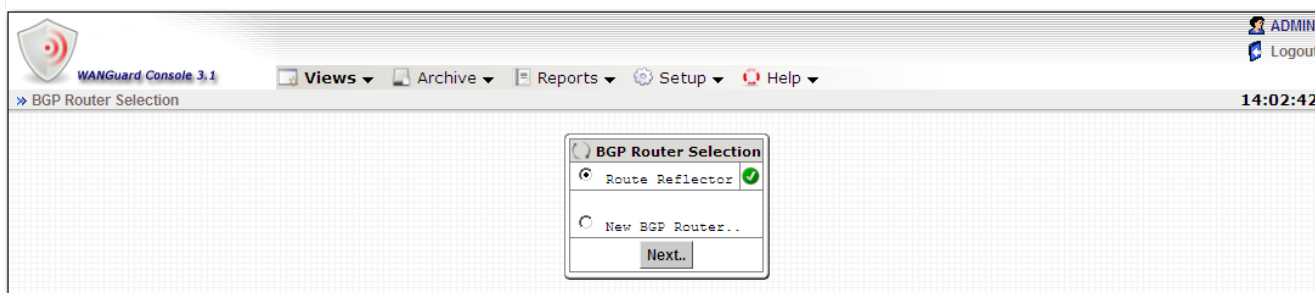
- **Blackhole password**

The password for the zebra or quagga daemons.

- **Details**

You can use this field to store comments regarding the current BGP router configuration.

After adding a new BGP router, the BGP Router Selection window is updated. If there is a green “OK” sign on the right of the BGP Router then the BGP Router is active. If there is a “X” red sign instead, then the BGP Router is inactive.



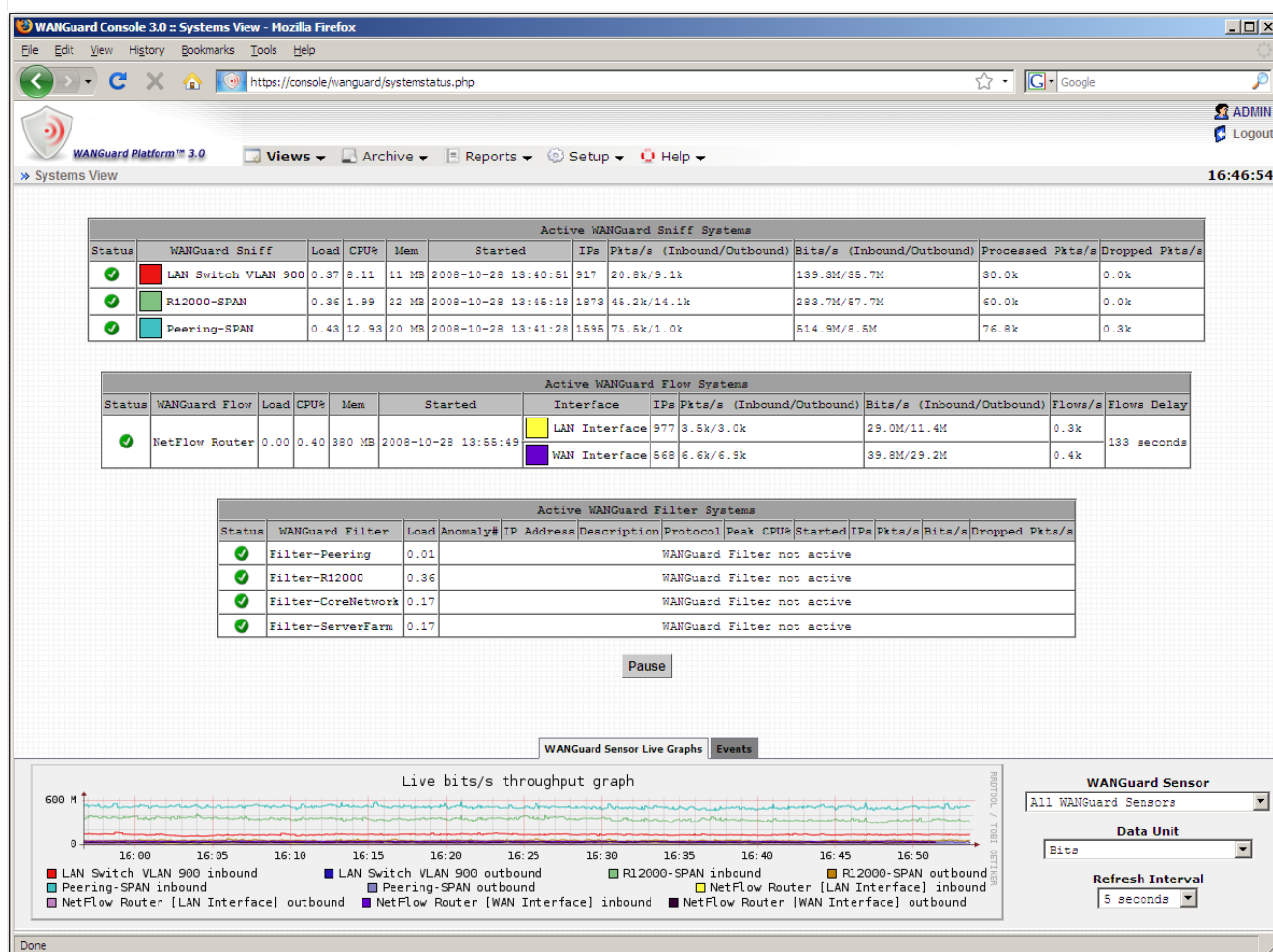
To **edit** or **delete** an existing BGP router you must select it first and then click the <Next..> button.

Views

Views are WANGuard Console windows that display the latest information collected from WANGuard Platform 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**, **Reports View**, **Security View** or **BGP Operations**.

Systems View

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



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	<p>If the active WANGuard Sniff system is functioning properly then a green “checked” arrow is displayed.</p> <p>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 <i>WANGuardController</i> daemon is running on all systems.</p>
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	<p>If the active WANGuard Flow system is functioning properly then a green “checked” arrow is displayed.</p> <p>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 <i>WANGuardController</i> daemon is running on all systems.</p>
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	<p>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.</p> <p>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.</p>

Active WANGuard Filter Systems Table

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

Status	<p>If the active WANGuard Filter system is functioning properly then a green “checked” arrow is displayed.</p> <p>If WANGuard Console cannot manage or reach the WANGuard Filter system then a red “X” icon is displayed. In this case make sure that WANGuard Filter is configured correctly, read the Events Log and make sure that the <i>WANGuardController</i> daemon is running on all systems.</p>
WANGuard Filter	Displays the description of the WANGuard Filter system.
Load	The load of the operating system for the last 5 minutes.
Anomaly#	The index of the traffic anomaly mitigated by the WANGuard Filter system. If this number is clicked then a new window opens with additional details about the traffic anomaly.
IP Address	The IP address from your network involved in the traffic anomaly. If the IP address is clicked then a new window opens with detailed information about reverse DNS, ISP, Country, AS number etc.
Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: <i>SYN, TCP, UDP, ICMP, OTHER</i> .
Peak CPU%	The maximum CPU percent used by the WANGuard Filter process.
Started	The date and time when the WANGuard Filter system was activated.
IPs	The number of unique IP addresses detected making traffic with the attacked IP address.
Pkts/s	The packets/second throughput towards the attacked IP address.
Bits/s	The bits/second throughput towards the attacked IP address.
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 Filter installation.

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

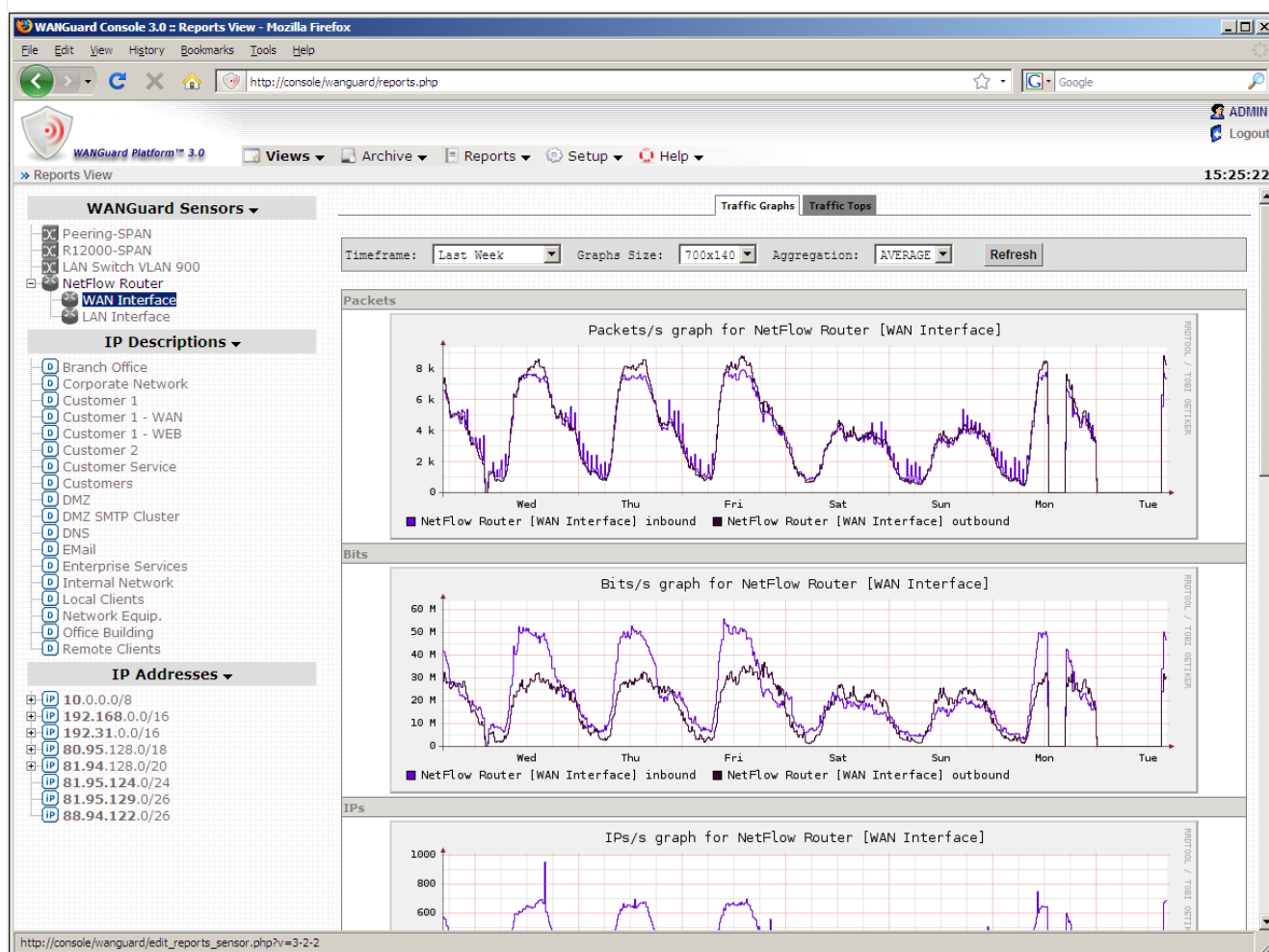
The Events Tab provides a list with the latest events recorded in the Events Log. Every field is explained in the Events Log section of the Archive chapter (Page 88).

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.

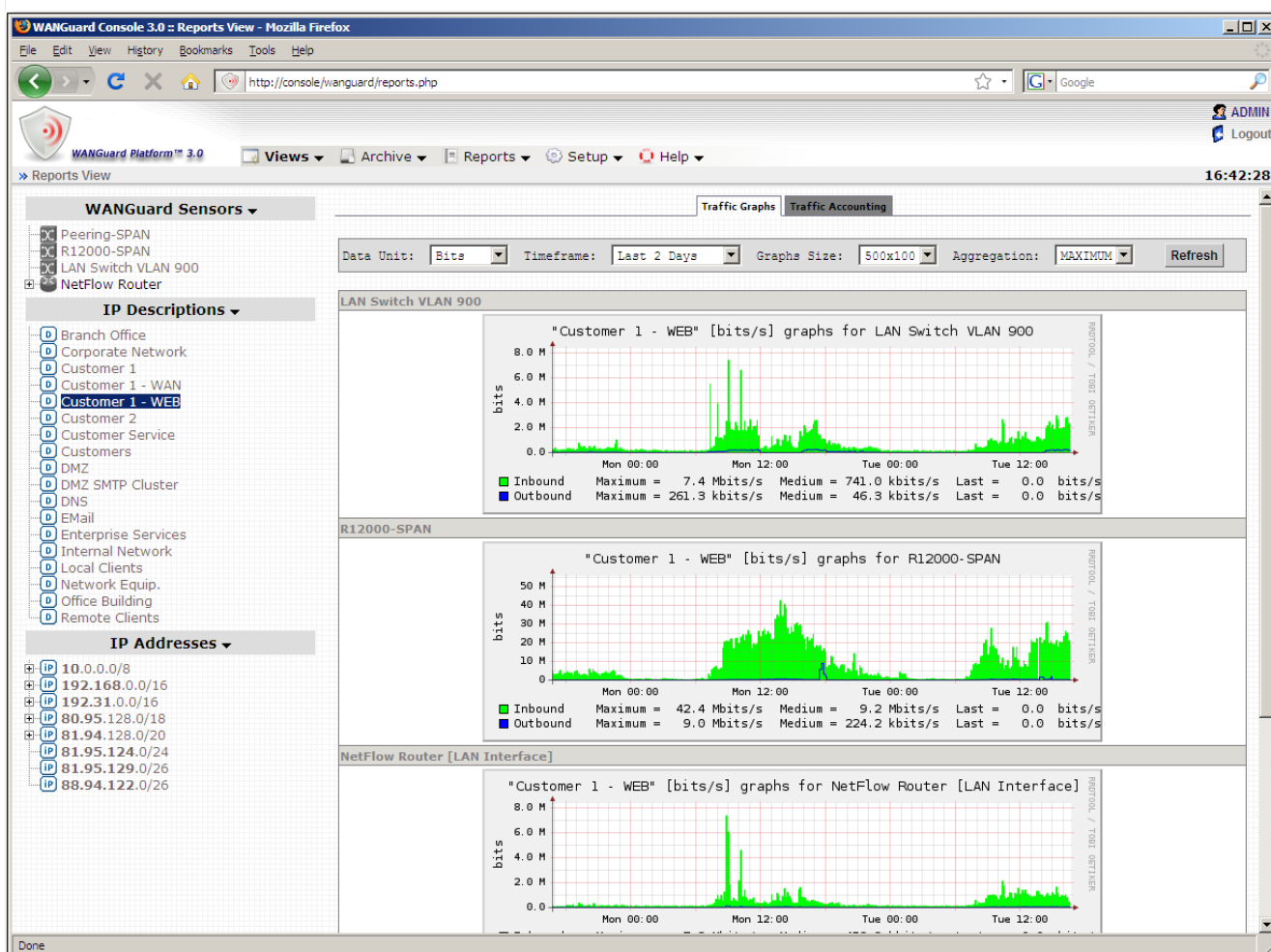


The **Traffic Tops** area provides live statistics about top hosts (“talkers”), top TCP ports, top UDP ports, top IP protocols and top AS Numbers (only when NetFlow is used). This tab is not available if the selected WANGuard Sensor does not have the “Top” option activated in its configuration.

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.

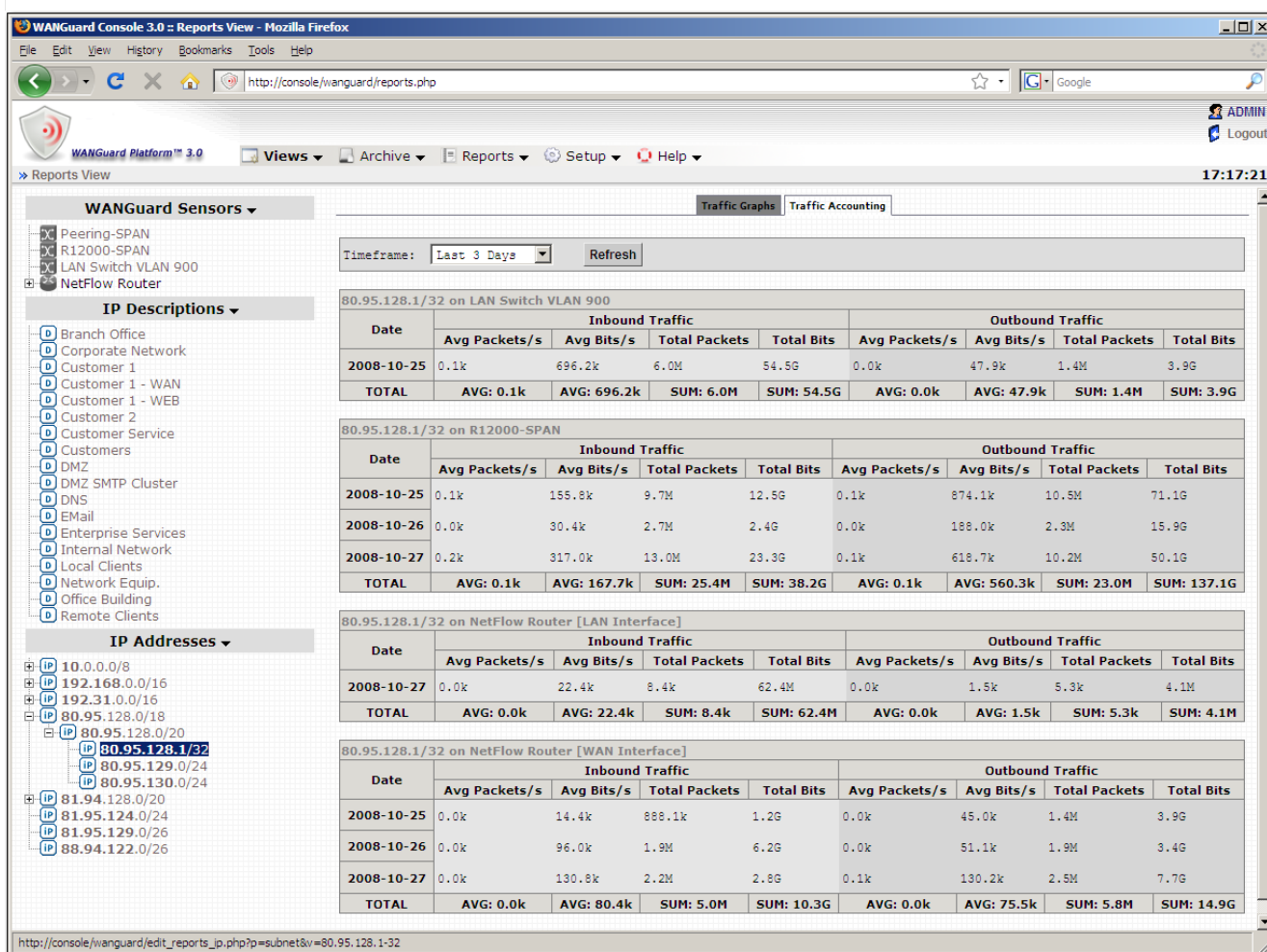
The **Traffic Accounting** area contains a traffic accounting report generated for the hosts or networks that have the selected IP Description.



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.



The screenshot displays the WANGuard Console 3.0 Reports View in Mozilla Firefox. The interface includes a sidebar with navigation menus for WANGuard Sensors, IP Descriptions, and IP Addresses. The main content area shows the Traffic Accounting tab for the selected IP address 80.95.128.1/32. The data is presented in four tables, each showing traffic statistics for the last 3 days.

WANGuard Sensors

- Peering-SPAN
- R12000-SPAN
- LAN Switch VLAN 900
- NetFlow Router

IP Descriptions

- Branch Office
- Corporate Network
- Customer 1
- Customer 1 - WAN
- Customer 1 - WEB
- Customer 2
- Customer Service
- Customers
- DMZ
- DMZ SMTP Cluster
- DNS
- Email
- Enterprise Services
- Internal Network
- Local Clients
- Network Equip.
- Office Building
- Remote Clients

IP Addresses

- 10.0.0.0/8
- 192.168.0.0/16
- 192.31.0.0/16
- 80.95.128.0/18
- 80.95.128.0/20
- 80.95.128.1/32**
- 80.95.129.0/24
- 80.95.130.0/24
- 81.94.128.0/20
- 81.95.124.0/24
- 81.95.129.0/26
- 88.94.122.0/26

Traffic Accounting Data

Timeframe: Last 3 Days Refresh

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

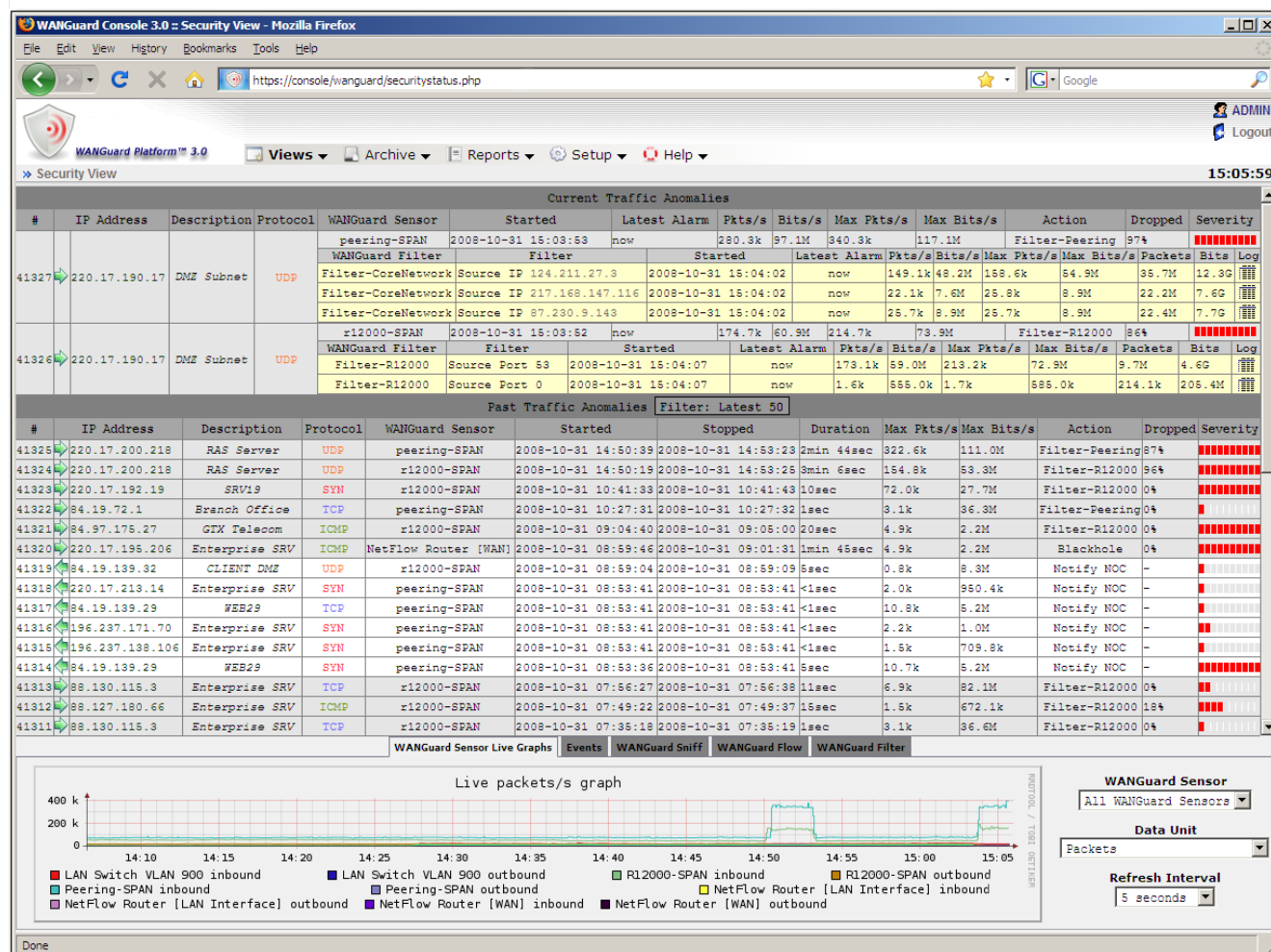
Security View

The Security View displays the latest traffic and security related information collected from WANGuard Sensor and WANGuard Filter systems. This View is split horizontally in two sides.

The upper side contains a table with **Current Traffic Anomalies** and a table with **Past Traffic Anomalies**.

The bottom side contains a tabbed interface that provides access to WANGuard Sensor Live Graphs, Events and system information about active WANGuard Platform components. All the information contained on the bottom side is explained in the Systems View chapter (Page 64).

Below you can see a screenshot taken during two DDoS attacks.



Current Traffic Anomalies

The Current Traffic Anomalies table is visible only when WANGuard Sensor detects one or more active traffic anomalies. Every row in the table represents an active traffic anomaly. The traffic anomalies are sorted by start time in descending order. The active traffic anomalies are presented in the following format:

#	The unique index number of the traffic anomaly. If this number is clicked then a new window opens with a list of activated WANGuard Filter systems for this traffic anomaly.
IP Address	<p>The IP address from your network involved in the traffic anomaly.</p> <p>In the front of the IP address, the graphic arrow indicates the direction of the traffic anomaly. When the arrow is pointing to the right, the threshold values were exceeded for inbound traffic. When the arrow is pointing to the left, the threshold values were exceeded for outbound traffic. Inbound anomalies are also represented by a gray background, while outbound anomalies are represented by a white background.</p> <p>If the IP address is clicked then a new window opens with detailed information about reverse DNS, ISP, Country, AS number etc.</p>
Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: <i>SYN, TCP, UDP, ICMP, OTHER</i> .
WANGuard Sensor	The description of the WANGuard Sensor that detected the traffic anomaly.
Started	The time and date when WANGuard Sensor began the detection of the traffic anomaly.
Latest Alarm	How much time passed since the last detection of the traffic anomaly.
Pkts/s	The latest packets/second throughput for the anomalous traffic.
Bits/s	The latest bits/second throughput for the anomalous traffic.
Max Pkts/s	The maximum packets/second throughput reached by the anomalous traffic.
Max Bits/s	The maximum bits/second throughput reached by the anomalous traffic.
Action	The description of the Action executed for this traffic anomaly.
Dropped	The percent of the anomalous traffic filtered by one or more WANGuard Filter systems.
Severity	The severity field represents graphically the ratio between the anomalous traffic and threshold values. Every red bar means 100% of the threshold value. The exact ratio is displayed as a tool-tip.

If one or more WANGuard Filter systems are activated to detect the attack patterns in a traffic anomaly, then a new yellow table will show up in the same traffic anomaly row. This yellow table contains information about the attack patterns in the following format:

WANGuard Filter	The description of the WANGuard Filter that detected the attack pattern.
Filter	<p>The filter applied by WANGuard Filter to remove the attack pattern's traffic. WANGuard Filter dynamically applies the following filter types: <i>Source IP, Source Port, Destination Port, Packet Length, TimeToLive, IP Protocol</i>.</p> <p>The filters are applied only when the filtering policy allows traffic filtering. If the filter conflicts with the WANGuard Filter's Whitelist, then a red exclamation point shows up and the filter is not applied.</p>
Started	The date and time when the attack pattern was first detected.
Latest Alarm	How much time passed since the last detection of the attack pattern.
Pkts/s	The latest packets/second throughput for the traffic matching the attack pattern.
Bits/s	The latest bits/second throughput for the traffic matching the attack pattern.
Max Pkts/s	The maximum packets/second throughput for the traffic matching the attack pattern.
Max Bits/s	The maximum bits/second throughput for the traffic matching the attack pattern.
Packets	The number of packets counted in the traffic matching the attack pattern.
Bits	The number of bits counted in the traffic matching the attack pattern.
Log	If this icon is clicked then a new window opens with additional details about the attack pattern.

Past Traffic Anomalies

The Past Traffic Anomalies table shows inactive traffic anomalies sorted by time in descending order, that match the Filter from the header of the table. By default, the Filter is set to show only the latest 50 inactive traffic anomalies. By clicking the Filter area you can change the Filter type and values.

Every row in the table represents an inactive traffic anomaly. The inactive traffic anomalies are presented in the following format:

#	The unique index number of the traffic anomaly. If this number is clicked then a new window
----------	---

	opens with a list of activated WANGuard Filter systems for this traffic anomaly.
IP Address	<p>The IP address from your network involved in the traffic anomaly.</p> <p>In the front of the IP address, the graphic arrow indicates the direction of the traffic anomaly. When the arrow is pointing to the right, the thresholds were exceeded for inbound traffic. When the arrow is pointing to the left, the thresholds were exceeded for outbound traffic. Inbound anomalies are also represented by a gray background, while outbound anomalies are represented by a white background.</p> <p>If the IP address is clicked then a new window opens with detailed information about reverse DNS, ISP, Country, AS number etc.</p>
Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: <i>SYN, TCP, UDP, ICMP, OTHER</i> .
WANGuard Sensor	The description of the WANGuard Sensor that detected the traffic anomaly.
Started	The time and date when WANGuard Sensor began the detection of the traffic anomaly.
Stopped	The time and date when WANGuard Sensor ended the detection of the traffic anomaly.
Duration	The duration of the traffic anomaly.
Max Pkts/s	The maximum packets/second throughput reached by the anomalous traffic.
Max Bits/s	The maximum bits/second throughput reached by the anomalous traffic.
Action	The description of the Action executed for this traffic anomaly.
Dropped	The percent of the anomalous traffic filtered by one or more WANGuard Filter systems.
Severity	The severity field represents graphically the ratio between the anomalous traffic and threshold values. Every red bar means 100% of the threshold value. The exact ratio is displayed as a tool-tip.

BGP Operations

The BGP Operations window provides live insight on BGP announcements made either by WANGuard Sensor through the BGP Announcement Action Module, or by WANGuard Filter for traffic diversion. The content is refreshed flicker-free every 5 seconds.

If you have *Administrator User* privileges then can **add** your own BGP announcements and you can **manually remove** existing BGP announcements. To add a new BGP announcement you must enter the

IP/Subnet, select the BGP router and provide comments to the form in the upper section of the window. If the announcement was successful, the BGP announcements table below will contain the new BGP announcement.

Users with *Normal User* privileges can only view the BGP announcements list.

The BGP announcements table contains the following fields:

BGP Router	The BGP Router description as defined in the BGP router configuration (Page61).
IP Address/Subnet	The IP address and the subnet in CIDR notation.
Start Time	The time and date when the BGP announcement was sent.
Details	<p>This field contains comments or details about the announcement.</p> <p>If the announcement was sent manually using the form in the upper section, the Details field contains the details entered in the form.</p> <p>If the announcement was sent automatically by WANGuard Sensor or by WANGuard Filter then the Details field contains the index of the traffic anomaly that generated the BGP announcement. By clicking the traffic anomaly index a new window will open that provides details from the Archive regarding the traffic anomaly.</p>
Action	The Action field is visible only if the logged on user has Administrator privileges. The Action field contains a button for the manual removal of the BGP announcement.

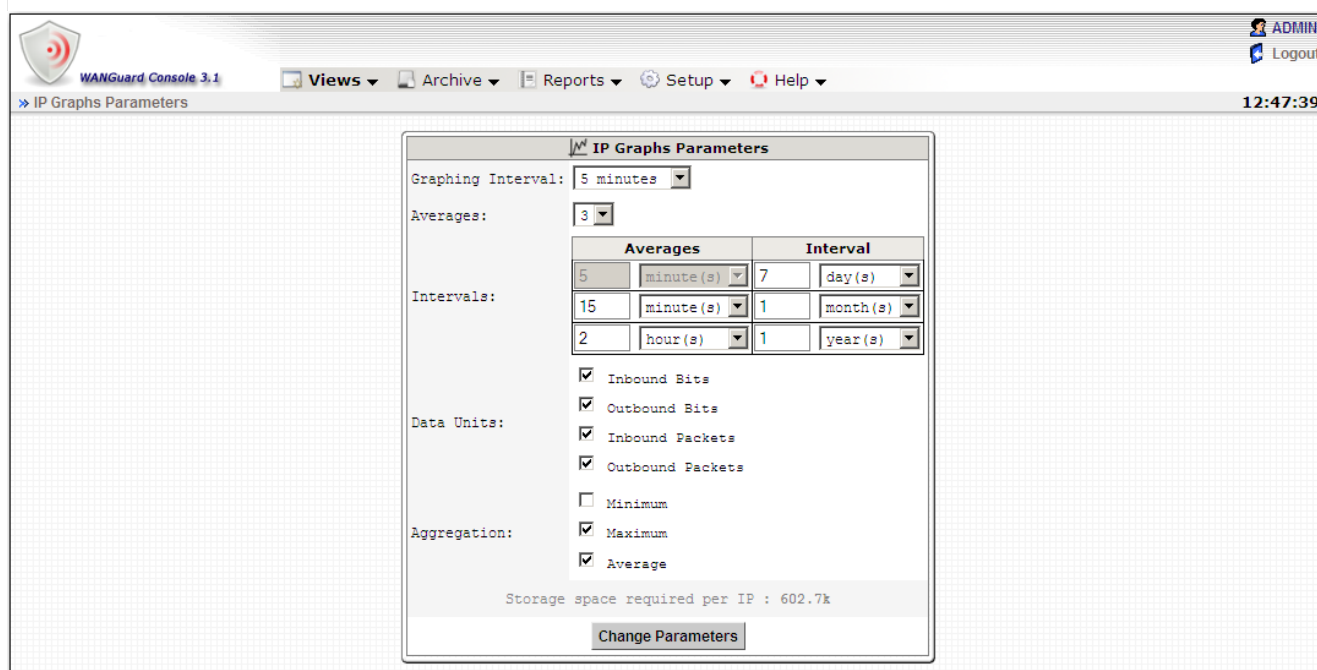
You can view details about old BGP announcements by accessing the BGP Logs (Page 87).

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 69).

IP Traffic Graphs Setup

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



WANGuard Console 3.1

Views Archive Reports Setup Help

IP Graphs Parameters

ADMIN Logout 12:47:39

IP Graphs Parameters

Graphing Interval: 5 minutes

Averages: 3

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

Intervals:

Data Units:

- ☒ Inbound Bits
- ☒ Outbound Bits
- ☒ Inbound Packets
- ☒ Outbound Packets
- ☐ Minimum
- ☒ Maximum
- ☒ Average

Aggregation:

Storage space required per IP : 602.7k

Change Parameters

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.

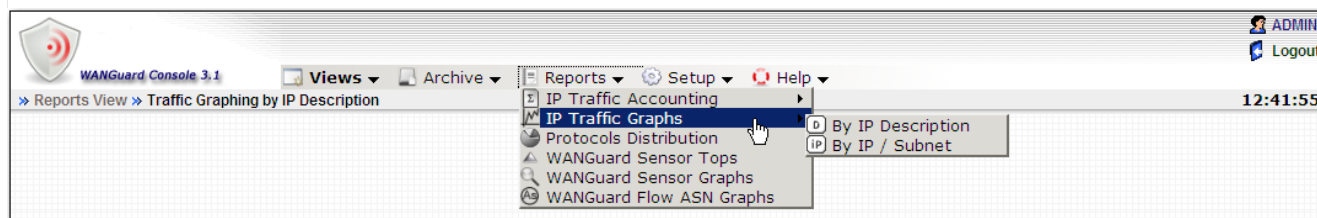
The **Data Units** options lets you select the traffic parameters that will be stored.

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 77).

- **Graph Size**

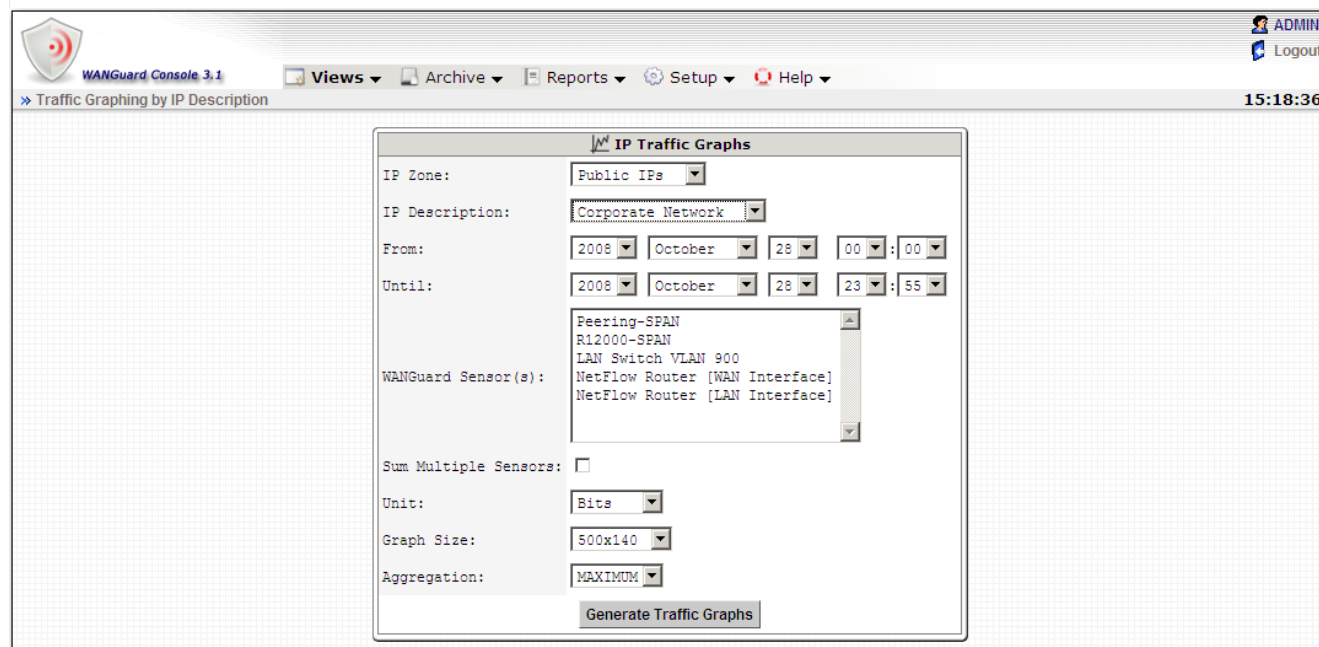
Select the graph size.

- **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 77).

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.



The screenshot shows the WANGuard Console 3.1 interface. The main menu bar includes Views, Archive, Reports, Setup, and Help. The current page is 'Traffic Graphing by IP Description'. The 'IP Traffic Graphs' window is open, displaying the following configuration:

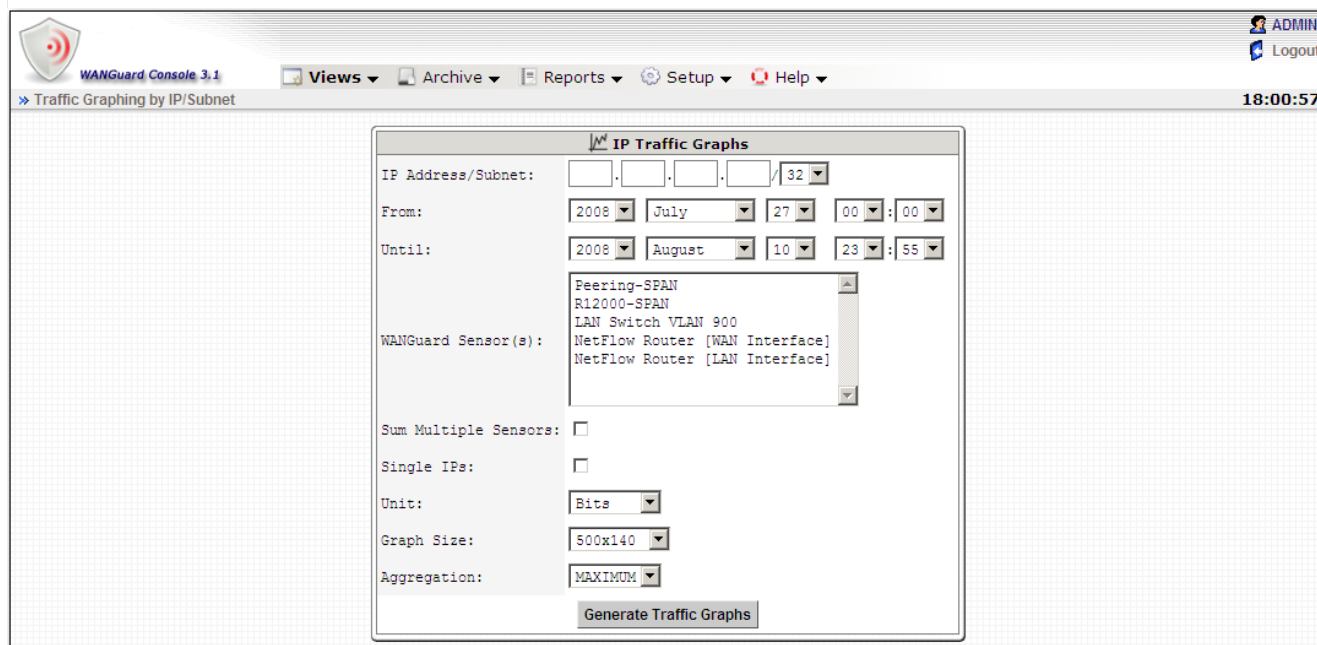
- IP Zone:** Public IPs
- IP Description:** Corporate Network
- From:** 2008, October, 28, 00:00
- Until:** 2008, October, 28, 23:55
- WANGuard Sensor(s):** Peering-SPAN, R12000-SPAN, LAN Switch VLAN 900, NetFlow Router [WAN Interface], NetFlow Router [LAN Interface]
- Sum Multiple Sensors:** ☐
- Unit:** Bite
- Graph Size:** 500x140
- Aggregation:** MAXIMUM
- Generate Traffic Graphs** button

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.



The screenshot shows the WANGuard Console 3.1 interface. The main window title is 'WANGuard Console 3.1' and the current view is 'Traffic Graphing by IP/Subnet'. The time is 18:00:57. The 'IP Traffic Graphs' dialog box is open, showing the following fields:

- 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
- Generate Traffic Graphs button

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 16).

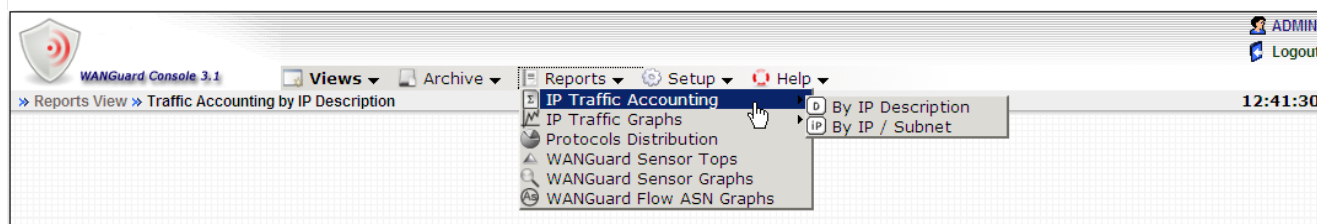
Check the **Single IPs** option if you want a different traffic graph displayed for every IP address contained in the selected subnet. For example, when this option is used with a /24 CIDR then 256 traffic graphs are displayed, one for each IP address in the "C" class.

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**

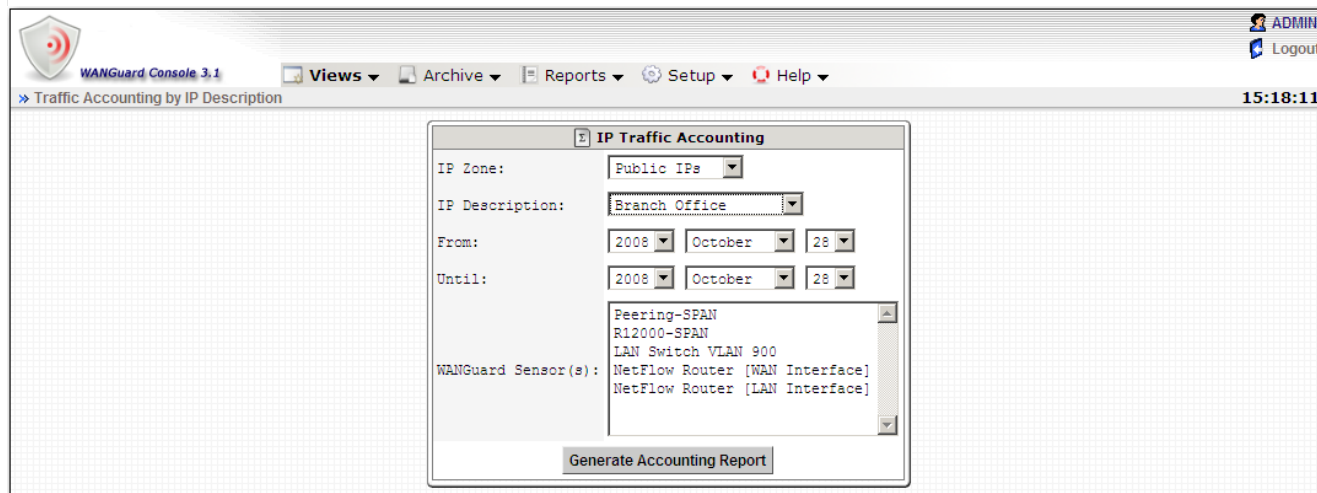
Enter the desired time-frame.

- **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.

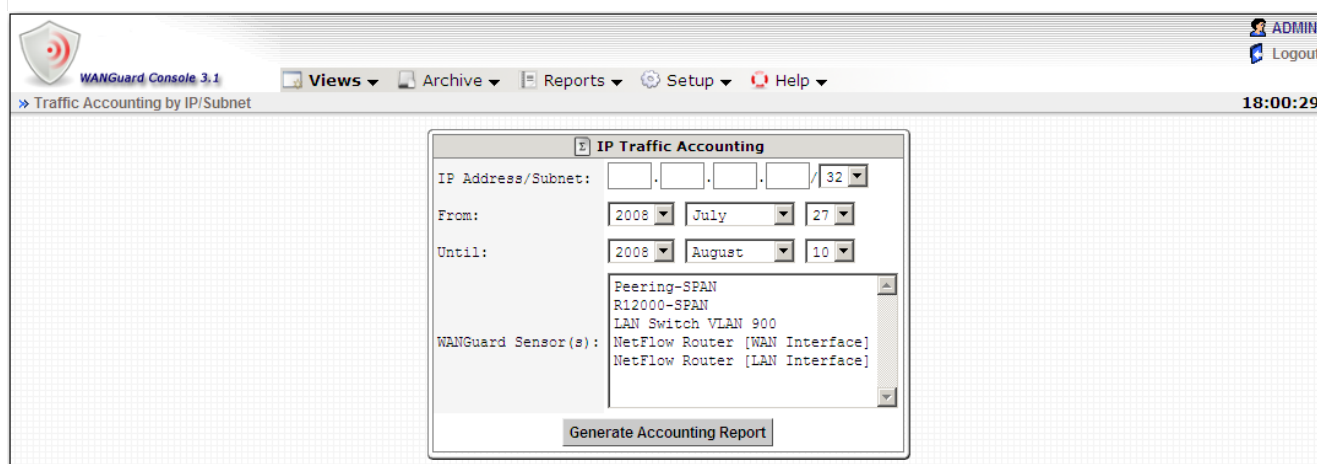


The **From**, **Until** and **WANGuard Sensor(s)** fields are explained in the beginning of this section.

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.



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

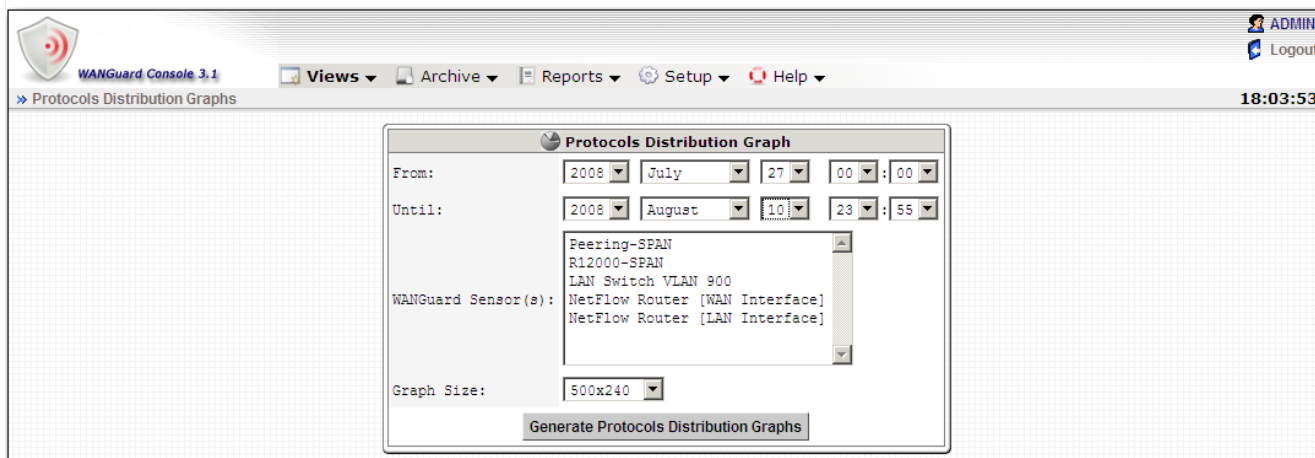
For the **IP Address / Subnet** fields use the CIDR notation. To generate traffic accounting reports for hosts - not networks, select the /32 CIDR. For more information about CIDR consult the Network Basics You Should Be Aware Of chapter (Page 16).

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.

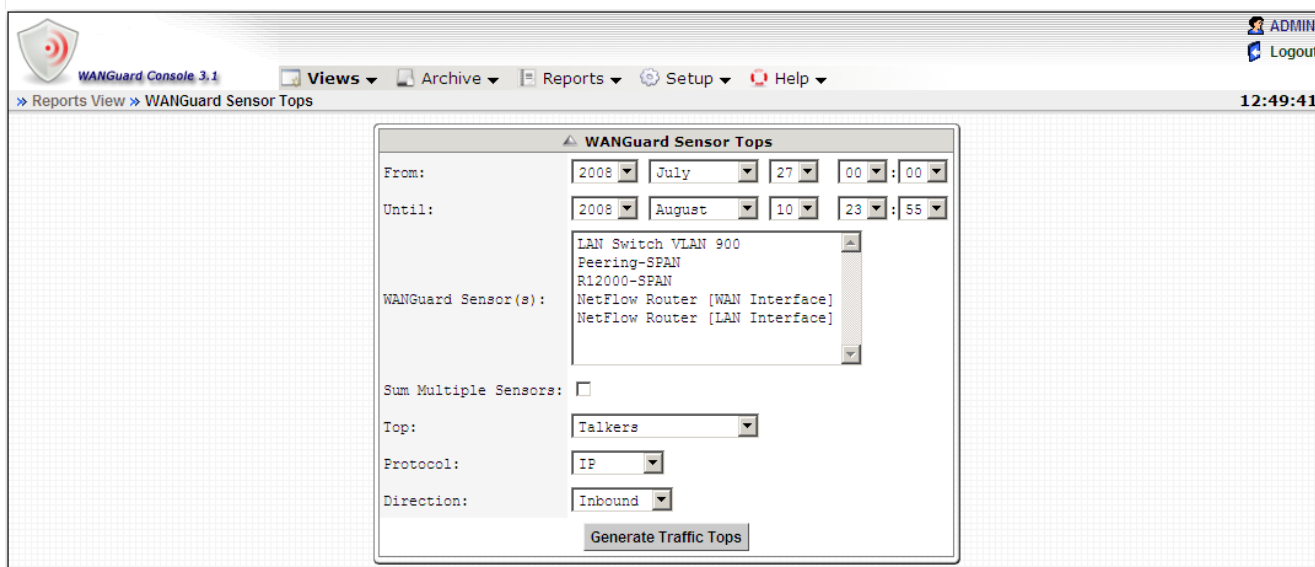


The screenshot shows the WANGuard Console 3.1 interface. The top menu bar includes Views, Archive, Reports, Setup, and Help. The main window displays the Protocols Distribution Graph configuration. The 'From' field is set to 2008 July 27 00:00, and the 'Until' field is set to 2008 August 10 23:55. The 'WANGuard Sensor(s):' list includes Peering-SPAN, R12000-SPAN, LAN Switch VLAN 900, NetFlow Router [WAN Interface], and NetFlow Router [LAN Interface]. The 'Graph Size' is set to 500x240. A 'Generate Protocols Distribution Graphs' button is at the bottom.

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

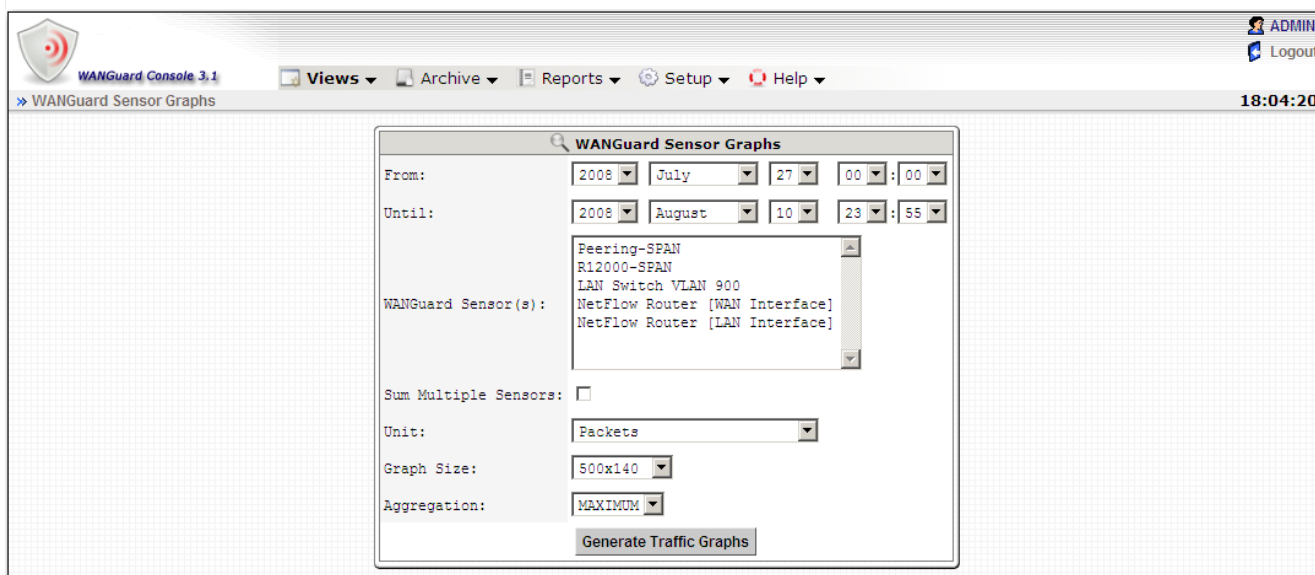
WANGuard Sensor systems configured with the “Top” option collect data that can be used to generate top statistics for any selected time-frame. Available statistics are: top hosts (“talkers”), top TCP ports, top UDP ports, top IP protocols and top AS Numbers (only when NetFlow is used). Top generation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



The screenshot shows the WANGuard Console 3.1 interface. The top menu bar includes Views, Archive, Reports, Setup, and Help. The main window displays the WANGuard Sensor Tops configuration. The 'From' field is set to 2008 July 27 00:00, and the 'Until' field is set to 2008 August 10 23:55. The 'WANGuard Sensor(s):' list includes LAN Switch VLAN 900, Peering-SPAN, R12000-SPAN, NetFlow Router [WAN Interface], and NetFlow Router [LAN Interface]. The 'Sum Multiple Sensors' checkbox is unchecked. The 'Top' dropdown is set to Talkers, the 'Protocol' dropdown is set to IP, and the 'Direction' dropdown is set to Inbound. A 'Generate Traffic Tops' button is at the bottom.

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.



The screenshot shows the WANGuard Console 3.1 interface. The top navigation bar includes 'Views', 'Archive', 'Reports', 'Setup', and 'Help'. The 'Reports' menu is selected, leading to the 'WANGuard Sensor Graphs' page. The form contains the following fields:

- From:** 2008, July, 27, 00:00
- Until:** 2008, August, 10, 23:55
- WANGuard Sensor(s):** A list box containing: Peering-SPAN, RI2000-SPAN, LAN Switch VLAN 900, NetFlow Router [WAN Interface], and NetFlow Router [LAN Interface].
- Sum Multiple Sensors:** An unchecked checkbox.
- Unit:** A dropdown menu set to 'Packets'.
- Graph Size:** A dropdown menu set to '500x140'.
- Aggregation:** A dropdown menu set to 'MAXIMUM'.
- Generate Traffic Graphs:** A button at the bottom of the form.

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

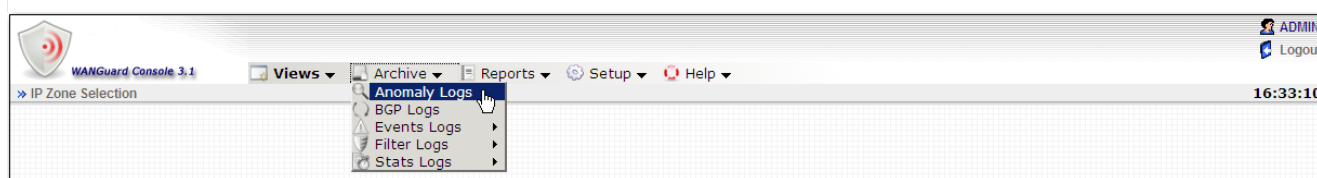
The WANGuard Flow ASN Graphs page will not be accessible through the Menu if there is no previously configured WANGuard Flow system.

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 than 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 Platform 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.



Anomaly Logs

The Anomaly Logs contain details about every traffic anomaly detected by WANGuard Sensor systems. Every traffic anomaly record contains the following fields:

Anomaly#	The unique index number of the traffic anomaly. If this number is clicked then a new window opens with a list of activated WANGuard Filter systems for the traffic anomaly.
WANGuard Sensor	The description of the WANGuard Sensor that detected the traffic anomaly.
IP Address	The IP address from your network involved in the traffic anomaly. If the IP address is clicked then a new window opens with detailed information about reverse DNS, ISP, Country, AS number etc.
Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Details	This field contains information provided by third party applications.
Protocol	The traffic type that exceeded the threshold value: <i>SYN, TCP, UDP, ICMP, OTHER</i> .
Direction	The direction of the anomalous traffic: <i>inbound, outbound</i> .
Latest Pkts/s	The latest packets/second throughput reached by the anomalous traffic.
Latest Bits/s	The latest bits/second throughput reached by the anomalous traffic.

Peak Pkts/s	The maximum packets/second throughput reached by the anomalous traffic.
Peak Bits/s	The latest bits/second throughput reached by the anomalous traffic.
Threshold Pkts/s	The threshold packets/second value for the IP address and protocol.
Threshold Bits/s	The threshold bits/second value for the IP address and protocol.
Concurrency	The concurrency value for the IP address extracted from the WANGuard Sensor's IP Zone.
Latest Total Pkts/s	The latest packets/second throughput recorded for the IP address by WANGuard Sensor.
Latest Total Bits/s	The latest bits/second throughput recorded for the IP address by WANGuard Sensor.
Action	The description of the Action executed for this traffic anomaly.
From Time	The time and date when WANGuard Sensor started the detection of the traffic anomaly.
Until Time	The time and date when WANGuard Sensor stopped detecting the traffic anomaly.
Packets	The number of packets recorded by WANGuard Sensor in the anomalous traffic.
Bits	The number of bits recorded by WANGuard Sensor in the anomalous traffic.
WANGuard Filters	The number of WANGuard Filter systems activated to mitigate or analyze the traffic anomaly.
BGP Log	Bgpd and zebra commands executed by the BGP Announcement Action Module or by the activated WANGuard Filter systems.
Traffic Sample	If you are using WANGuard Sniff, this field contains a tcpdump-like log with a sample of 100 packets from the anomalous traffic. If you are using WANGuard Flow this field is empty.
Emails	This field contains the contents of the emails sent by the WANGuard Sensor Email Action Module or by the WANGuard Filter Action Module.

BGP Logs

BGP Logs contain details about the BGP announcements sent by WANGuard Platform components. Every BGP announcement record contains the following fields:

Anomaly#	The traffic anomaly that generated the BGP announcement. This field is empty if the BGP announcement was sent manually through WANGuard Console.
-----------------	--

Router	The BGP router used to send the BGP announcement.
IP Address	The announced IP address.
Subnet	The announced subnet in CIDR form. It is /32 for single IP addresses.
Start Time	The date & time when the BGP announcement was sent.
Stop Time	The date & time when the BGP announcement was deleted.
Status	The current status of the BGP announcement: <i>FINISHED, ACTIVE, WAITING</i> .
User	If the BGP announcement was sent manually then this field contains the logged user.
Details	If the BGP announcement was sent manually then this field contains the details field.

Events Logs

Events Logs contain all events generated by WANGuard Platform 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 Platform component that generated the event.
Anomaly#	If the event was generated by a WANGuard Filter system then this field contains the traffic anomaly index for which the WANGuard Filter was activated. Otherwise the field is empty.
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 22).
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.

Filter Logs

The Filter Logs sub-menu contains Attacks Pattern Logs and WANGuard Filter Logs:

Attacks Patterns

The Attacks Patterns table contains details about every attacks pattern detected by WANGuard Filter systems. Each record has the following format:

Anomaly#	The index of the traffic anomaly for which the WANGuard Filter was activated.
Victim	The IP address from your network involved in the traffic anomaly.
Protocol	The traffic type that exceeded the threshold: <i>SYN, TCP, UDP, ICMP, OTHER</i> .
Direction	The direction of anomalous traffic: <i>inbound, outbound</i> .
Filter Type	The attack pattern type: <i>Source IP, Source Port, Destination Port, Packet Length, TimeToLive, IP Protocol</i> . If the filtering policy permits it, WANGuard Filter dynamically applies filters that match the attack pattern.
Filter Value	The attack pattern value.
Start Time	The date and time when the attack pattern was first detected.
Stop Time	The date and time when the attack pattern was last detected.
Peak Pkts/s	The maximum packets/second throughput of the traffic matching the attack pattern.
Peak Bits/s	The maximum bits/second throughput of the traffic matching the attack pattern.
Packets	The number of IP packets matching the attack pattern.
Bits	The number of bits matching the attack pattern.
Latest Pkts/s	Most recent packets/second throughput of the traffic matching the attack pattern.
Latest Bits/s	Most recent bits/second throughput of the traffic matching the attack pattern.
Traffic Sample	This field contains a tcpdump-like log with a sample of 100 packets from the traffic matching the attack pattern.
Emails	This field contains the content of the emails sent by the WANGuard Filter Email Action Module.
Whitelisted	If the filter could not be applied because it conflicted with the WANGuard Filter's Whitelist, this value is 1. Otherwise the value is 0.

WANGuard Filters

The WANGuard Filters table contains details about all activated WANGuard Filter systems. All fields recorded in the table are explained below:

Filter#	The index number of the activated WANGuard Filter system. If this number is clicked then a new window opens with the list of attack patterns detected by the WANGuard Filter system.
Anomaly#	The index of the traffic anomaly for which the WANGuard Filter is activated.
WANGuard Filter	The description of the activated WANGuard Filter.
Filtered Pkts	The number of packets filtered by the activated WANGuard Filter.
Filtered Bits	The number of bits filtered by the activated WANGuard Filter.
Filter Peak Pkts/s	The maximum packets/second throughput recorded by the activated WANGuard Filter.
Filter Peak Bits/s	The maximum bits/second throughput recorded by the activated WANGuard Filter.
Latest Filter Pkts/s	Most recent packets/second throughput recorded by the activated WANGuard Filter.
Latest Filter Bits/s	Most recent bits/second throughput recorded by the activated WANGuard Filter.
Start Time	The date and time when the WANGuard Filter system was activated.
Stop Time	The date and time when the WANGuard Filter system was stopped.
Peak CPU%	The maximum CPU percent used by the WANGuard Filter process.

Stats Logs

Statistics Logs contain traffic statistics recorded by WANGuard Platform 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 Platform 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 than inter VLAN traffic use CatOS 7.2 or higher and issue the following command:

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

And enable NDE:

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

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

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

Configuring NDE on a Native IOS Device

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

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

The following commands break up flows into shorter segments: ~1 minute for active flows and ~ 30 seconds for inactive flows. 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;
            }
        }
    }
}
```

Appendix 2 – Conditional & Dynamic Parameters

#	Conditional Parameter	Type	Dynamic Parameter	Description
General Parameters				
1	Anomaly #	Number	{anomaly_id}	The unique identification number of the traffic anomaly.
2	IP Address	String	{ip}	It represents the IP address from your network, involved in the traffic anomaly.
3	IP Description	String	{description}	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
4	Protocol (syn, udp, tcp, icmp, other)	String	{protocol}	The traffic type that exceeded the threshold value.
5	Direction (inbound, outbound)	String	{direction}	The direction of the traffic anomaly, inbound or outbound.
6	Severity	Number	{severity}	The severity field represents the ratio between the anomalous traffic rate and threshold value.
7	Action Description	String	{action}	The description of the Action executed for this traffic anomaly, as extracted from WANGuard Sensor's IP Zone.
8	WANGuard Sensor's IP address	String	{wanguardsensor_ip}	The WANGuard Sensor's IP address, as defined in the WANGuard Flow / Sniff Configuration.
9	WANGuard Sensor's Description	String	{wanguardsensor_description}	The WANGuard Sensor's description as defined in the WANGuard Flow / Sniff Configuration.
10	Tick	Number	{tick}	The number of times the WANGuard Sensor detected anomalous traffic during the traffic anomaly's lifetime.
11	BGP Log Size (bytes)	Number	{bgplog_size}	The size in bytes of the BGP logs. Useful as a precondition in Action Modules when you want them executed after a BGP announcement is performed (and subsequently a BGP log is generated).
12	Traffic Sample Size (bytes)	Number	{tcpdump_size}	The size of the Traffic Sample logs. Useful when you want an action performed only if a traffic sample was already generated.
13	WANGuard Filters CPU Usage	Number	{wanguardfilters_max_cpu_usage}	The maximum CPU percent used by WANGuard Filter processes during mitigation phase.
14	Concurrency	Number	{concurrency}	The concurrency value for the IP address extracted from the WANGuard Sensor's IP Zone.
15	Unique Dynamic Parameter	String	{exclusive}	The Unique Dynamic Parameters contain Dynamic Parameters that must be unique for the validation of an Action Module.
16	WANGuard Filters	Number	{wanguardfilters}	The number of WANGuard Filters activated to detect and mitigate the attack patterns.
Traffic Related Parameters				
17	Threshold Pkts/s	Number	{threshold_pps}	The threshold packets/second value for the IP address and protocol, extracted from the WANGuard Sensor's IP Zone.

18	Threshold Bits/s	Number	{threshold_bps}	The threshold bits/second value for the IP address and protocol, extracted from the WANGuard Sensor's IP Zone.
19	WANGuard Sensor Pkts/s	Number	{wanguardsensor_pps}	The latest packets/second throughput recorded by WANGuard Sensor in the anomalous traffic.
20	WANGuard Sensor Bits/s	Number	{wanguardsensor_bps}	The latest bits/second throughput recorded by WANGuard Sensor in the anomalous traffic.
21	WANGuard Sensor Total Pkts/s	Number	{wanguardsensor_total_pps}	The latest packets/second throughput recorded for the IP address, for all traffic.
22	WANGuard Sensor Total Bits/s	Number	{wanguardsensor_total_bps}	The latest packets/second throughput recorded for the IP address, for all traffic.
23	WANGuard Sensor Peak Pkts/s	Number	{wanguardsensor_max_pps}	The maximum packets/second throughput recorded by WANGuard Sensor in the anomalous traffic.
24	WANGuard Sensor Peak Bits/s	Number	{wanguardsensor_max_bps}	The maximum bits/second throughput recorded by WANGuard Sensor in the anomalous traffic.
25	WANGuard Sensor Total Packets	Number	{wanguardsensor_total_packets}	The number of packets recorded by WANGuard Sensor in the anomalous traffic.
26	WANGuard Sensor Total Bits	Number	{wanguardsensor_total_bits}	The number of bits recorded by WANGuard Sensor in the anomalous traffic.
27	WANGuard Filters Pkts/s	Number	{wanguardfilters_pps}	The latest packets/second throughput recorded by active WANGuard Filter(s) in the anomalous traffic.
28	WANGuard Filters Bits/s	Number	{wanguardfilters_bps}	The latest bits/second throughput recorded by active WANGuard Filter(s) in the anomalous traffic.
29	WANGuard Filters Max Pkts/s	Number	{wanguardfilters_max_pps}	The maximum packets/second throughput recorded by active WANGuard Filter(s) in the anomalous traffic.
30	WANGuard Filters Max Bits/s	Number	{wanguardfilters_max_bps}	The maximum bits/second throughput recorded by active WANGuard Filter(s) in the anomalous traffic.
31	Filtered Packets	Number	{wanguardfilters_filtered_packets}	The number of packets filtered by active WANGuard Filter(s).
32	Filtered Bits	Number	{wanguardfilters_filtered_bits}	The number of bits filtered by active WANGuard Filter(s).
33	Peak Pkts/s	Number	{max_pps}	The maximum value between {wanguardsensor_max_pps} and {wanguardfilters_max_pps}.
34	Peak Bits/s	Number	{max_bps}	The maximum value between {wanguardsensor_max_bps} and {wanguardfilters_max_bps}.
Time Related Parameters				
35	WANGuard Sensor Time Interval (seconds)	Number	{wanguardsensor_difftime}	The duration of the traffic anomaly reported by WANGuard Sensor.
36	WANGuard Filter Time Interval (seconds)	Number	{wanguardfilters_difftime}	The maximum duration of the traffic anomaly reported by active WANGuard Filter(s).
37	Time Interval (seconds)	Number	{difftime}	The maximum value between {wanguardsensor_difftime} and {wanguardfilters_difftime}.
38	-	Number	{wanguardsensor_first_unixtime}	The time in unix format when the traffic anomaly started.
39	-	Number	{wanguardsensor_last_unixtime}	The latest time in unix format when the traffic anomaly was still active.
40	-	String	{wanguardsensor_last_time}	The latest time in iso8601 format when the traffic anomaly was still active on WANGuard Sensor.

41	-	String	{wanguardfilters_last_time}	The latest time in iso8601 format when the traffic anomaly was still active on WANGuard Filter(s).
42	-	String	{first_time}	The time in iso8601 format when the traffic anomaly started.
43	-	String	{last_time}	The latest time in iso8601 format when the traffic anomaly was still active on WANGuard Sensor or on WANGuard Filter(s).
Filter Related Parameters				
44	Filter #	Number	{filter_id}	The unique ID of the attack pattern.
45	Filter Type (ip, source, dest, proto, len, ttl)	String	{filter_type}	The attack pattern type: - ip (Attacker's IP Address) - source (Source Port of the Attacker) - dest (Destination Port of the Victim) - proto (The IP Protocol Field) - len (The Size of the Packets) - ttl (The TimeToLive Field).
46	Filter Value	String	{filter_value}	The attack pattern's value.
47	Filter Pkts/s	Number	{filter_pps}	The attack pattern's latest packets/second throughput.
48	Filter Bits/s	Number	{filter_bps}	The attack pattern's latest bits/second throughput.
49	Filter Peak Pkts/s	Number	{filter_max_pps}	The maximum packets rate matched by the attack pattern.
50	Filter Peak Bits/s	Number	{filter_max_bps}	The maximum bits rate matched by the attack pattern.
51	Filter Severity	Number	{filter_severity}	The severity field represents the ratio between attack pattern traffic and threshold values.
52	Filter Packets	Number	{filter_packets}	The number of packets matched by the attack pattern.
53	Filter Bits	Number	{filter_bits}	The number of bits matched by the attack pattern.
54	Filter Time Interval (seconds)	Number	{filter_difftime}	The duration of the attack pattern.
55	-	Number	{filter_first_unixtime}	The time in unix format when the attack pattern was detected.
56	-	Number	{filter_last_unixtime}	The latest time in unix format when the attack pattern was still active.
57	-	String	{filter_first_time}	The time in iso8601 format when the attack pattern was detected.
58	-	String	{filter_last_time}	The latest time in iso8601 format when the attack pattern was still active.
59	Filter Whitelisted	Number	{filter_whitelisted}	If the attack pattern is whitelisted, the value is 1. Otherwise it's 0.
60	-	String	{filter_tcpdump}	Contains a tcpdump-like log with a sample of traffic matching the attack pattern.
61	Filter Traffic Sample Size (bytes)	Number	{filter_tcpdump_size}	Attack pattern traffic sample size.
62	-	String	{attacker_whois}	{attacker_whois} extracts from the whois database (RIPE, ARIN, APNIC, AfriNIC, LacNIC) the ISP contact email of the attacker's ip address.

Appendix 3 – Configuring Traffic Diversion

This appendix describes how to configure traffic diversion for WANGuard Filter. Information provided here regarding router configurations is for informational purposes only. Please refer to the appropriate router user guides for detailed information.

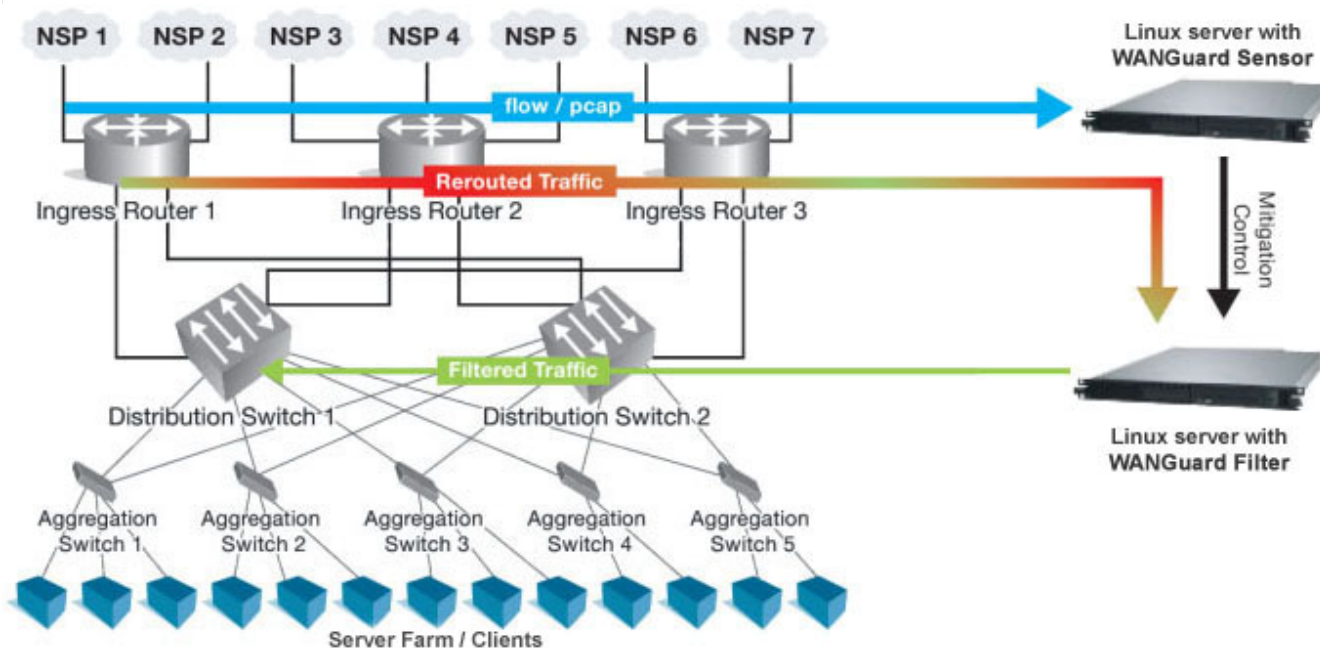
Understanding the BGP Diversion Method

Following standard Border Gateway Protocol (BGP) routing definitions, routers select the routing path with the longest matching prefix (also known as the “most specific”). After establishing a BGP session with the router, WANGuard Filter sends a routing update where the WANGuard Filter system is listed as the best path for the attacked destinations.

The network prefix that WANGuard Filter announces is longer than the one already listed in the router’s routing table, overriding the router's routing table definition.

To configure traffic diversion in Layer 2 or Layer 3 network topologies, perform the following:

1. Configure traffic diversion using BGP
2. Configure the appropriate traffic forwarding method



The figure above provides an example of traffic diversion from Ingress Router 1,2,3 towards a Linux server running the WANGuard Filter software.

After BGP diversion is established, the router's routing tables points to the WANGuard Filter server as the best route to the attacked addresses and the router forwards all traffic destined to those addresses to the WANGuard Filter server.

BGP Configuration Guidelines

This section provides general guidelines for BGP configuration on the WANGuard Filter server and on a divert-from router.

The guidelines provided in this section apply to the BGP configuration on any router from which WANGuard Filter system diverts the traffic. The following examples are provided using common External Border Gateway Protocol v4 (eBGP). You should consider the network configuration and determine whether eBGP or iBGP should be implemented in your network.

Follow these guidelines when the WANGuard Filter system and adjacent routers operate using common eBGP:

1. Configure bgpd with an easy recognizable AS (Autonomous System) number.

The bgpd sends routing information only when it diverts traffic. This route appear in the router's routing tables. Using a recognizable value allows you to easy identify the WANGuard Filter system in the router's routing tables.

2. To ensure that the bgpd routing information is not redistributed to other internal and external BGP neighboring devices, perform the following:

- Configure the bgpd not to send routing information and to drop incoming BGP routing information
- Set the bgpd BGP community attribute values to *no-export* and *no-advertise*.

A match in the community attributes enables bgpd to filter BGP announcements on the router and enforce this policy.

3. Enter the *soft-reconfiguration inbound* command during the setup procedures. This command is useful for troubleshooting and allows you to restore a routing table without reconnecting to neighboring device.

WANGuard Filter System BGP Configuration

You must configure the BGP using the Zebra software (<http://www.zebra.org>) or the Quagga software (<http://www.quagga.net>). Quagga is a fork of Zebra and the differences are minimal. Quagga keeps it's configuration files in */etc/quagga* while Zebra keeps it's configuration files in */etc/zebra*.

After installing Quagga or Zebra, you will have to create some basic configuration files, so both zebra and bgp daemons could start. Setting the passwords for the two daemons is enough to get them started. You should change “zebrapass” and “bgppass” with your own passwords.

```
[root@localhost ~]# echo 'password zebrapass' > /etc/quagga/zebra.conf
[root@localhost ~]# echo 'password bgppass' > /etc/quagga/bgpd.conf
[root@localhost ~]# /etc/init.d/zebra start
[root@localhost ~]# /etc/init.d/bgpd start
```

It is a good idea to tighten the security in the zebra daemon. You must connect to the zebra daemon with telnet on localhost port 2601 (default zebra port) with the previously defined password (“zebrapass”) and issue the following commands:

```
[root@localhost ~]# telnet 127.0.0.1 2601
localhost> enable
localhost# config terminal
localhost(config)# service password-encryption
localhost(config)# write
localhost(config)# exit
localhost# exit
```

To configure the bgpd daemon you must telnet to port 2605 and enter the previously defined password (“bgppass”). You must then switch to the privileged mode by entering the *enable* command.

```
[root@localhost ~]# telnet 127.0.0.1 2605
localhost> enable
localhost#
```

Switch to terminal configuration mode by entering the *config terminal* command. The prompt will change indicating that the system has entered the configuration mode:

```
localhost# config terminal
localhost(config)#
```

You should then enable encrypted passwords and set a new password for the configuration mode:

```
localhost(config)# service password-encryption
localhost(config)# enable password enablepass
```

Configure routing on bgpd using the commands shown in the following example. Please note that you can use the prefix-list, route-map, or distribute-list method for filtering outgoing routing information about the router. The following example describes the distribute-list method. You can use the prefix-list or route-map filtering method types as long as the routing information is not sent to bgpd.

```
localhost(config)# router bgp <WANGuard-Filter-AS-number>
localhost(config-router)# bgp router-id <WANGuard-Filter-IP-address>
localhost(config-router)# neighbor <Router-IP-address> remote-as <Router-AS-number>
localhost(config-router)# neighbor <Router-IP-address> description <description>
localhost(config-router)# neighbor <Router-IP-address> soft-reconfiguration inbound
localhost(config-router)# neighbor <Router-IP-address> distribute-list nothing-in in
localhost(config-router)# neighbor <Router-IP-address> route-map WANGuard-Filter-out out
localhost(config-router)# exit
```

```
localhost(config)# access-list nothing-in deny any
localhost(config)# route-map WANGuard-Filter-out permit 10
localhost(config-route-map)# set community x:x no-export no-advertise
localhost(config-route-map)# exit
localhost(config)# write
localhost(config)# exit
```

WANGuard Filter System BGP Configuration Example

To display the router configuration, enter the *show running-config* command from the “enable” command level. In the following example, the router's AS number is 1000, and the bgpd AS number is 64000.

The following partial sample output is displayed:

```
localhost# show running-config
... ..
router bgp 64000
  bgp router-id 192.168.1.100
  neighbor 192.168.1.1 remote-as 1000
  neighbor 192.168.1.1 description divert-from router
  neighbor 192.168.1.1 soft-reconfiguration inbound
  neighbor 192.168.1.1 distribute-list nothing-in in
  neighbor 192.168.1.1 route-map WANGuard-Filter-out out
!
access-list nothing-in deny any
!
route-map WANGuard-Filter-out permit 10
  set community 1000:64000 no-export no-advertise
!
line vty
... ..
```

Cisco Router BGP Configuration

This section describes the router's BGP configuration used when you configure traffic diversion. The syntax in the commands is taken from the BGP configuration on a Cisco router.

The following configuration steps shows the commands to use to configure BGP on a Cisco router:

```
r7500(config)# router bgp <Router-AS-number>
r7500(config-router)# bgp log-neighbor-changes
r7500(config-router)# neighbor <WANGuard-Filter-IP-address> remote-as <WANGuard-Filter-AS-
number>
r7500(config-router)# neighbor <WANGuard-Filter-IP-address> description <description>
r7500(config-router)# neighbor <WANGuard-Filter-IP-address> soft-reconfiguration-inbound
r7500(config-router)# neighbor <WANGuard-Filter-IP-address> distribute-list
routesToWANGuardFilter out
r7500(config-router)# neighbor <WANGuard-Filter-IP-address> route-map WANGuard-Filter-in in
r7500(config-router)# no synchronization
r7500(config-router)# exit
r7500(config)# ip bgp-community new-format
r7500(config)# ip community-list expanded <WANGuard-Filter-community-name> permit no-export
no-advertise
r7500(config)# route-map WANGuard-Filter-in permit 10
```

```
r7500(config-route-map)# match community <WANGuard-Filter-community-name> exact match
r7500(config-route-map)# exit
r7500(config)# ip access-list standard routesToWANGuardFilter
r7500(config-std-nacl)# deny any
```

The *no synchronization* command prevents the distribution of the bgpd routing updates into Interior Gateway Protocol (IGP).

Cisco Router BGP Configuration Example

To display the router configuration, enter the *show running-config* command from the router global command level. In the following example, the router's AS number is 1000 and the bgpd AS number is 64000.

The following partial output is displayed:

```
r7500# show running-config
... ..
router bgp 1000
  bgp log-neighbor-changes
  neighbor 192.168.1.100 remote-as 64000
  neighbor 192.168.1.100 description WANGuard Filter appliance
  neighbor 192.168.1.100 soft-reconfiguration inbound
  neighbor 192.168.1.100 distribute-list routesToWANGuardFilter out
  neighbor 192.168.1.100 route-map WANGuard-Filter-in
  no synchronization
!
ip bgp community new-format
ip community-list expanded WANGuard-Filter permit 1000:64000 no-export no-advertise
!
route-map WANGuard-Filter-in permit 10
  match community WANGuard-Filter exact match
ip access-list standard routesToWANGuardFilter
  deny any
... ..
```

Understanding Traffic Forwarding Methods

This section provides details on traffic forwarding methods. Traffic forwarding methods are used to forward the cleaned traffic from the WANGuard Filter system to a downstream router.

The following terminology is used in this section:

- Divert-from router – Router from which the bgpd diverts the attacked destinations traffic.
- Inject-to router – Router where bgpd forwards the cleaned traffic towards attacked destinations.
- Next-hop router – Router that is the next-hop to the destinations according to the routing table on the divert-from router before traffic diversion is activated.

Static Routing – Layer 2 Forwarding Method

In a Layer 2 topology, the WANGuard Filter system, divert-from router, and next-hop router are on the same network or VLAN. In a Layer 2 topology, a divert-from router and an inject-to router are two different devices. The next-hop router and the inject-to router are the same device.

GRE / IP over IP Tunneling – Layer 3 Forwarding Method

In a Layer 3 topology, the divert-from and inject-to routers are the same router (referred to as the router in this chapter). WANGuard Filter sends a BGP announcement that modifies the router's routing table to divert the zone traffic to the WANGuard Filter system. WANGuard Filter cleans the traffic and returns the cleaned traffic to the same router. The divert-from router then sends the traffic to the router that appears as the best path to the zone. This process may result in a malicious routing loop. In this case you may have to use a tunnel that is configured between the WANGuard Filter system and the next-hop router to forward clean traffic. The inject-to router does not perform routing decisions according to the zone address and forwards the packets to the next-hop router.

Configuring Static Routing – Layer 2 Forwarding Method

The Layer-2 Forwarding (L2F) method is used in a Layer 2 topology when all three devices—the WANGuard Filter system, the divert-from router, and the next-hop router—are located in one shared IP network. In a Layer 2 topology, a divert-from router and an inject-to router are two separate devices. The next-hop router and the inject-to router are the same device.

The WANGuard Filter system issues an ARP query to resolve the MAC address of the inject-to/next-hop router and then forwards the traffic. For this reason, no configuration on the routers is required when using the L2F method. The only thing you have to configure when using this method is the default gateway on the WANGuard Filter system so that it points to the inject-to/next-hop router.

Configuring GRE / IP over IP Tunneling – Layer 3 Forwarding Method

In the tunnel diversion method, you configure a tunnel between the WANGuard Filter system and each of the next-hop routers. The WANGuard Filter system sends the traffic over the tunnel that ends in the next-hop router of the destined zone. Because the returned traffic goes over a tunnel, the inject-to router performs a routing decision on the end point of the tunnel interface only, not on the zone's address.

To use this method you have to run the standard Linux tool *ip* to create and route GRE / IP over IP tunnels that will be used to inject the cleaned traffic back into the network. You must then configure WANGuard Filter (Page 55) with the Outbound Interface set to the virtual network interface created by the tunnel.