WANGuard Platform 4.0

User Manual

WANGuard Console + WANGuard Sensor + WANGuard Filter

Revision 2.00

Copyright & trademark notices

This edition applies to version 4.0 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.

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

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

Table of Contents

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 and enforced. The significant degradation of the network 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 solution 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 or your users 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.)
- Extensive MRTG-style traffic graphs and traffic accounting reports for IP addresses and IP classes in your network for any time-frame, including 95th Percentile for burstable billing.
- 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, easy-to-use 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, sFlow®, Cisco NetFlow® and Huawei NetStream®
- You can access various real-time parameters (top talkers, number of IP addresses, top protocols, protocols distribution etc.) of 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 intuitive, easy-to-use, rich Ajax-based (Web 2.0) web interface
- IP Zones support for segmenting your network by departments, clients, server clusters etc.
- Intuitive and customizable Dashboards with widgets defined by you
- 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 fine-grained security profiles

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 section in order to get a clear overview of the basic premises required for the proper operation of the software. If you're an administrator and you want to setup WANGuard Platform skip to the Installation Chapter (page 36).

A First Look at the WANGuard Console

You can change the Default Tab by editing User preferences. Because no WANGuard Sensor or WANGuard Filter system was previously configured and enabled and no data was gathered, the most content does not exist yet.

To understand the operation of WANGuard Console please be aware of the structure of the web application:

West Panel

The West Panel is located on the left (west) edge of the screen and it is used for navigation throughout the WANGuard Console. If you cant see the West Panel then it may be either collapsed (so click the edge to expand it) or hidden by an Administrator.

West Panel contains 2 regions: Reports and Configuration (hidden if you have “User” role) that can be collapsed or expanded by clicking the title bar. In multiple user environments the regions may contain old data but you can refresh them by clicking the right button on the title bar.

Each of those regions contain panels that can be either collapsed or expanded, their state being kept between sessions. Each of these panels are explained in detail in the following chapters.

Center Panel

WANGuard Console offers various ways to look at historic or live collected data. Each Report you request through the West Panel opens a new tab on the Center Panel. You may switch between tabs or close them all except for the Home Tab that's defined in your User Profile.

South Panel

The south panel is collapsed by default and it is located on the bottom of the browser Window. To expand it click the bottom edge. If you can't see it then it's hidden through your User Profile.

It provides a quick way to view live data collected from WANGuard Platform components, structured in tabs:

- **WANGuard Sensor Live Graphs**

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 Sensors**

  Select only the WANGuard Sensor systems that you're interested in.

- **Data Unit**

  Select the traffic parameter the graph will represent:

  - *Bits* - The bits/second throughput recorded by WANGuard Sensors.
  - *Bytes* - The bytes/second throughput recorded by WANGuard Sensors.
  - *Packets* - The packets/second throughput recorded by WANGuard Sensors.
  - *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 frames* - 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 frames* - 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 frames* - 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.

- **Latest Events**

  The Latest Events tab provides a list with the latest records from Logs & Events. The records are explained in the Logs & Events chapter (Page 34).

- **WANGuard Platform Components**

  Each tables belonging to WANGuard Components is explained in detail in the Reports – Device Groups Chapter (page 21).

Reports - Alarms

The Alarms Panel contains 2 items that when clicked will open 2 tabs: Active Traffic Anomalies and Archived Traffic Anomalies. The number of Active Traffic Anomalies is displayed with a red background, and refreshed every 5 seconds within the Alarms Panel. It's not displayed if it's zero.

Active Traffic Anomalies

The Active Traffic Anomalies table is visible only when WANGuard Sensors detect 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 and are presented in the following format:

#	The unique index number of the traffic anomaly.
IP Address	The IP address from your network involved in the traffic anomaly. 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. If clicked, a new tab opens with IP Graphs and IP Accounting information for that IP.
IP Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: *TCP+SYN, TCP, UDP, ICMP, OTHER*.
WANGuard Sensor	The description of the WANGuard Sensor that detected the traffic anomaly. If clicked, a new tab will open that contains Sensor Graphs, Tops and Protocol Distribution for that WANGuard Sensor.
From	The time and date when WANGuard Sensor began 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 of the anomalous traffic.
Bits/s	The latest bits/second throughput of 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.
Log	If this icon exists then if it is clicked a new window opens with a tcpdump capture of the anomalous traffic.
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 table will show up in the same traffic anomaly row. The rows in the table will have red background for active attack patterns and yellow background for inactive attack patterns:

WANGuard Filter	The description of the WANGuard Filter that detected the attack pattern.
Filter	The filter applied by WANGuard Filter to remove the attack pattern's traffic. WANGuard Filter dynamically applies the following filter types: *Source IP, Source Port, Destination Port, Packet Length, TimeToLive, IP Protocol.* 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.
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 exists then if it is clicked a new window opens with a tcpdump capture of the attack pattern.

Archived Traffic Anomalies

The Archived Traffic Anomalies tab shows all traffic anomalies sorted by time in descending order, that match the Filters from the header of the table. By clicking the down arrow on any column header, you can change Filters, Ascending/ Descending Sorting and Hide/Show Columns.

Every row in the table represents a traffic anomaly in the following format:

+	By clicking the <+> sign the selected traffic anomaly will be expanded with additional information about traffic samples, WANGuard Filters etc.
#	The unique index number of the traffic anomaly.
IP Address	The IP address from your network involved in the traffic anomaly. 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. If clicked then a new tab opens with IP Graphs and IP Accounting information for that IP.
IP Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: *TCP+SYN, TCP, UDP, ICMP, OTHER.*
WANGuard Sensor	The description of the WANGuard Sensor that detected the traffic anomaly.
From	The time and date when WANGuard Sensor began the detection of the traffic anomaly.
Until	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.

Reports - Autonomous Systems

The Autonomous Systems Panel contains 2 items that open 2 tabs: BGP Announcements and Autonomous Systems. The number of active BGP Announcements is displayed with a red background within the panel. It's refreshed every 5 seconds but it's not displayed if it's zero.

BGP Announcements

The BGP Announcements tab 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 constantly refreshed every 5 seconds as long as the <Refresh> button remains pressed.

If you have *Administrator* or *Operator* privileges then you can add your own BGP announcements or you can manually remove existing BGP announcements. To add a new BGP announcement you must enter the IP / CIDR, select the BGP router and provide comments to the New BGP Announcement Window. If the announcement was successful, the BGP announcements table below will contain the new BGP announcement.

The BGP Announcements table contains the following fields:

BGP Router	The BGP Router description as defined in the BGP router configuration (Page 77).
IP / CIDR	The IP address and the subnet in CIDR notation. /32 for individual hosts.
Start Time	The time and date when the BGP announcement was sent.
Details / Comments	This field contains comments or details about the BGP announcement. If the BGP announcement was sent manually using the form in the upper section, the Details field contains the comments entered in the form. 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 tab will open that provides details regarding the traffic anomaly.
Action	The Action field is visible only if the logged on user has Administrator or Operator privileges. The Action field contains a link for the manual removal of the BGP announcement.

You can view a list of old BGP announcements by accessing the Logs & Events Panel (page 34).

Autonomous Systems

If you are using the flow-based WANGuard Sensor – WANGuard Flow, then you will be able to generate very accurate Autonomous Systems 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.

The Autonomous Systems tab parameters are:

- **WANGuard Sensors**

  Select the WANGuard Flow systems that captured the traffic you're interested in. Multiple selections can be made. Administrators can filter what WANGuard Sensors are available to individual users.

- **Time Frame**

  Select predefined time-frames or enter your own by selecting Custom.

- **Export**

  You can print the generated ASN graphs or you can save them as PDF through plug-ins.

- **Refresh**

  By default the resulted report is refreshed only when you press the <On Demand> button. If you select a refresh interval then the report will be constantly refreshed and if a predefined time-frame was selected then that will be updated too.

- **Autonomous Systems Number(s)**

  Here you can enter the ASNs you're interested in, separated by space. If you don't know what ASN is a particular ISP having then you can click on the upper-right side of the window: Help → AS Information → AS Numbers List. You can then apply different filters by clicking table header's down icon.

- **Graphs Size**

  You can select a predefined graphs size OR you may enter your own graphs size as <xpixels> x <ypixels>.

- **Sum Sensors**

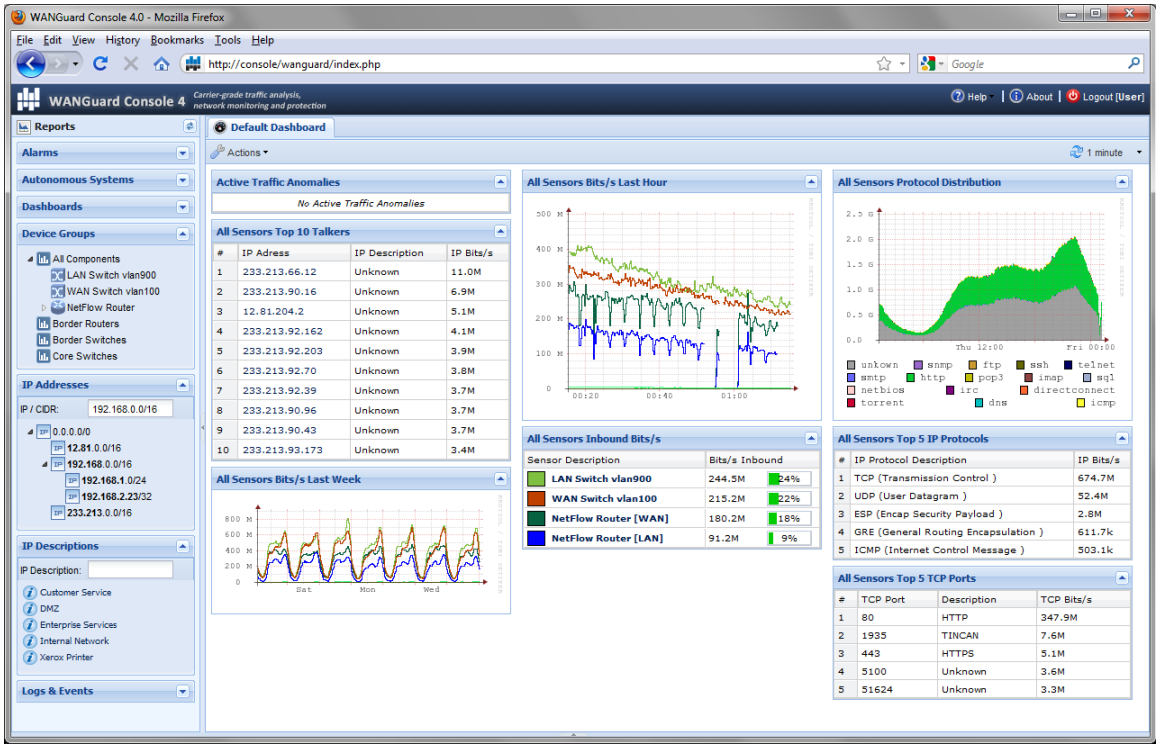
  If unchecked, each WANGuard Sensor generates a different ASN graph. If checked, all selected WANGuard Sensors generate a single ASN graph that contains summed traffic data.

- **Sum ASNs**

  If you entered multiple Autonomous Systems Numbers then you can sum all of them in a single ASN graph. This is extremely useful with ISPs and ASN owners that have more than 1 allocated ASN.

Reports - Dashboards

Dashboards are the best way to organize data so that it can suit your particular needs. WANGuard Console allows users with *Administrator* or *Operator* roles to create and edit dashboards that contain custom widgets. Administrators can also restrict what Dashboards are available to individual users.



Managing Dashboards

You can **add** new Dashboards by clicking <Actions> in the **Default Dashboard** and select <Add Dashboard...>**.** The Default Dashboard cannot be deleted or edited. However any other Dashboard can be edited or deleted by clicking the same <Actions> button and then by clicking <Edit Dashboard...>. You can then change the Description, add your own Comments and set the number of columns and the percentage each column should have of the Center Panel's width. The sum of all percentages should be 100%.

Managing Widgets

If you are an Administrator or an Operator you can add, edit or delete Widgets. To sort them click the title bar and move them around. To collapse a widget click the first icon on the widget title bar. To edit a widget click the second icon on the widget title bar. To delete a widget click the third icon on the widget title bar.

To add a new Widget click <Actions> in the toolbar and then select the Widget Type you like. Widgets have the following common fields:

- **Widget Title**

  Enter a relevant description of the widget. What it should display.

- **Widget Height**

  Leave the Widget Height to Auto for the widget to take all the vertical space it needs. Or you can specify the number of pixels for the Widget Height.

- **WANGuard Sensors**

  Select the WANGuard Sensors that are allowed to provide information to the widget.

All other options are self-explanatory or are described in the next Reports Chapters.

Reports - Device Groups

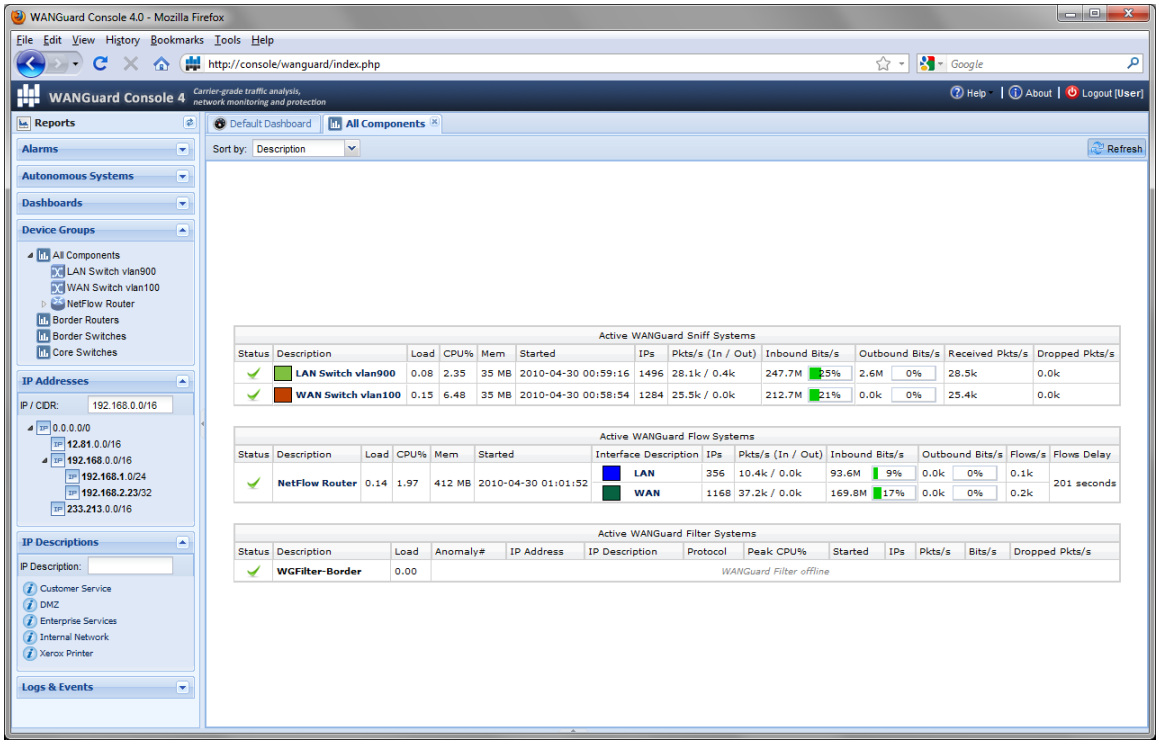
The Device Groups Panel offers a intuitive, complete view on all WANGuard Platform components. It includes a “All Components” tree and a separate item for each Device Group configured for WANGuard Sensors and WANGuard Filters. The “All Components” tree can be expanded to show all active WANGuard Flow and WANGuard Sniff systems.

By clicking “All Components”, a new tab opens that contains live tables for all WANGuard Platform components. By clicking a Device Group, a new tab opens that contains live tables for each WANGuard Sensor and WANGuard Filter included in that Device Group.

By clicking a WANGuard Sensor included in the “All Components” tree, a new tab opens that contains Sensor Graphs, Sensor Tops and Protocol Distribution Data.

All Components and Device Group Tabs

These tabs display tables with the latest system parameters collected from active WANGuard Platform components. Administrators can restrict what Device Groups are available to individual users.



WANGuard Console System

The WANGuard Console System table is only displayed if you select “All Components” as it cannot be assigned to a particular Device Group. The table has the following format:

Status	If the WANGuard Console system is functioning properly then a green “checked” arrow is displayed.
Load	The load of the operating system for the last 5 minutes.
Mem	The amount of RAM memory used by the current PHP process.
Started	The time and date when WANGuard Console's database server has been started.
Online Users	The number of active WANGuard Console sessions.
Free Graphs Disk	The disk space available on the partition configured to store IP graphs data.
Free DB Disk	The disk space available on the partition that is configured to store the MySQL database.
DB Size	The amount of disk space used by the WANGuard Database.
DB Active Clients	The number of clients that are currently using the MySQL server.
DB Active Connections	The number of active connections on the MySQL server.
Avg DB Queries/s	The average number of database queries per second reported by the MySQL server.

Active WANGuard Sniff Systems

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

Status	If the active WANGuard Sniff system is functioning properly then a green “checked” arrow is displayed. If WANGuard Console cannot manage or reach the WANGuard Sniff system then a red “X” icon is displayed. In this case make sure that WANGuard Sniff is configured correctly, read the Events Logs and make sure that the *WANGuardController* daemon is running on all systems.
Description	Displays the description of the WANGuard Sniff system and a colored box with the

	Graph Color IN as defined in its configuration. When clicked a new WANGuard Sensor Tab is opened (see next paragraph).
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 RAM 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 (In / Out)	The packets/second throughput after validation and filtering.
Bits/s (In / Out)	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

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

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

Active WANGuard Filter Systems

The Active WANGuard Filter Systems table displays the latest system information collected from active WANGuard Filter systems that are included in the selected Device Group. If there are no WANGuard Filter systems configured then this table is not displayed. The table has the following format:

Status	If the active WANGuard Filter system is functioning properly then a green “checked” arrow is displayed. 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 Logs and make sure that the *WANGuardController* daemon is running on all systems.
Description	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 tab 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 tab opens with IP Graphs and IP Accounting reports for the IP.
IP Description	The description of the IP address extracted from the WANGuard Sensor's IP Zone.
Protocol	The traffic type that exceeded the threshold: *TCP+SYN, TCP, UDP, ICMP, OTHER.*
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 Tabs

When clicking a WANGuard Sensor new tab opens that includes 3 additional sub-tabs located on the bottom of the window: Sensor Graphs, Sensor Tops and Protocol Distribution. All these sub-tabs use the following common toolbar fields:

- **WANGuard Sensors**

  Select the WANGuard Sensors you're interested in. Multiple selections can be made. Administrators can filter what WANGuard Sensors are available to individual users.

- **Time Frame**

  Select predefined time-frames or enter your own by selecting Custom.

- **Export**

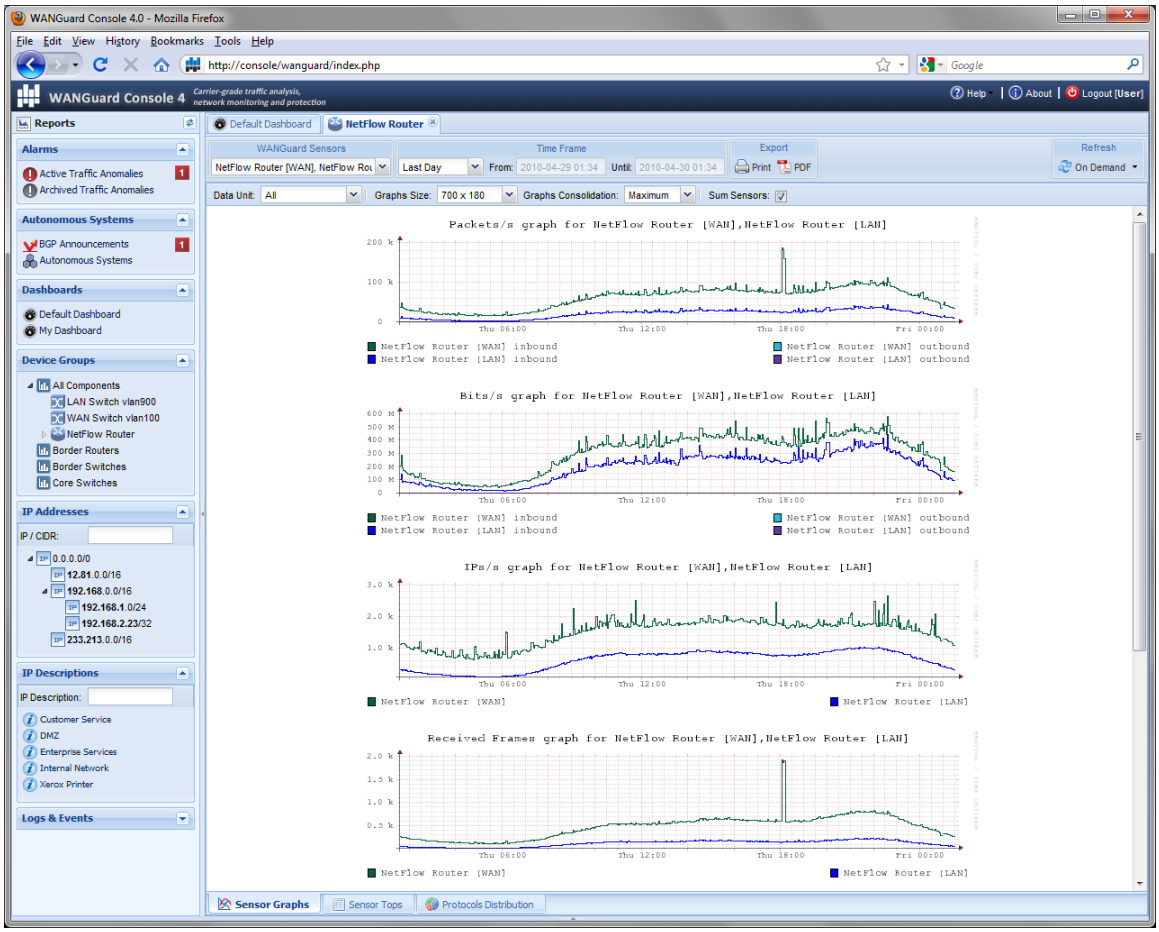
  You can print the generated WANGuard Sensors reports or you can save them as PDF through plug-ins.

- **Refresh**

  By default the resulted report is refreshed only when you press the <On Demand> button. If you select a refresh interval then the report will be constantly refreshed and if a predefined time-frame was selected then that will be updated too.

Sensor Graphs

The Sensor Graphs sub-tab generates various traffic parameters graphs for the selected WANGuard Sensors.



The following options are available:

- **Data Unit**

  Select the traffic parameter the graphs will represent:

  - *All* - All of the below, each one in a different graph.
  - *Packets* - The packets/second throughput recorded by WANGuard Sensor.
  - *Bits* - The bits/second throughput recorded by WANGuard Sensor.
  - *Bytes* - The bytes/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 frames* - 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 frames* - 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 frames - 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.

- **Graphs Size**

  You can select a predefined graphs size OR you may enter your own graphs size as <xpixels> x <ypixels>.

- **Graphs Consolidation**

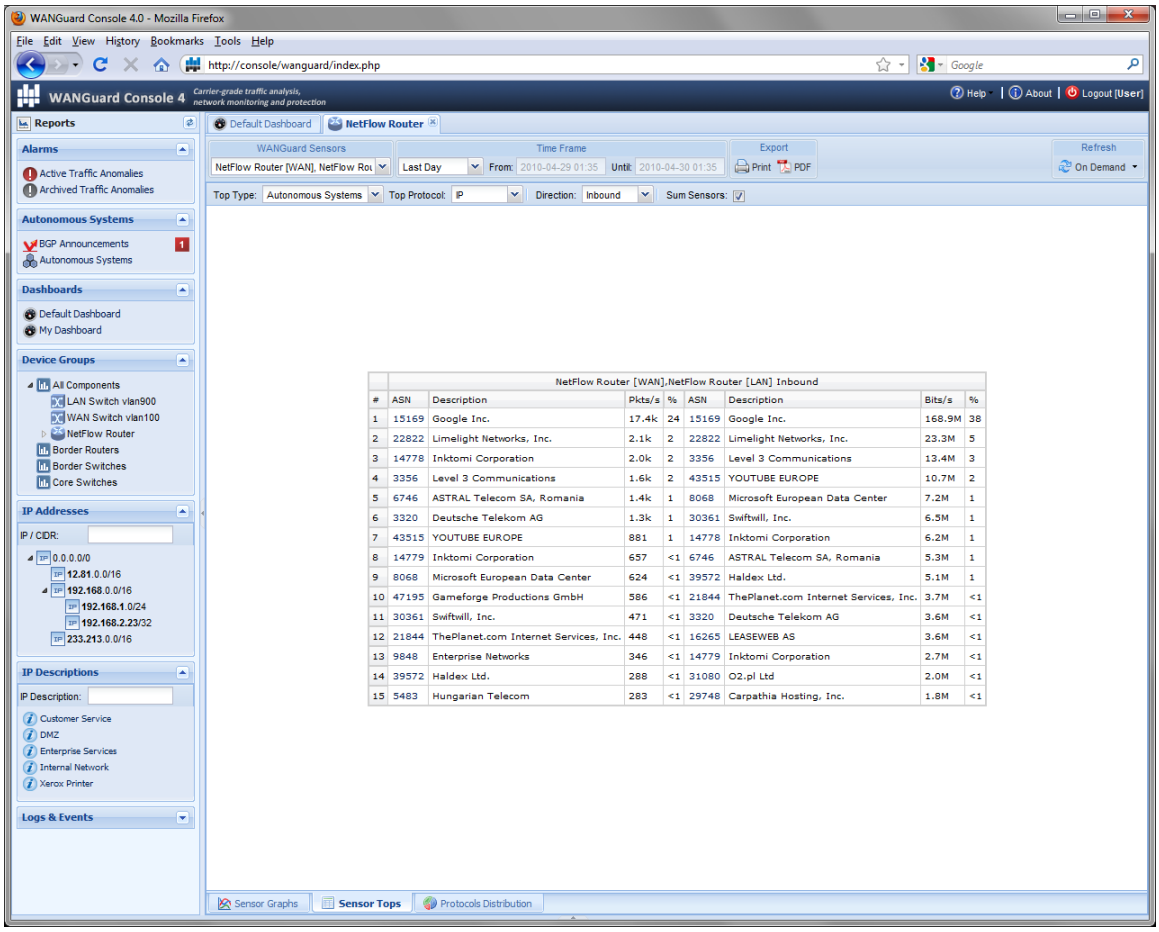
  Select the graphs consolidation procedure for the graph: *MINIMUM*, *MAXIMUM* or *AVERAGE*. If you are interested in traffic spikes, select the *MAXIMUM* aggregation type. If you are interested in average values, select the *AVERAGE* aggregation type. If you are interested in low traffic values, select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

- **Sum Sensors**

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

Sensor Tops

The Sensor Tops sub-tab generates various traffic tops for the selected WANGuard Sensors. Top generation for large time-frames may take minutes. In this case increase the *max_execution_time* parameter from *php.ini*.



NetFlow Router [WAN].NetFlow Router [LAN] Inbound

#	ASN	Description	Pkts/s	%	ASN	Description	Bits/s	%
1	15169	Google Inc.	17.4k	24	15169	Google Inc.	168.9M	38
2	22822	Limelight Networks, Inc.	2.1k	2	22822	Limelight Networks, Inc.	23.3M	5
3	14778	Inktomi Corporation	2.0k	2	3356	Level 3 Communications	13.4M	3
4	3356	Level 3 Communications	1.6k	2	43515	YOUTUBE EUROPE	10.7M	2
5	6746	ASTRAL Telecom SA, Romania	1.4k	1	8068	Microsoft European Data Center	7.2M	1
6	3320	Deutsche Telekom AG	1.3k	1	30361	Swiftwill, Inc.	6.5M	1
7	43515	YOUTUBE EUROPE	881	1	14778	Inktomi Corporation	6.2M	1
8	14779	Inktomi Corporation	657	<1	6746	ASTRAL Telecom SA, Romania	5.3M	1
9	8068	Microsoft European Data Center	624	<1	39572	Haldex Ltd.	5.1M	1
10	47195	Gameforge Productions GmbH	586	<1	21844	ThePlanet.com Internet Services, Inc.	3.7M	<1
11	30361	Swiftwill, Inc.	471	<1	3320	Deutsche Telekom AG	3.6M	<1
12	21844	ThePlanet.com Internet Services, Inc.	448	<1	16265	LEASEWEB AS	3.6M	<1
13	9848	Enterprise Networks	346	<1	14779	Inktomi Corporation	2.7M	<1
14	39572	Haldex Ltd.	288	<1	31080	O2.pl Ltd	2.0M	<1
15	5483	Hungarian Telecom	283	<1	29748	Carpathia Hosting, Inc.	1.8M	<1

The following options are available:

- **Top Type**

  You can select to see top 15 hosts (“Talkers”) that make traffic, top 15 TCP/UDP ports used, top 15 IP Protocols and top 15 Autonomous Systems (only when WANGuardFlow is used). Clicking IP Addresses and ASNs open new tabs with more details about the selection.

- **Top Protocol**

  You may further customize the Top Type by selecting only the IP protocols you're interested in.

- **Direction**

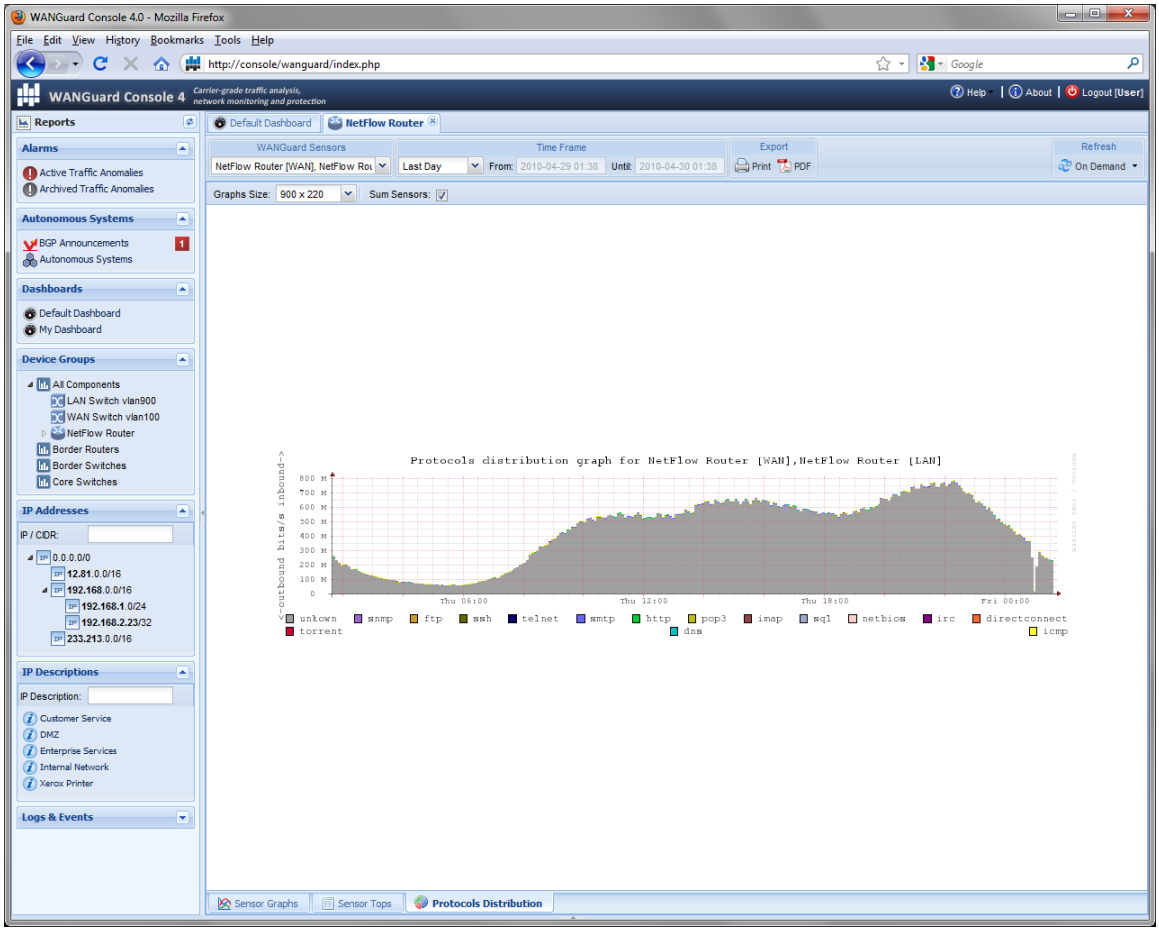
  The direction of the traffic: *Inbound* or *Outbound*.

- **Sum Sensors**

  If unchecked, each WANGuard Sensor generates a different top. If checked, all selected WANGuard Sensors generate a single top instead.

Protocols Distribution

WANGuard Sensor systems collect protocols distribution data. Currently supported protocols are: SNMP, FTP, SSH, TELNET, SMTP, HTTP, POP3, IMAP, SQL, NETBIOS, IRC, DIRECTCONNECT, TORRENT, DNS, ICMP. Protocol detection is unreliable for applications that use non-standard, randomized source or destination ports - torrent is the best example.



You can view protocols distributions graphs for the selected WANGuard Sensors with the following options:

- **Graphs Size**

  You can select a predefined graphs size OR you may enter your own graphs size as <xpixels> x <ypixels>.

- **Sum Sensors**

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

Reports - IP Addresses & IP Descriptions

This chapter describes how to generate advanced IP traffic graphs and IP traffic accounting reports from data collected by WANGuard Sensor systems.

Both IP Addresses Panel and IP Descriptions Panel generate the same reports and that's why those reports are treated in the same chapter. If the reports are empty, check if the selected IP Class / IP Description have “IP Accounting” parameter and “IP Graphs” parameter set to *Yes* in the IP Zones.

IP Addresses Panel allows quick generation of IP traffic reports by entering the IP / CIDR in the upper side of the Panel, or by selecting an IP class or host from the Subnets tree.

IP Descriptions Panel lists all IP Descriptions extracted from existing IP Zones. You can filter displayed IP Descriptions by entering a string that exists in the IP Description you're interested in. IP Descriptions are a great way to generate IP traffic reports for clients that have multiple allocated IP classes. You just have to define those IP classes with the same IP Description.

Administrators can filter what IP Addresses and IP Descriptions are available to individual Users.

By clicking a subnet or IP Description a new tab will open that includes 2 additional sub-tabs located on the bottom of the window: IP Graphs and IP Accounting. Both sub-tabs use the following common toolbar fields:

- **WANGuard Sensors**

  Select the WANGuard Sensor systems that captured the traffic you're interested in. Multiple selections can be made and by default all WANGuard Sensors are selected. Administrators can filter what WANGuard Sensors are available to individual users.

- **Data Unit**

  IP Graphs and IP Accounting reports can be generated for *Bits/second*, *Bytes/second* and *Packets/second*.

- **Time Frame**

  Select predefined time-frames or enter your own by selecting Custom.

- **Export**

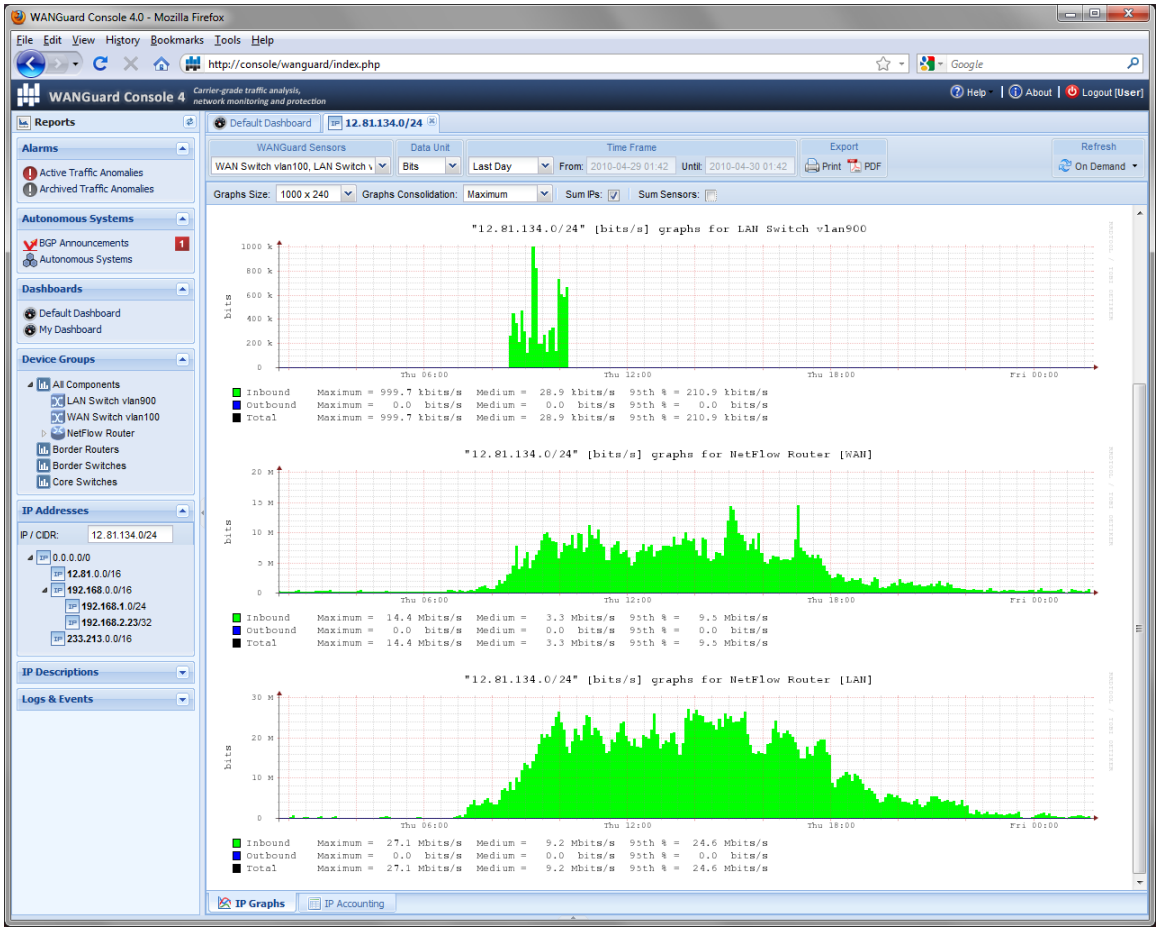
  You can print the generated IP reports or you can save them as PDF through plug-ins.

- **Refresh**

  By default the resulted report is refreshed only when you press the <On Demand> button. If you select a refresh interval then the report will be constantly refreshed and if a predefined time-frame was selected then that will be updated too.

IP Graphs

The IP Graphs sub-tab generates IP traffic graphs for the selected IP class, host or IP Description that include 95th percentile information useful for burstable billing.



The following options are available:

- **Graphs Size**

  You can select a predefined graphs size OR you may enter your own graphs size as <xpixels> x <ypixels>.

- **Graphs Consolidation**

  Select the aggregation procedure old data: *MINIMUM*, *MAXIMUM* or *AVERAGE*. If some aggregation types are missing, see the IP Traffic Graphs configuration (Page 79). 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.

- **Sum IPs**

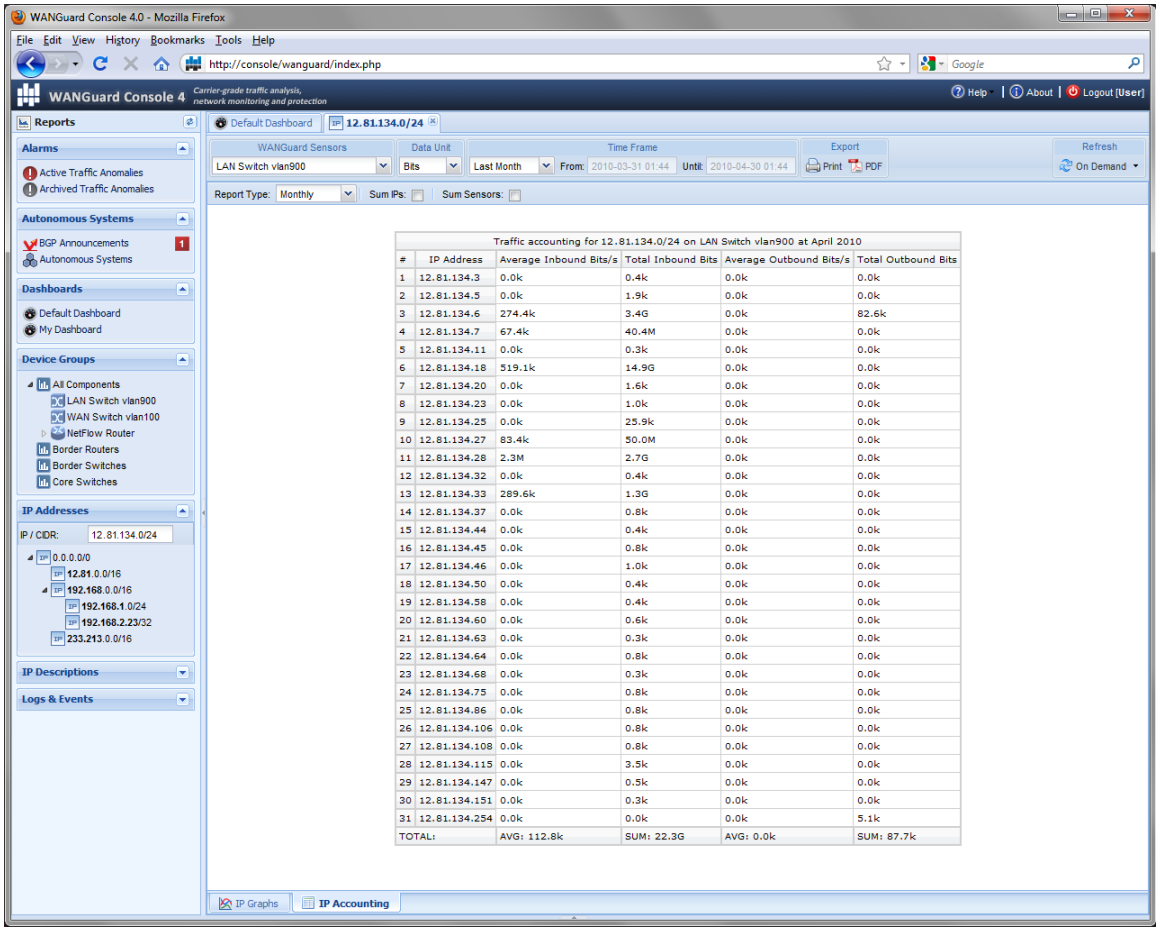
  Don't check the **Sum IPs** option if you want a different traffic graph displayed for every IP address contained in the selected IP class or IP Description. For example, when this option is used with a /24 CIDR then 256 traffic graphs are displayed, one for each IP address in the “C” class.

- **Sum 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.

IP Accounting

The IP Accounting sub-tab generates IP traffic accounting reports for the selected IP class, host or IP Description.



Traffic accounting for 12.81.134.0/24 on LAN Switch vlan900 at April 2010

#	IP Address	Average Inbound Bits/s	Total Inbound Bits	Average Outbound Bits/s	Total Outbound Bits
1	12.81.134.3	0.0k	0.4k	0.0k	0.0k
2	12.81.134.5	0.0k	1.9k	0.0k	0.0k
3	12.81.134.6	274.4k	3.4G	0.0k	82.6k
4	12.81.134.7	67.4k	40.4M	0.0k	0.0k
5	12.81.134.11	0.0k	0.3k	0.0k	0.0k
6	12.81.134.18	519.1k	14.9G	0.0k	0.0k
7	12.81.134.20	0.0k	1.6k	0.0k	0.0k
8	12.81.134.23	0.0k	1.0k	0.0k	0.0k
9	12.81.134.25	0.0k	25.9k	0.0k	0.0k
10	12.81.134.27	83.4k	50.0M	0.0k	0.0k
11	12.81.134.28	2.3M	2.7G	0.0k	0.0k
12	12.81.134.32	0.0k	0.4k	0.0k	0.0k
13	12.81.134.33	289.6k	1.3G	0.0k	0.0k
14	12.81.134.37	0.0k	0.8k	0.0k	0.0k
15	12.81.134.44	0.0k	0.4k	0.0k	0.0k
16	12.81.134.45	0.0k	0.8k	0.0k	0.0k
17	12.81.134.46	0.0k	1.0k	0.0k	0.0k
18	12.81.134.50	0.0k	0.4k	0.0k	0.0k
19	12.81.134.58	0.0k	0.4k	0.0k	0.0k
20	12.81.134.60	0.0k	0.6k	0.0k	0.0k
21	12.81.134.63	0.0k	0.3k	0.0k	0.0k
22	12.81.134.64	0.0k	0.8k	0.0k	0.0k
23	12.81.134.68	0.0k	0.3k	0.0k	0.0k
24	12.81.134.75	0.0k	0.8k	0.0k	0.0k
25	12.81.134.86	0.0k	0.8k	0.0k	0.0k
26	12.81.134.106	0.0k	0.8k	0.0k	0.0k
27	12.81.134.108	0.0k	0.8k	0.0k	0.0k
28	12.81.134.115	0.0k	3.5k	0.0k	0.0k
29	12.81.134.147	0.0k	0.5k	0.0k	0.0k
30	12.81.134.151	0.0k	0.3k	0.0k	0.0k
31	12.81.134.254	0.0k	0.0k	0.0k	5.1k
TOTAL:		AVG: 112.8k	SUM: 22.3G	AVG: 0.0k	SUM: 87.7k

The following options are available:

- **Report Type**

  Select the interval you want for the data to be aggregated for. Could be *Daily*, *Weekly*, *Monthly* and *Yearly*.

- **Sum IPs**

  Don't check the **Sum IPs** option if you want a different traffic accounting report displayed for every IP address contained in the selected IP class or IP Description. For example, when this option is used with a /24 CIDR then 256 traffic accounting reports are displayed, one for each IP address in the “C” class.

- **Sum Sensors**

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

Reports – Logs & Events

The Logs & Events panel located in the Reports region of the West Panel provides a way to access the wanguard database for troubleshooting and debugging purposes.

BGP Announcement Archive

BGP Announcement Archive stores every BGP announcement sent by WANGuard Platform components. Every BGP announcement record contains the following fields:

#	The index of the traffic anomaly that generated the BGP announcement. This field is empty if the BGP announcement was sent manually through WANGuard Console.
BGP Router	The BGP router used to send the BGP announcement.
IP Address	The announced IP address.
CIDR	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: *FINISHED, ACTIVE, WAITING.* To manually override the status, double-click the row and select another status.
User	If the BGP announcement was sent manually then this field contains the logged user. This column is hidden by default but can be shown by clicking the down arrow on column headers.
Details	If the BGP announcement was sent manually then this field contains the details field. This column is hidden by default but can be shown by clicking the down arrow on column headers.

Events Logs

Events Logs contain all events generated by WANGuard Platform components. You can sort, filter and manage the columns of the tables by clicking the down arrow on any column header.

Each component that generates events is listed in the Logs & Events panel. Record are shown the following format:

<+>	You can see details about each event by clicking this button.
Description	The 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.
Level	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 40).
Event	The text of the event.
Date	The date and time when the notification was generated.

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 4.0 has been tested with the following Linux distributions: **Red Hat Enterprise Linux 5.0 (** commercial Linux distribution), **CentOS 5.x** (free, Red Hat Enterprise Linux based distribution), **OpenSuSE 10.3, 11.x (** free, Novel Enterprise Linux based distribution), **Debian Linux 5.0** (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 4.0	**WANGuard Flow 4.0**
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 4.0 WANGuard-Controller 4.0	WANGuard-Sensor 4.0 WANGuard-Controller 4.0
Disk Space	5 GB (including OS)	5 GB (including OS)

When using WANGuard Flow, network devices must be configured to send NetFlow® v.5 or sFlow 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 81).

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 mandatory. 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 4.0 WANGuard-BGPSupport 4.0 WANGuard-Controller 4.0
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 88).

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 up to 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 5.2+ mysql 5.x rrdtool 1.3+ perl 5.x perl-rrdtool perl-MailTools perl-DBD-MySQL ping, whois, traceroute, telnet WANGuard-Console 4.0 WANGuard-Controller 4.0
Disk Space	4GB (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 3.5 or later, Apple Safari 3.0 or later, Konqueror 4.0 or later, Google Chrome 4.0 or later. Internet Explorer 7.0+ has a slow javascript engine and a non-standard behavior so it's not recommended.

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

For the best WANGuard Console experience we highly recommend the Firefox 3.6 browser, and a 1280x1024 pixels or higher resolution monitor.

Software Installation & Download

Software installation instructions are listed and updated on the Andrisoft website for RedHat-based, SuSE-based and Debian-based Linux distributions.

You may a 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.

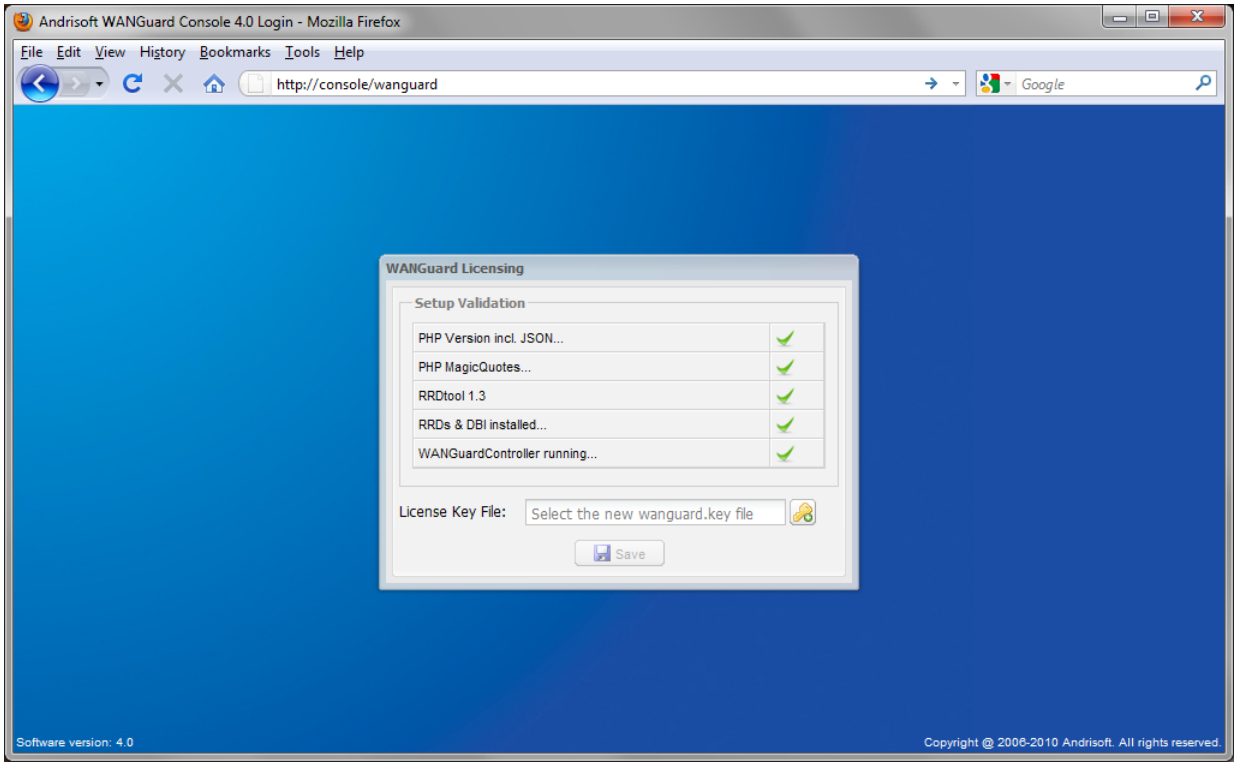
Binary WANGuard Platform components are packaged differently for i686 architectures (32 bit Pentium and beyond) and for x86_64 architectures (64 bit Intel / AMD processors).

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 38) 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.

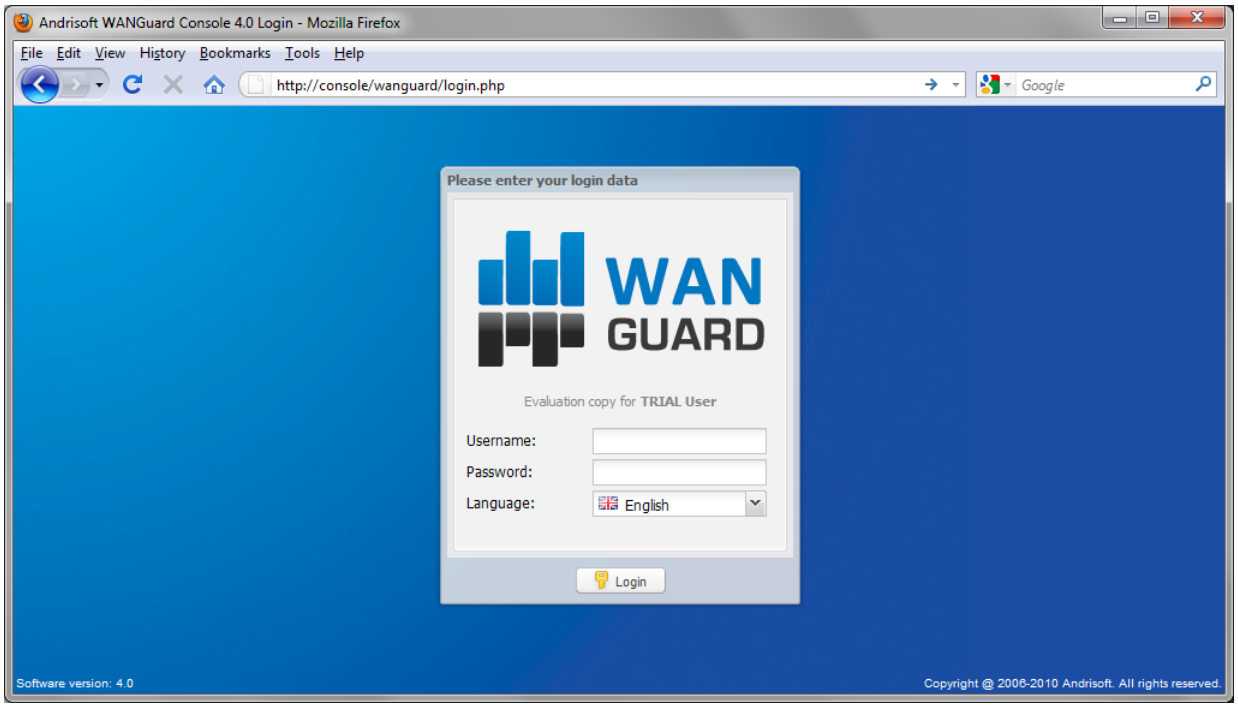
If you haven't licensed WANGuard Platform yet, you will be asked to do so:



You must then upload the *wanguard.key* file we sent you by email by clicking the key icon.

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**.



After you logged into WANGuard Console you can view and change license information by pressing the <About> button in the upper-right part of the window.

The next steps in quickly configuring WANGuard Platform are: Modify the Administrator's password (next paragraph), define your subnets in a new IP Zone (next chapter) and then configure WANGuard Sensors and WANGuard Filters.

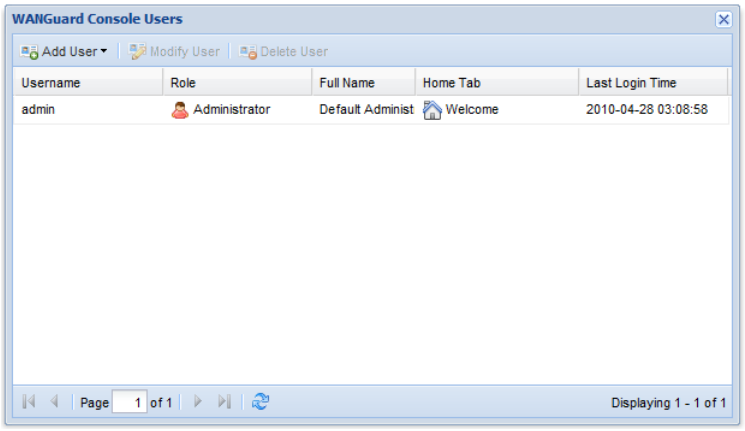
Managing WANGuard Console Users

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 Configuration from the West Panel and then expand the WANGuard Console panel.

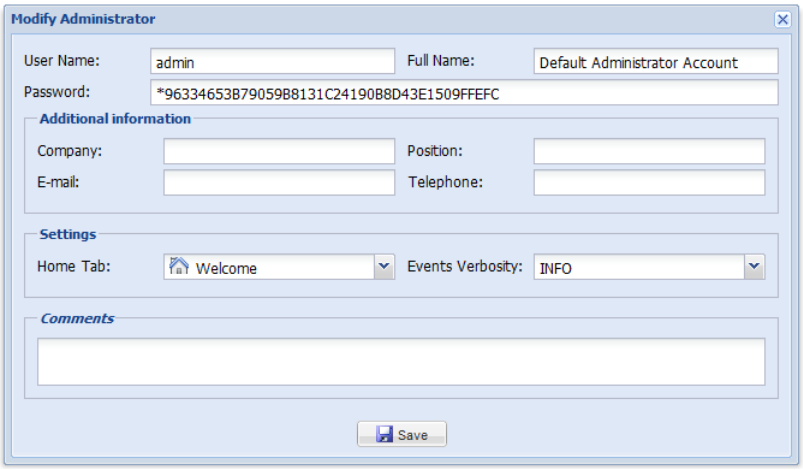
Currently there are three available access levels (**Roles**) for users:

- *Administrator* – This role 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).
- *Operator* – This role has all privileges to view and manage WANGuard Platform components, but cannot add or modify other users.

- *User* – This role cannot configure anything, but if access is permitted it can generate various reports.



To modify an user you can double-click it or select it and then press Modify User. Administrators and Operators have the following properties:



The **Full Name**, **Company**, **Position**, **E-mail, Telephone** and **Comments** fields are optional.

The **Home Tab** lets you decide which tab from the Reports Panel should be opened immediately after logging in. After Sensors are configured, choosing the Default Dashboard is a good option.

The **Events Verbosity** field lets you select the minimum severity level of the events that will be displayed in the South Panel and Logs & Events Panel:

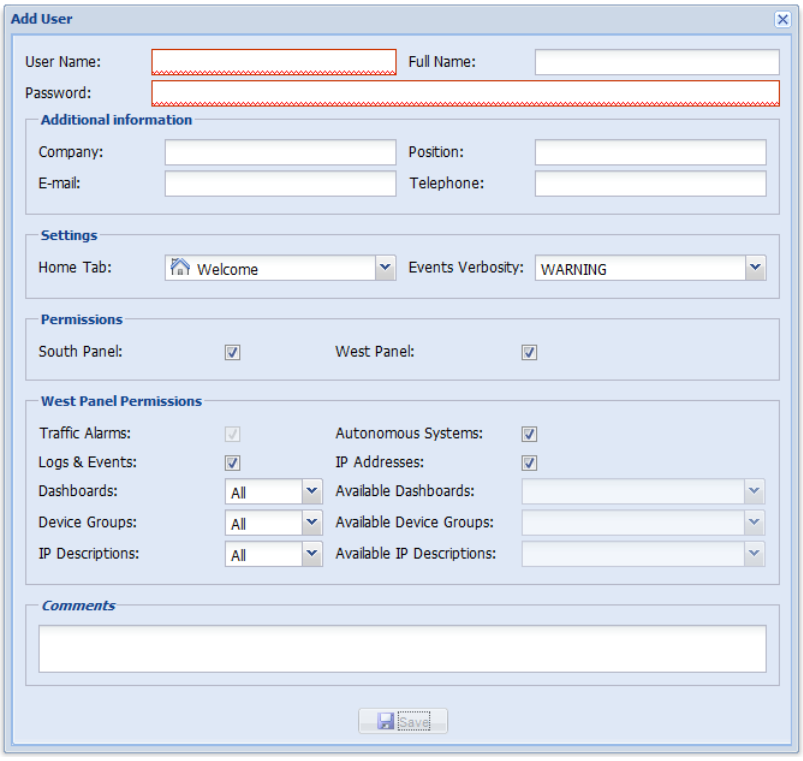
- *MELTDOWN* - Meltdown events are generated when a very serious error is detected in the system such as a hardware error.
- *CRITICAL* - Critical events are generated when a significant software error is detected such as a memory

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 or 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.

Administrators can restrict Users to access the following reports and panels: South Panel, West Panel, Traffic Alarms (only for WANGuard Platform), Autonomous Systems, Logs & Events, IP Addresses, Dashboards, Device Groups and IP Descriptions.

Dashboards, Device Groups and IP Descriptions can be filtered so you can give your customers access only to traffic reports and dashboards that contain fine-grained, relevant data.



IP Zones Setup

This chapter describes how to create and manage IP Zones. To add a new IP Zone, select Configuration from the West Panel and then expand the IP Zones Panel.

Understanding IP Zones

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

- 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 it's current IP Zone 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 55) 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 IPs and IP classes 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 the Network Basics You Should Be Aware Of chapter (Page 9).

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 the selected 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 and its not recommended setting *IP Graphs* and *IP Accounting* to “On” for it.

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

Changing Description, Duplicating & Deleting IP Zones

To change the description of an IP Zone you must first open the IP Zone Configuration Window, provide a new description and then press <Change Description>.

To copy the selected IP Zone you must click the <Duplicate IP Zone> 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 duplicate an existing IP Zone and modify only few parameters.

To delete an IP Zone you must first open the IP Zone Configuration Window, press <Delete IP Zone> button and then confirm the deletion.

IP Zone Configuration

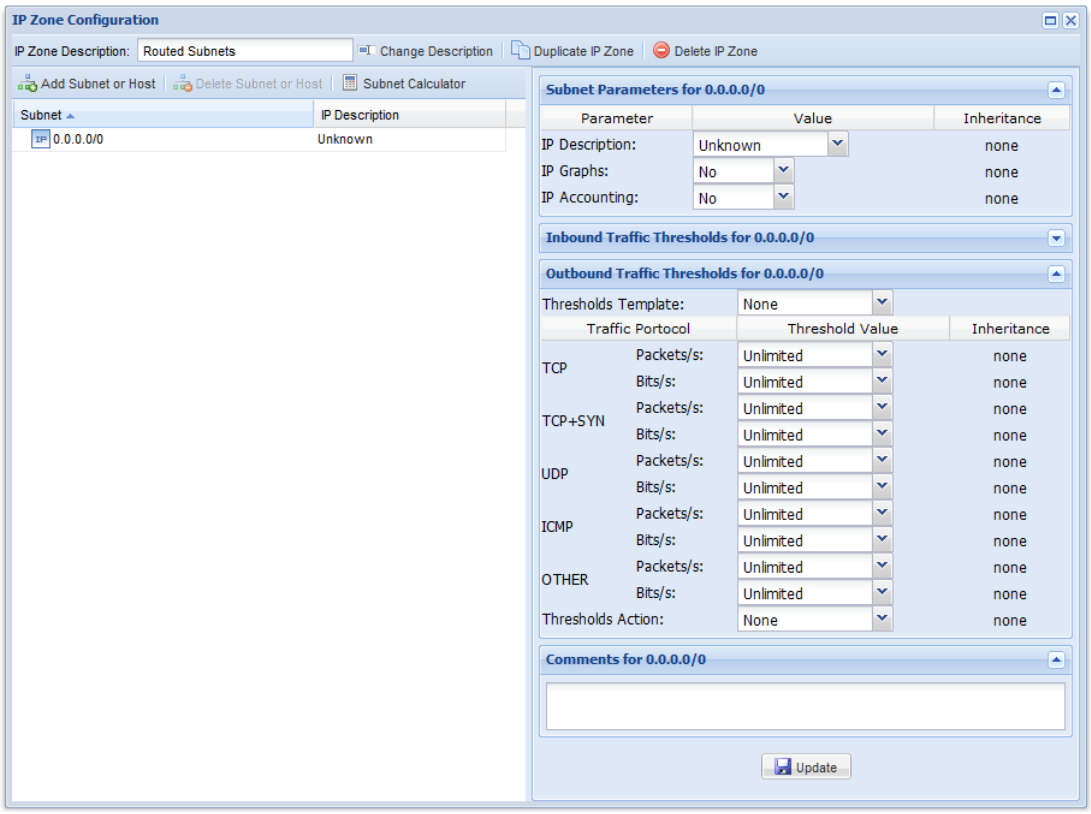
The IP Zone Configuration window is divided in two sections, one on the left and one on the right.

In the upper side of the left section you will see a button that is used to add IP addresses / subnets to the IP Zone. Below you will the allocated IP classes tree. When adding a new IP class, the tree is automatically updated. You may add or delete subnets by right-clicking any subnet row.

In the right section you will see detailed information about the selected IP class or IP address.

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 Subnets tree.

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



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 record stores the following information:

Subnet Parameters Panel

IP Description

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

IP Accounting

If the *IP 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 *IP 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.

IP Graphs

If the *IP Graphs* parameter is set to “Yes” then WANGuard Sensor records graphs data for every IP address included in the selected IP class. Graphs data contains accurate information about inbound and outbound

packets/second and bits/second rates. If the *IP Graphs* parameter is set to “Inherit” then the value is inherited from the parent IP class. If the parameter is set to “No” then no graphs will be generated for the current IP class.

Inbound and Outbound Traffic Thresholds Panel

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 Alarms Panel 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 (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 set the Threshold Value to Unlimited. To inherit the value of the parent IP class you must set the drop-down field to Inherit. To enter a threshold value, simple write the new value in the corresponding drop-down field. You can enter absolute values or multiples of 1.000 with K appended, 1.000.000 with M appended.

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.

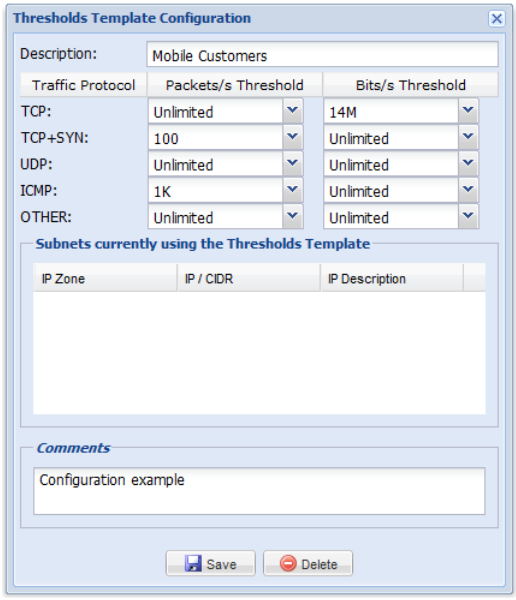
Comments Panel

Here you can provide details and comments about the subnet.

Thresholds Template

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 Configuration from the West Panel and then expand the Thresholds Template Panel.

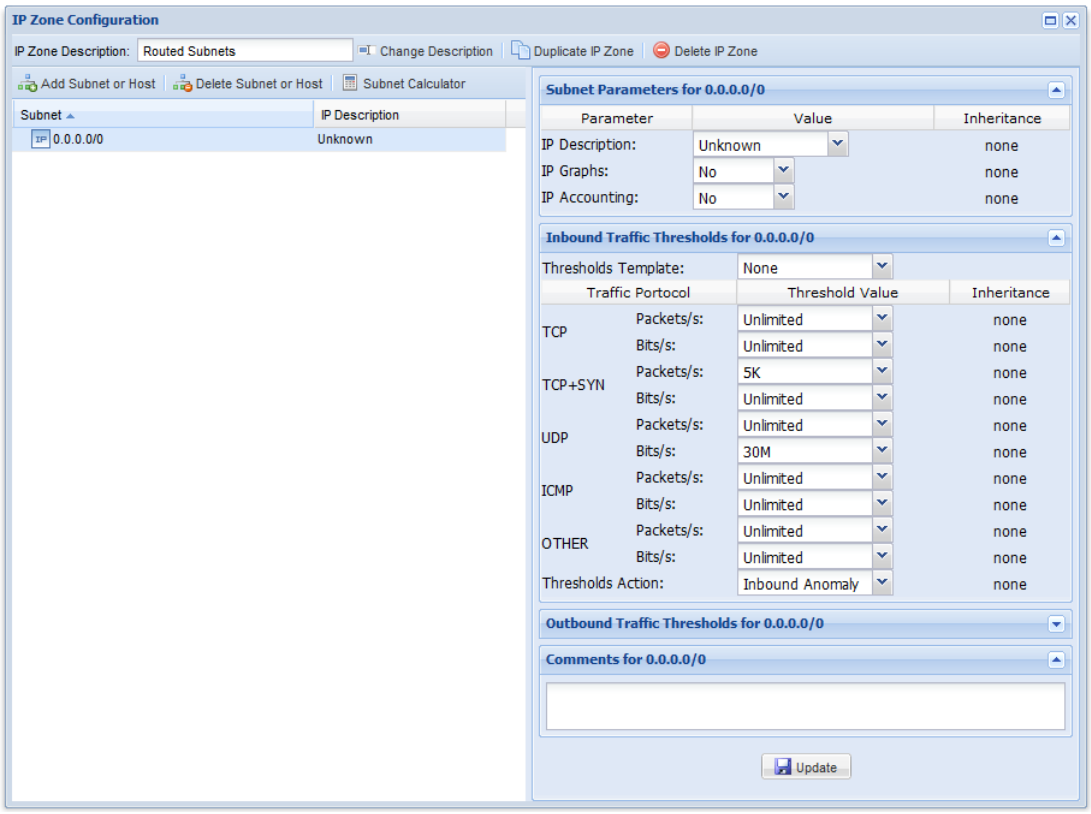
Most fields are explained in the Inbound and Outbound Traffic Thresholds section above. You will also see the IP classes and IP Zones that are using the selected template. When you update a template, every record using it will be updated too. An example of a Thresholds Template configuration is shown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



IP Zone Configuration Example

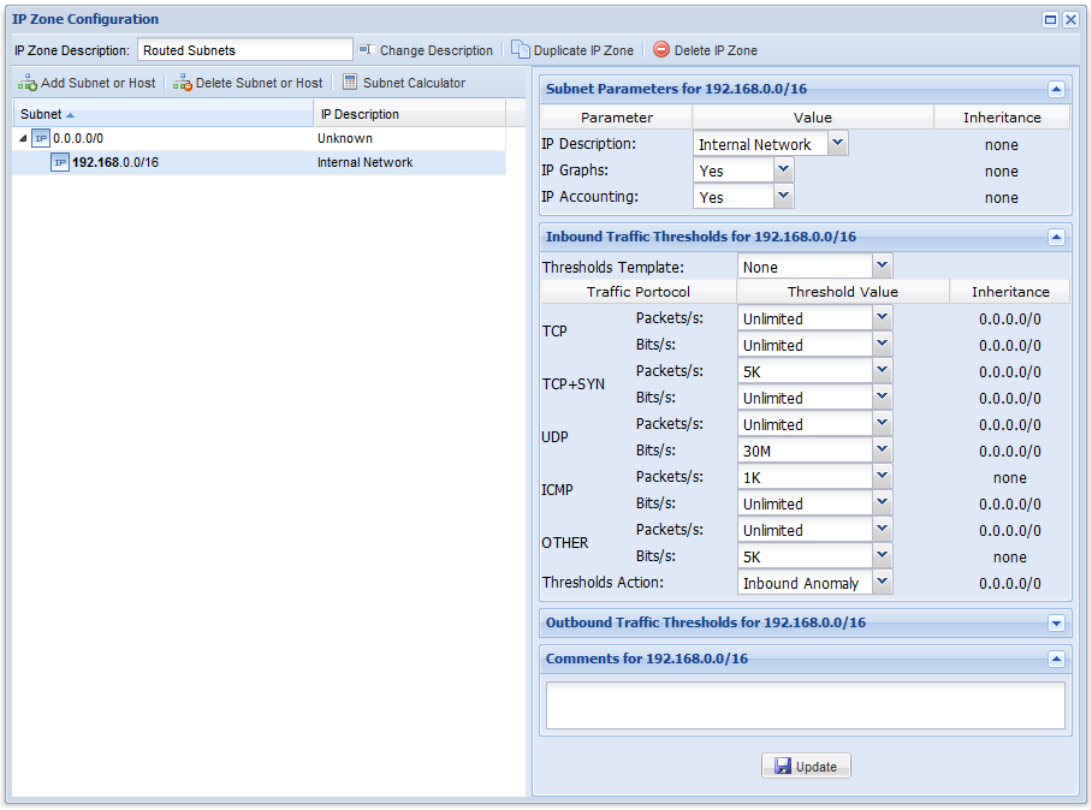
In the following images you can see how IP Zone inheritance works and how you can configure WANGuard Platform's features for various IP classes and IP addresses.

By default, the 0.0.0.0/0 IP class has all threshold values set to “Unlimited”, *Thresholds Actions* set to “None” and *IP Accounting* and *IP Graphs* set to “No”. In the screenshot below we defined new values for *TCP+SYN Packets/second* and *UDP Bits/second*, and we defined a new Inbound *Threshold Action*.



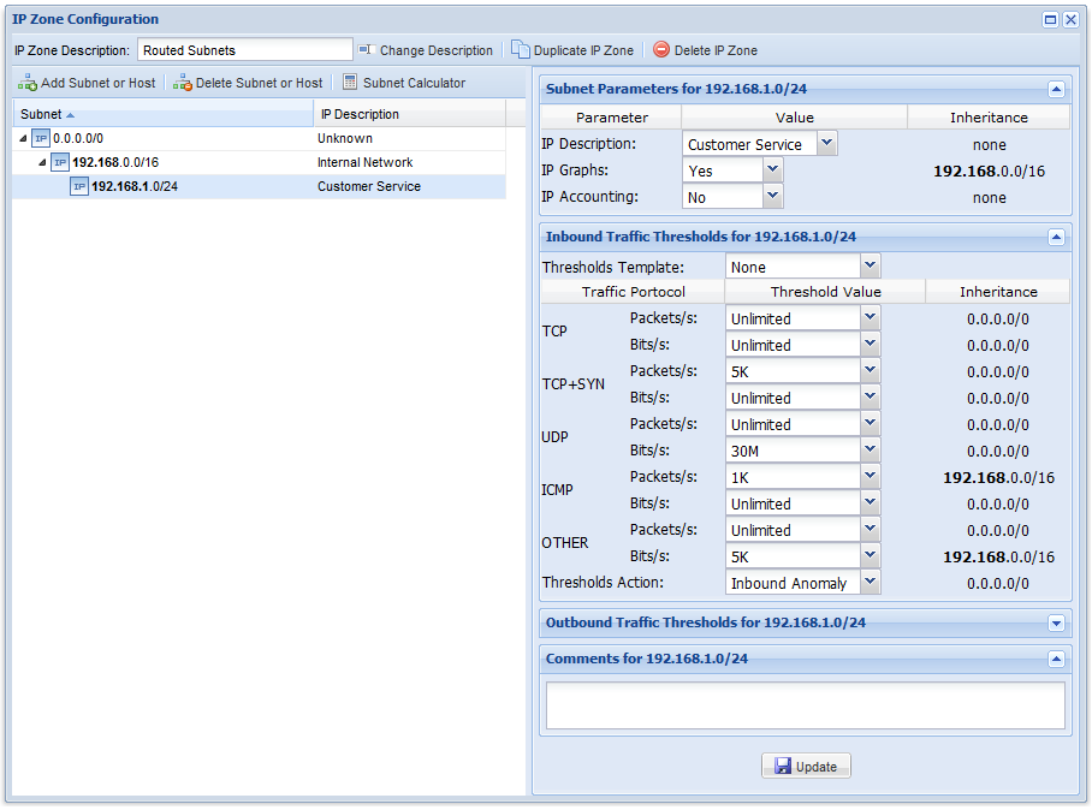
In the image below you can see that all the values are inherited from 0.0.0.0/0, except the following values: *ICMP Packets/second* (1000), *Other Packets/second* (10000) , *IP Accounting* (YES), *IP Graphs* (YES) and *IP Description* (Internal Network).

After adding the 192.168.0.0/16 IP class using the <Add Subnet or Host> button, 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.



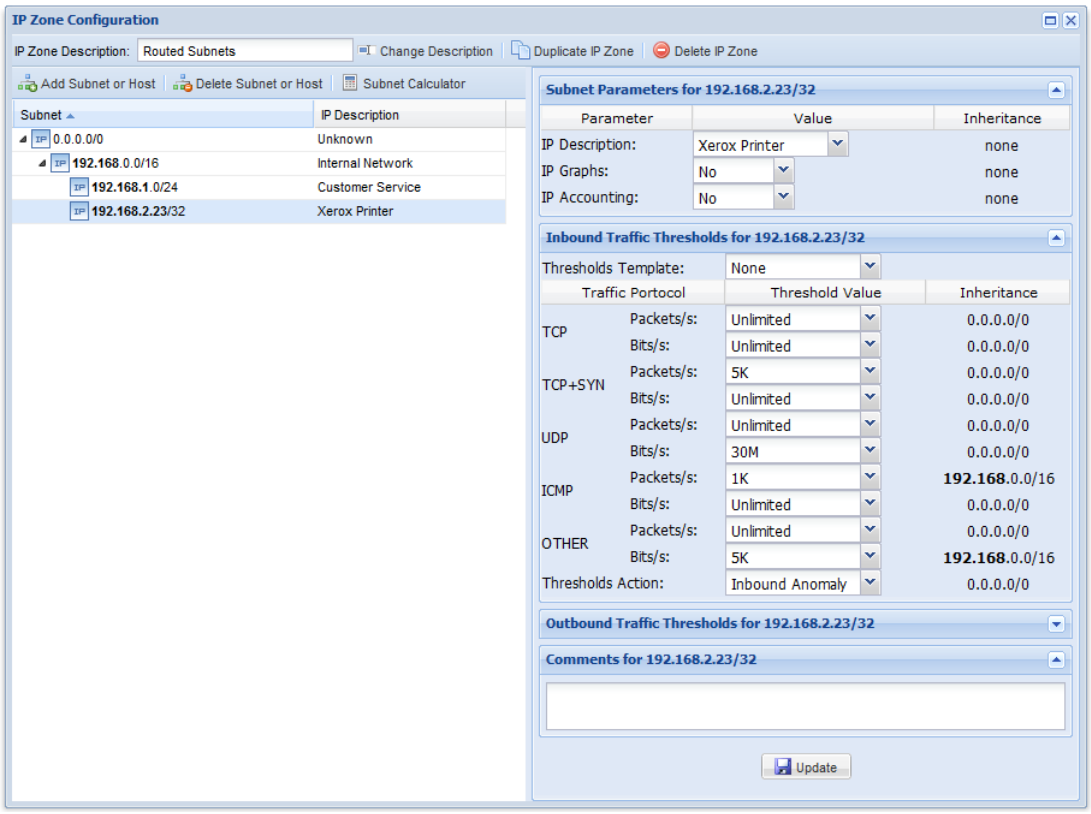
In the image below you can see that we added a new IP class called “Customer Service”, and only the *IP Description* and the *IP Accounting* values were changed. The other values are inherited from the direct parent 192.168.0.0/16, or from the parent's parent 0.0.0.0/0, if the direct parent didn't change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

Because the parent IP class has the *IP Accounting* parameter set to “Yes” and this IP class has the *IP Accounting* 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.



In the image below you can see that a new IP address called “Xerox Printer” is added, and only the *IP Accounting*, *IP Graphs* and *IP Description* values were changed. The rest of the values from “Internal Network” propagated to “Xerox Printer” because they were not modified.

“Xerox Printer” IP address is placed in the tree together with the “Customer Service” IP class because both are contained in the “Internal Network” IP class.


IP Zone Configuration
IP Zone Description: Routed Subnets
Change Description
Duplicate IP Zone
Delete IP Zone
Add Subnet or Host
Delete Subnet or Host
Subnet Calculator
Subnet
IP Description
0.0.0.0/0 Unknown
192.168.0.0/16 Internal Network
192.168.1.0/24 Customer Service
192.168.2.23/32 Xerox Printer
Subnet Parameters for 192.168.2.23/32
Parameter
Value
Inheritance
IP Description: Xerox Printer none
IP Graphs: No none
IP Accounting: No none
Inbound Traffic Thresholds for 192.168.2.23/32
Thresholds Template: None
Traffic Portocol
Threshold Value
Inheritance
TCP Packets/s: Unlimited 0.0.0.0/0
Bits/s: Unlimited 0.0.0.0/0
TCP+SYN Packets/s: 5K 0.0.0.0/0
Bits/s: Unlimited 0.0.0.0/0
UDP Packets/s: Unlimited 0.0.0.0/0
Bits/s: 30M 0.0.0.0/0
ICMP Packets/s: 1K 192.168.0.0/16
Bits/s: Unlimited 0.0.0.0/0
OTHER Packets/s: Unlimited 0.0.0.0/0
Bits/s: 5K 192.168.0.0/16
Thresholds Action: Inbound Anomaly 0.0.0.0/0
Outbound Traffic Thresholds for 192.168.2.23/32
Comments for 192.168.2.23/32
Update

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 in your network.

Supported Traffic Capturing Methods

WANGuard Sensor was designed to monitor the largest enterprises with hundreds of thousands of endpoints to the smallest branch office with tens of endpoints. The supported traffic capturing methods work with most switches, routers, firewalls and other network devices. The 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® & sFlow® Monitoring** – The analysis of pre-aggregated data flows sent by NetFlow®, sFlow® or NetStream® enabled routers and Layer 3 switches. The WANGuard Sensor that handles NetFlow®, sFlow® 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 topology and configuration, your needs and your hardware, you must choose between the three methods of traffic capturing. For high availability scenarios you could 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 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® & sFlow® Monitoring

NetFlow or sFlow Monitoring is the domain of networks that usually use layer 3 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® & sFlow® Monitoring Works

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

Network devices with NetFlow & sFlow 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® & sFlow® Monitoring

Because the NetFlow and sFlow protocols already perform 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 or sFlow the ideal option for monitoring remote, high-traffic networks.

The downside of the NetFlow and sFlow 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 packet sampling is used.

Comparison between Packet Sniffing and NetFlow® / sFlow® Monitoring

The table below provides a quick comparison between the three available traffic capturing technologies. The system 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	sFlow®, 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, HP and others.

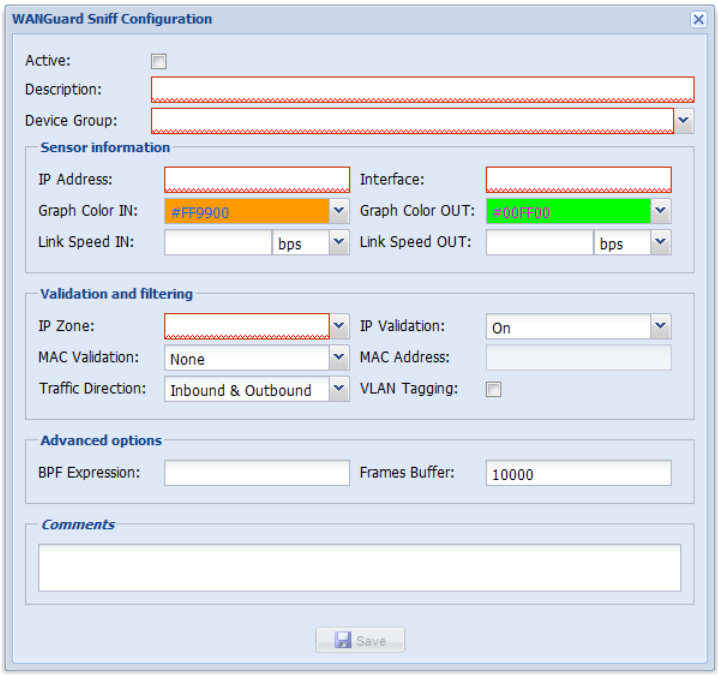
WANGuard Sensor Setup

This chapter describes how to configure WANGuard Sensor systems through WANGuard Console. To manage WANGuard Sensor systems you must first click Configuration from the West Panel and then expand the WANGuard Sensor Panel. 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 52).

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 Configuration window contains the following fields (red fields are mandatory):

- **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.

- **Device Group**

  A short description of the role the monitored device plays within the network, it's location etc.

- **IP Address**

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

- **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.

  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.

- **Graph Color In + Out**

  Here you can select the color you will see on sensor graphs as inbound and 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 clicking the drop-down menu.

- **Link Speed In + Out**

  The speed of the monitored links for Inbound traffic and for Outbound traffic. This is used to generate reports based on usage percent.

- **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 consult IP Zones Setup chapter (page 43).

- **IP Validation**

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

  IP Validation parameter has three options:

  - *Off* - Will disable IP Validation. Make sure MAC Validation 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.

- **MAC Validation + MAC Address**

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

  The MAC Address should contain the MAC address of the upstream router (with the MAC Validation field set to Upstream) or the MAC address of the downstream router (with the MAC Validation field set to Downstream). The MAC Address must be written using the Linux convention - six groups of two hexadecimal values separated by colons (**:**).

- **Traffic 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.

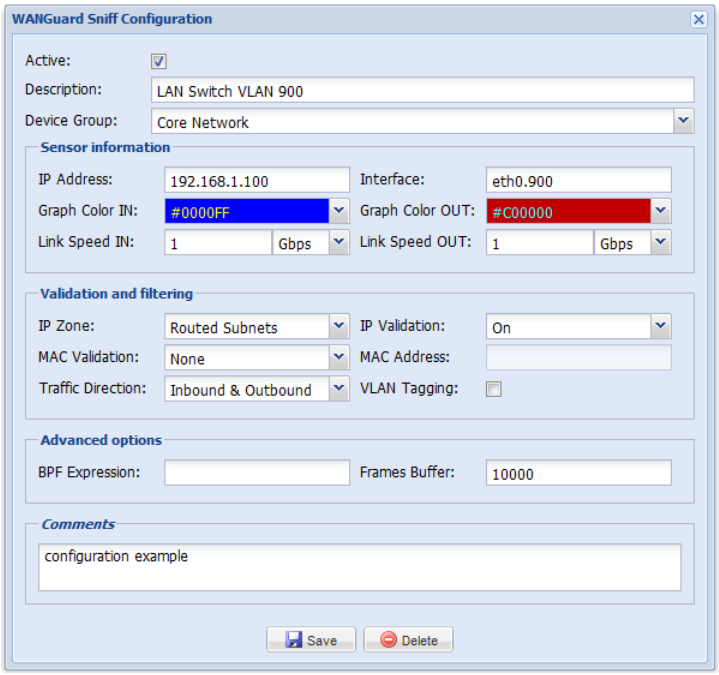
- **VLAN Tagging**

  If the traffic is tagged with a VLAN header and you check VLAN Tagging then the VLAN header for each packet 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.

- **Comments**

  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 and uses IP class information found in the “Routed Subnets” IP Zone for validation.

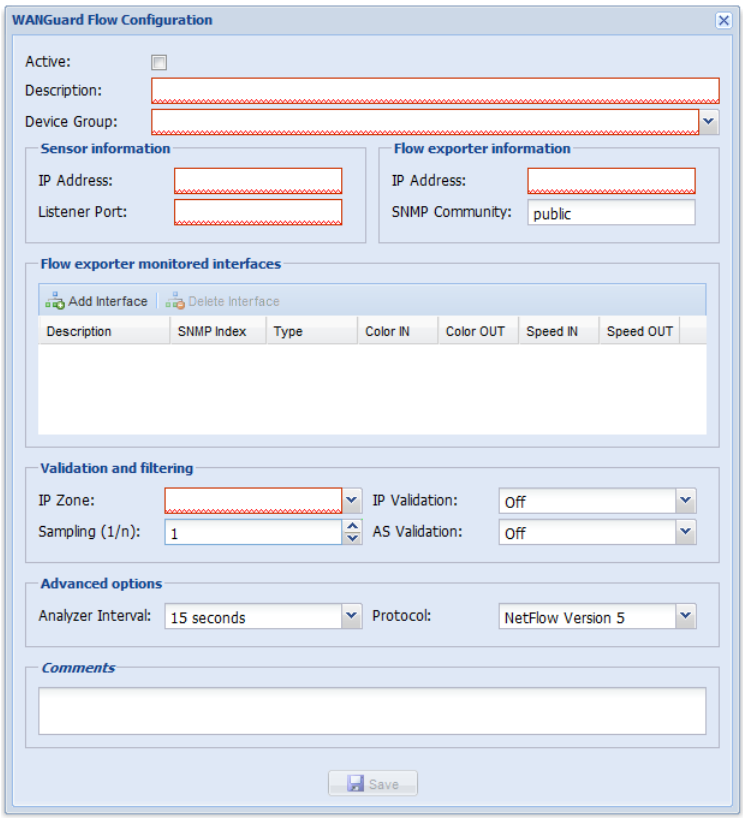


After a new WANGuard Sniff system is added, the WANGuard Sensor panel is updated. If there is a green “OK” sign on the right of the WANGuard Sniff's description then the WANGuard Sniff is running. If there is a “X” red sign instead, then the WANGuard Sniff is inactive or not running.

If you checked the Active switch but the WANGuard Sniff is still not running after few seconds, you can find a description of the error in the WANGuard Sniff Events Logs (see Logs & Events chapter – Page 34) or in the Events Tab in South Panel.

WANGuard Flow Configuration

When using WANGuard Flow, network devices must be configured to send sFlow or NetFlow® v. 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 81).



The WANGuard Flow Configuration window contains the following fields (red fields are mandatory):

- **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.

- **Device Group**

  A short description of the role the monitored device plays within the network, it's location etc.

- **Sensor IP Address + Listener Port**

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

- **Flow Exporter IP Address + SNMP Community**

  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.

  The read-only SNMP community of the network device allows WANGuard Console to connect to the

flow exporter and request SNMP indexes and other useful information for adding new interfaces.

- **Flow Exporter Monitored Interfaces**

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

  - *Description* - A short, generic description used for interface identification.
  - *SNMP Index* - The SNMP index of the interface. When adding a new interface, if you entered the SNMP community then simply click the interface to automatically add required parameters.
  - *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 In + Graph Color Out* - Here you can select the color you will see on sensor graphs as inbound and Outbound traffic for the current WANGuard Flow. 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.
  - *Link Speed In + Link Speed Out* - The speed of the monitored interface for Inbound traffic and for Outbound traffic. This is used to generate reports based on usage percent.

- **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 consult IP Zones Setup chapter (page 43).

- **Sampling (1/n)**

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

- **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.

- **Analyzer Interval**

  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.

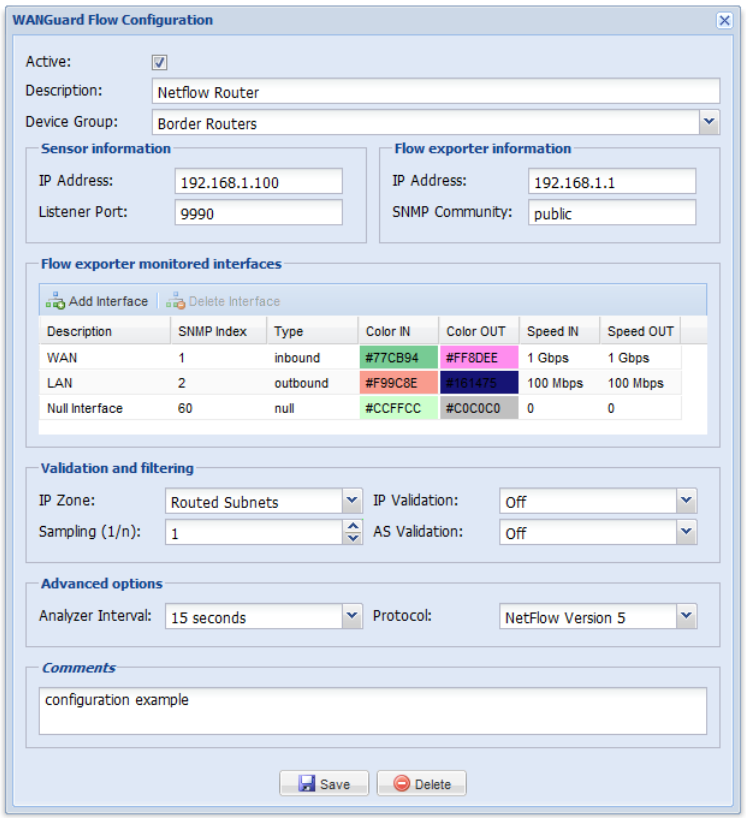
- **Protocol**

  You can use WANGuard Flow with Netflow version 5, or sFlow through a sflowtool wrapper.

- **Comments**

  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 uses IP class information found in the “Routed Subnets” IP Zone.



After a new WANGuard Flow system is added, the WANGuard Sensor panel is updated. If there is a green “OK” sign on the right of the WANGuard Flow's description 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 after few seconds, you can find a description of the error in the WANGuard Flow Events Logs (see Logs & Events chapter – Page 34) or in the Events Tab in South Panel.

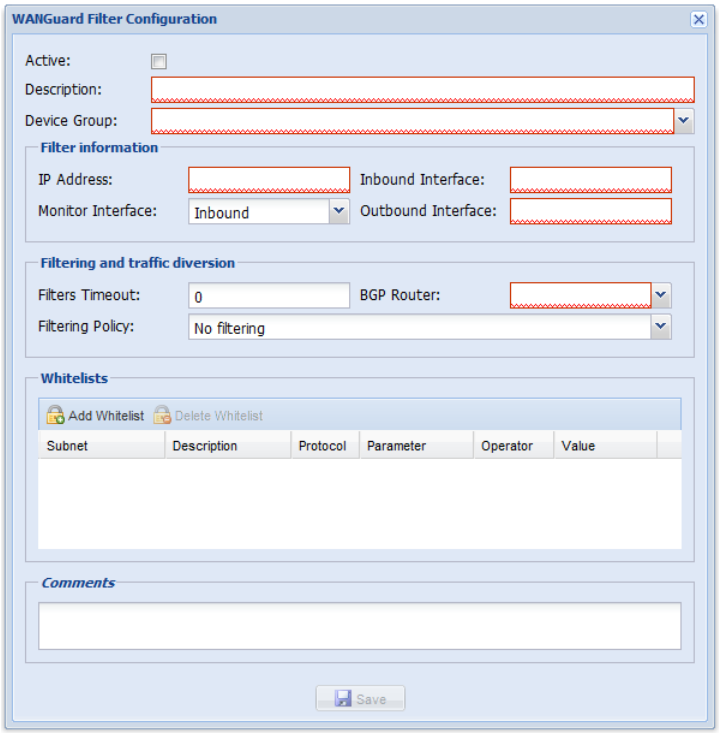
WANGuard Filter Setup

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 88). Keep in mind that our support team can help you with any configuration issues.

If you don't plan to use WANGuard Filter or the license you acquired does not include it, you can skip this chapter.

WANGuard Filter Configuration

This chapter describes how to configure WANGuard Filter systems through WANGuard Console. To manage WANGuard Filter systems you must first click Configuration in the West Panel and then expand the WANGuard Filter panel. Keep in mind that our support team can help you with any configuration issues you might have.



The WANGuard Filter Configuration window contains the following fields (red fields are mandatory):

- **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.

- **Device Group**

  A short description of the role the protection server plays within the network, it's location etc.

- **IP Address**

  An unique IP address configured on the machine that runs 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 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 though the outbound interface, and are not being analyzed. The disadvantage is that the attack statistics are not complete.

- **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 77). 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 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 used only when debugging Netfilter rules.

- **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 you don't want to 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 add a new rule to the Whitelist you must enter the following fields:

- **Subnet**

  The attacked IP address should be included in this subnet. You can set this to 0.0.0.0/0 for generic whitelists.

- **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.

When an attack pattern cannot be filtered because it conflicts with the WANGuard Filter's Whitelist then the attack pattern is reported in the Active Traffic Anomalies Tab with a red exclamation point besides.

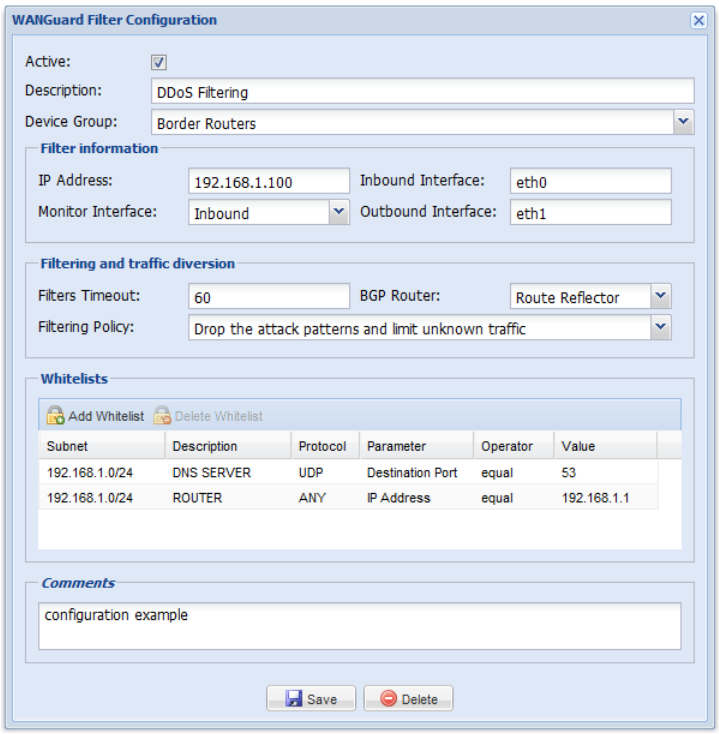
- **Comments**

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

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

WANGuard Filter Configuration Example

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 Active Traffic Anomalies Tab with the latest information about the detected attack patterns. The malicious traffic will be dropped, while the clean traffic will be forwarded through the eth1 interface and injected back into the network.



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.

Every monitored IP class that's defined in the current IP Zone may have it's own Action configured. When a traffic threshold value defined for an IP is reached, the defined Action for the IP's subnet is executed by WANGuard Sensor and, if installed and activated, by WANGuard Filter.

To add a new Action, select Configuration from the West Panel and then expand the Actions Panel.

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.

Action Modules are executed in three situations, each having it's own panel:

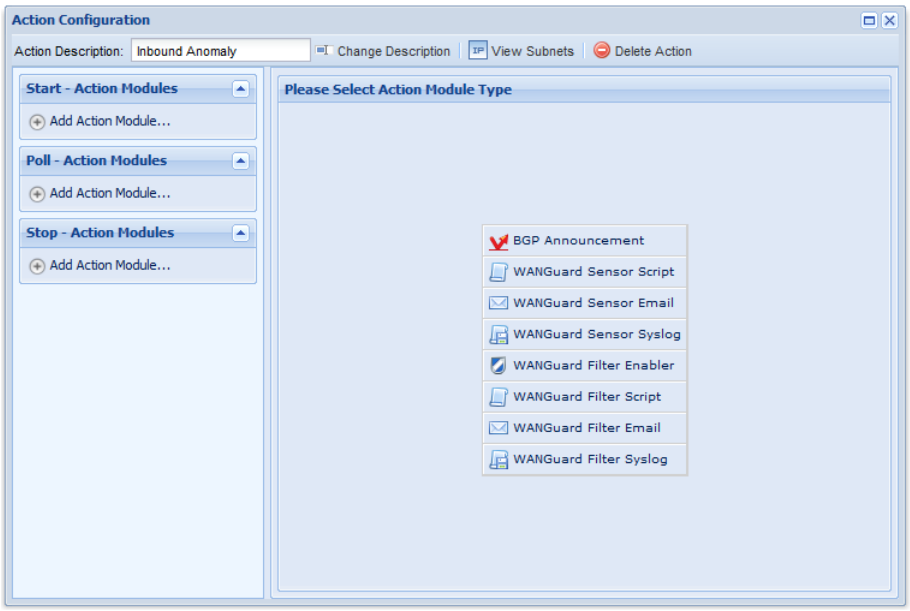
- **Start – Action Modules** - Action Modules added to this panel are executed once, immediately after the traffic anomaly or attack pattern has been detected.
- **Poll – Action Modules** - Action Modules added to this panel are executed periodically, every 5 seconds, while the traffic anomaly or attack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

To modify, delete or rename an Action Module you must select the Action Module description in the left section.

The <View Subnets> button allows you to 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 need 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 left panel and click Add Action Module.



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

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 panel. 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

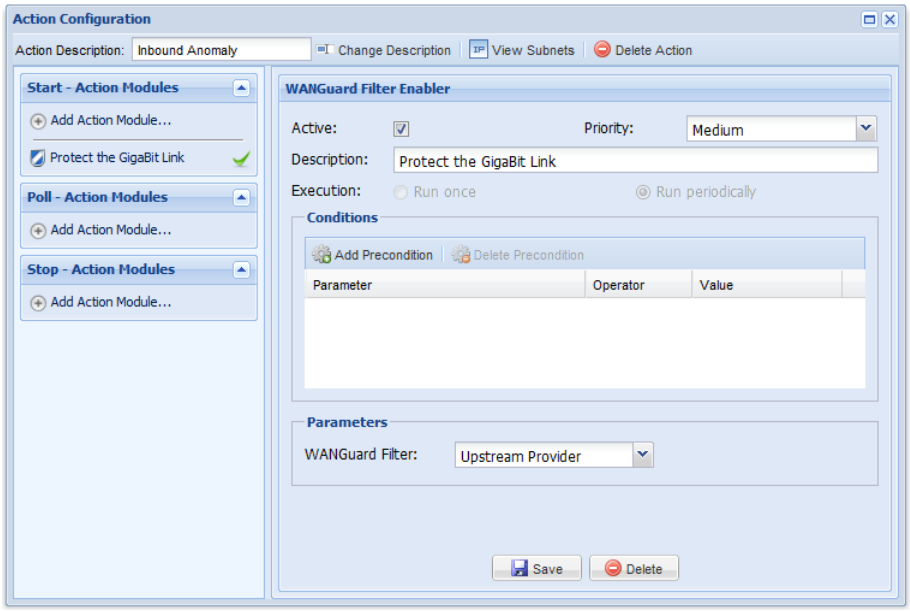
Sensor and WANGuard Filter systems. A complete list of Conditional Parameters is available in Appendix 2 – Conditional & Dynamic Parameters (Page 85).

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

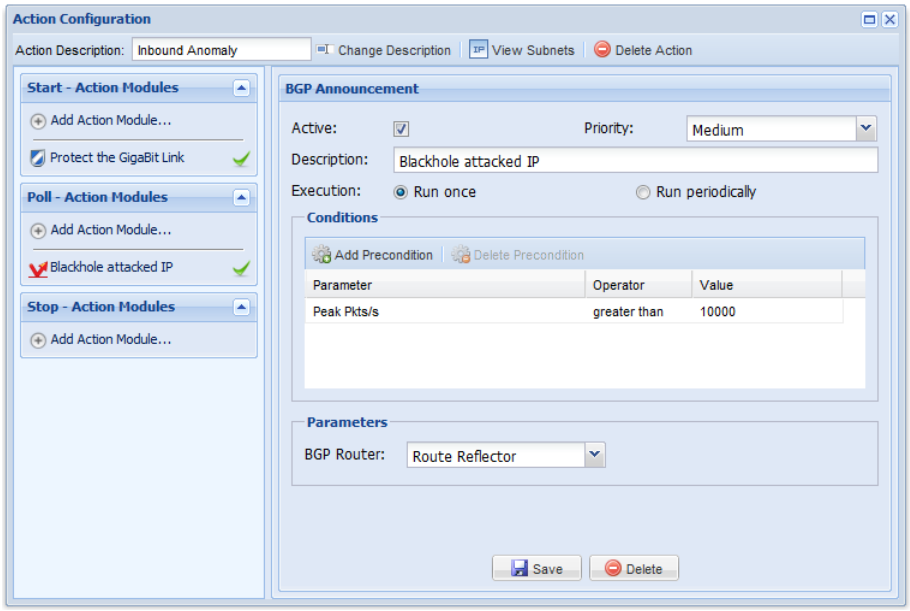
The WANGuard Filter Enabler Action Module is used by WANGuard Sensor to activate a WANGuard Filter for mitigation purposes. This module should be activated at the beginning of a traffic anomaly, or while polling the traffic anomaly if you check the *Run Once* checkbox and use Preconditions (to check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



BGP Announcement Action Module

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 77).

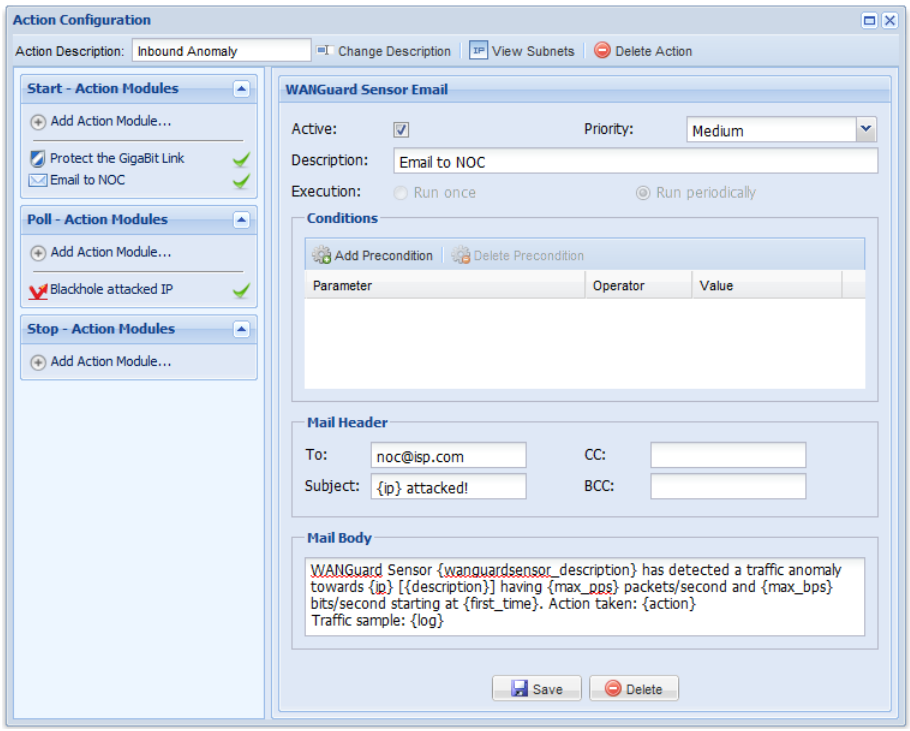


WANGuard Sensor Email Action Module

This module is used by WANGuard Sensor to send notification emails at the beginning (Start – Action Modules), during (Poll - Action Modules), or at the end (Stop – Action Modules) of a traffic anomaly.

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 85).

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.



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 (Start – Action Modules), during (Poll - Action Modules), or at the end (Stop – Action Modules) of a traffic anomaly.

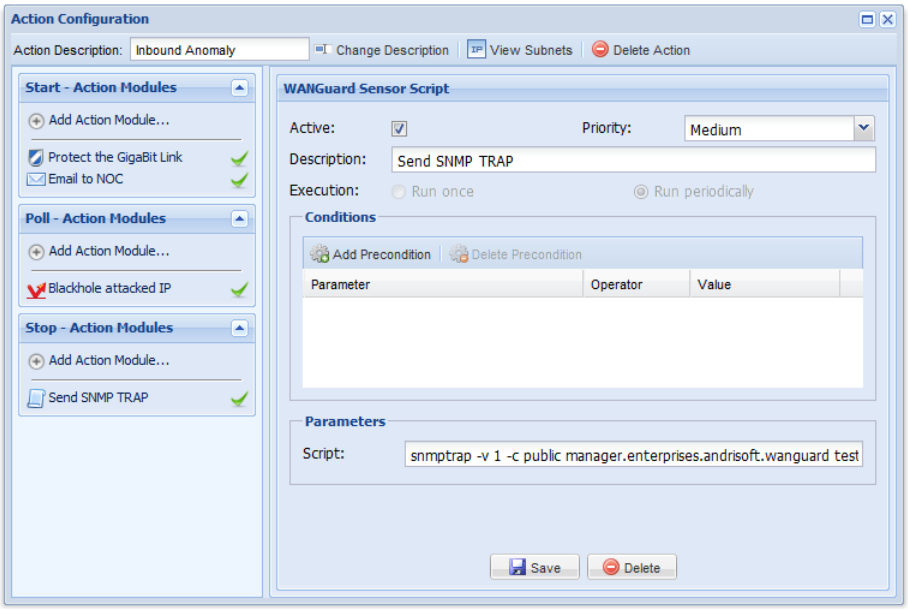
Scripts can access WANGuard Sensor Dynamic Parameters through command-line parameters / options. The scripts are executed locally on each WANGuard Sensor system that uses Actions that include this module. Multiple commands can be executed using the ";" separator.

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.



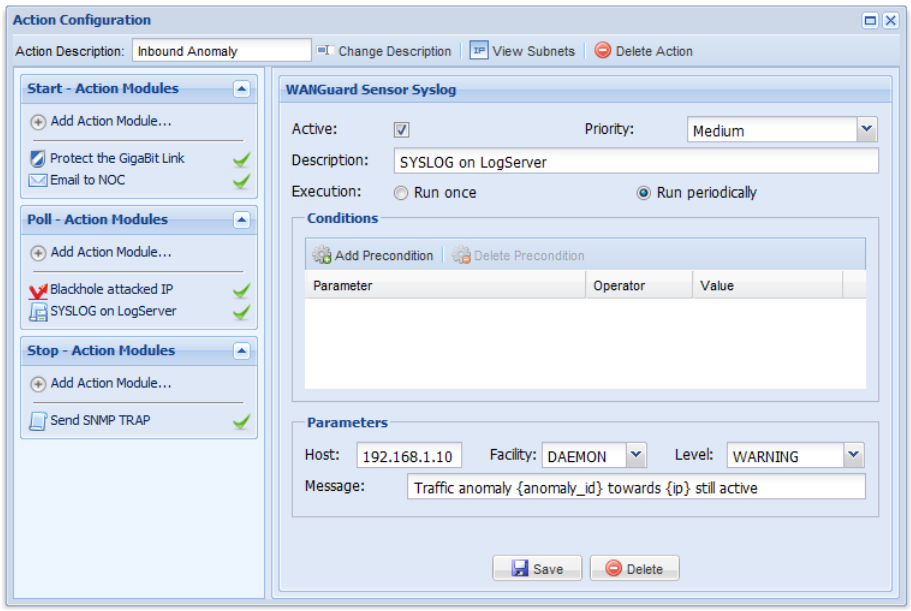
WANGuard Sensor Syslog Action Module

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 (Start – Action Modules), during (Poll - Action Modules), or at the end (Stop – Action Modules) 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 (Start – Action Modules), during (Poll Action Modules), or at the end (Stop – Action Modules) of an attack pattern.

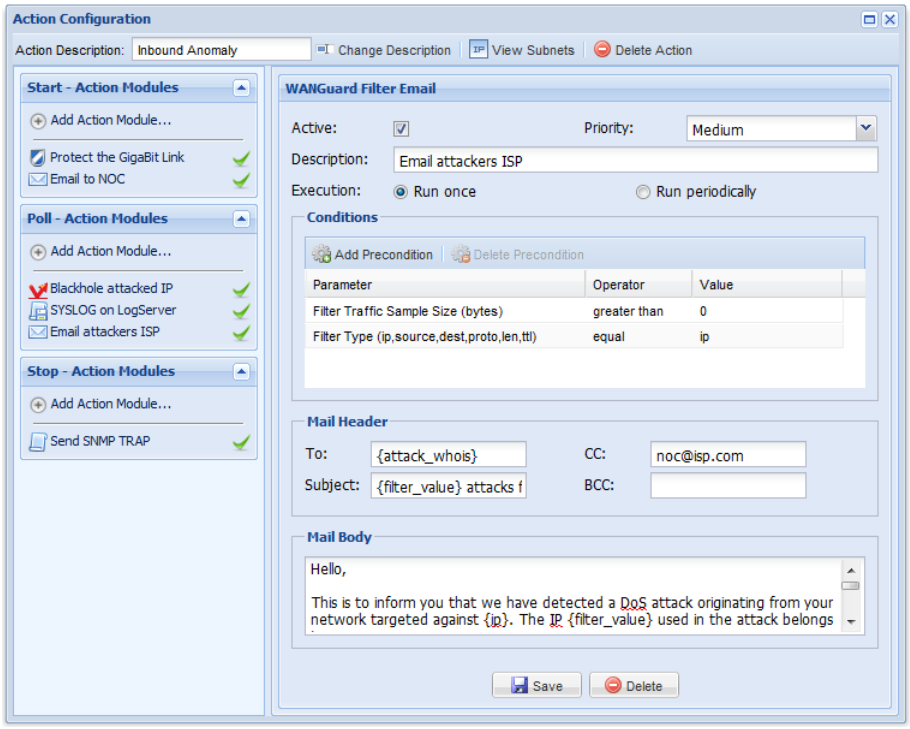
The *Subject* and *Body* fields can contain any number of WANGuard Sensor and WANGuard Filter Dynamic Parameters. Dynamic Parameters are explained at the beginning of the chapter. A complete list of Dynamic Parameters available can be found in Appendix 2 – Conditional & Dynamic Parameters (Page 85).

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 {filter_tcpdump}, you must do the following:

- Send the notification emails in the Poll – Action Modules panel instead of the Start – Action Modules panel.
- 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 *Run Once* to only allow the module to be executed one time per attack pattern. If you do not check that emails will be sent every 5 seconds.

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



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.

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 (Start – Action Modules), during (Poll - Action Modules), or at the end (Stop – Action Modules) 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 85).

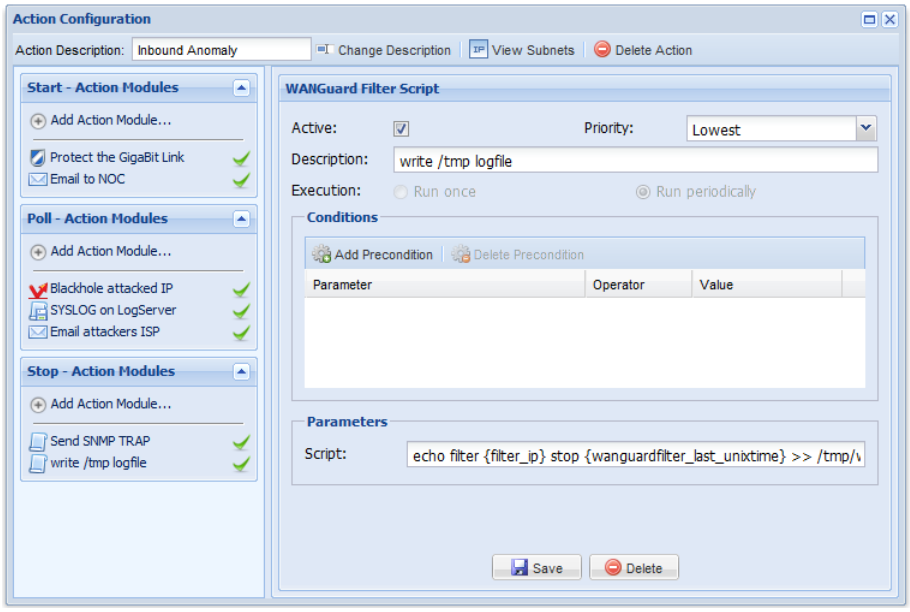
The scripts are executed locally on each WANGuard Filter system that uses Actions that include this module. Multiple commands can be executed using the ";" separator. Scripts executed through the WANGuard Filter Action

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 (Start – Action Modules), during (Poll - Action Modules), or at the end (Stop – Action Modules) 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 85).

BGP Router Setup

Operators can view, send and withdraw BGP announcements from WANGuard Console through the Autonomous Systems Panel. All records about BGP announcements are stored in the Logs & Events Panel (Page 34).

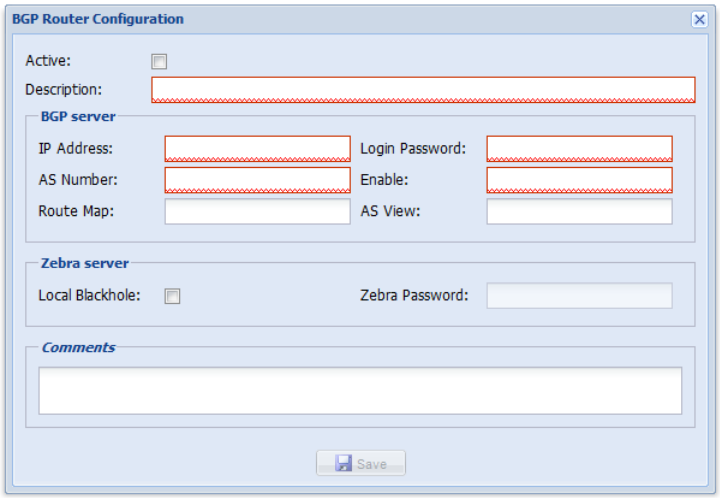
WANGuard Sensor and WANGuard Filter can be configured to send and withdraw BGP announcements automatically, in the following cases:

- 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.

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 88).

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 70) is executed. BGP announcements are sent automatically by WANGuard Filter when a BGP router is selected in the WANGuard Filter's configuration (Page 63).



The BGP Router Configuration window contains the following fields (fields in red are mandatory):

- **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.

- **Login Password**

  The password required when connecting to the bgpd daemon.

- **Enable Password**

  Configuration mode password of the bgpd daemon.

- **Route Map**

  The route-map that should be appended to each announcement.

- **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.

- **Local Blackhole**

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

- **Zebra Password**

  The password for the zebra or quagga daemons.

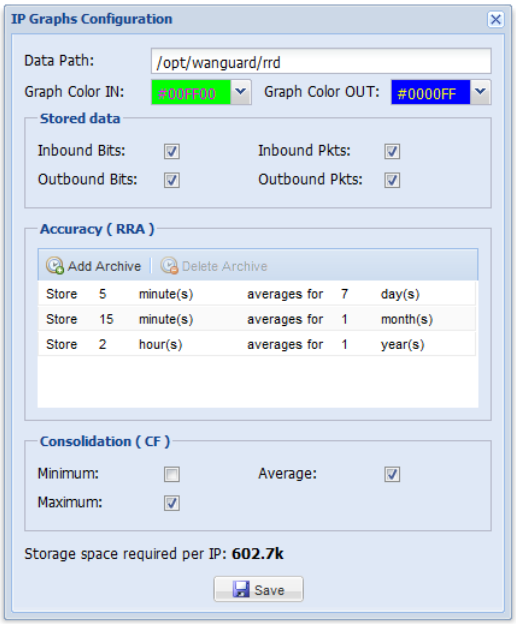
- **Comments**

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

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

IP Graphs Setup

To configure IP traffic graphs parameters expand the WANGuard Console Panel from the Configuration zone in the West Panel.



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

The first accuracy parameter (5 minutes) specifies the granularity of the graphs. You can set the granularity value between 5 seconds and 5 minutes. When using WANGuard Flow, do not set the granularity parameter to a lower value than the Analyzer Interval parameter. When granularity has a low value, 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 **Stored Data** options lets you select the traffic parameters that will be stored.

The **Consolidation** 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* value will be updated when you click the <Update> button. If you change the graphs parameters, make sure you delete old .rrd files from the defined **Data Path**.

Help Menu & About

Help Menu

The Help menu is located on the upper-right side of the WANGuard Console window.

User Manual

The User Manual provides a contextual access to the WANGuard Platform User Guide. Depending on the context, the User Guide will open at the chapter describing the last opened window or tab. 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 .

The IP Protocols List window provides access to a table that contains descriptions for all available IPv4 protocols. The TCP&UDP Ports List window provides access to a table that contains name, description, service, common servers and common clients for well known TCP and UDP port numbers.

Subnet Calculator

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

About

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

Appendix 1 – Configuring NetFlow Data Export

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

Configuring NDE on an IOS Device

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

First enable Cisco Express Forwarding:

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

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

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

For example:

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

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

Enable the exports of these flows with the global commands:

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

Use the IP address of your WANGuard Flow server and the configured listening port. UDP port 2000 is used as an example. WANGuard Flow is using NetFlow version 5. The ‘ip flow-export source’ command is used to set up the source IP address of the exports sent by the equipment.

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

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

The following commands break up flows into shorter segments: 1 minute for active traffic and 30 seconds for inactive traffic. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

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

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

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

Configuring NDE on a CatOS Device

In privileged mode on the Supervisor Engine enable NDE:

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

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

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

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

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

The following commands break up flows into shorter segments: ~1 minute for active flows and ~ 30 seconds for inactive flows. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

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

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

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

And enable NDE:

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

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

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

Configuring NDE on a Native IOS Device

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

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

The following commands break up flows into shorter segments: ~1 minute for active flows and ~ 30 seconds for inactive flows. Please use only this values as it decreases the RAM usage and increases performance of WANGuard Flow.

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

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

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

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

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

Configuring NDE on a 4000 Series Switch

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

Configuring NDE on a Juniper Router

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

```
interfaces {
      ge-0/1/0 {
            unit 0 {
                  family inet {
                        filter {
```

```
                                input all;
                                output all;
                        }
                        address 192.168.1.1/24;
                }
        }
    }
}
firewall {
    filter all {
        term all {
            then {
                sample;
                accept;
            }
        }
    }
}

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

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.

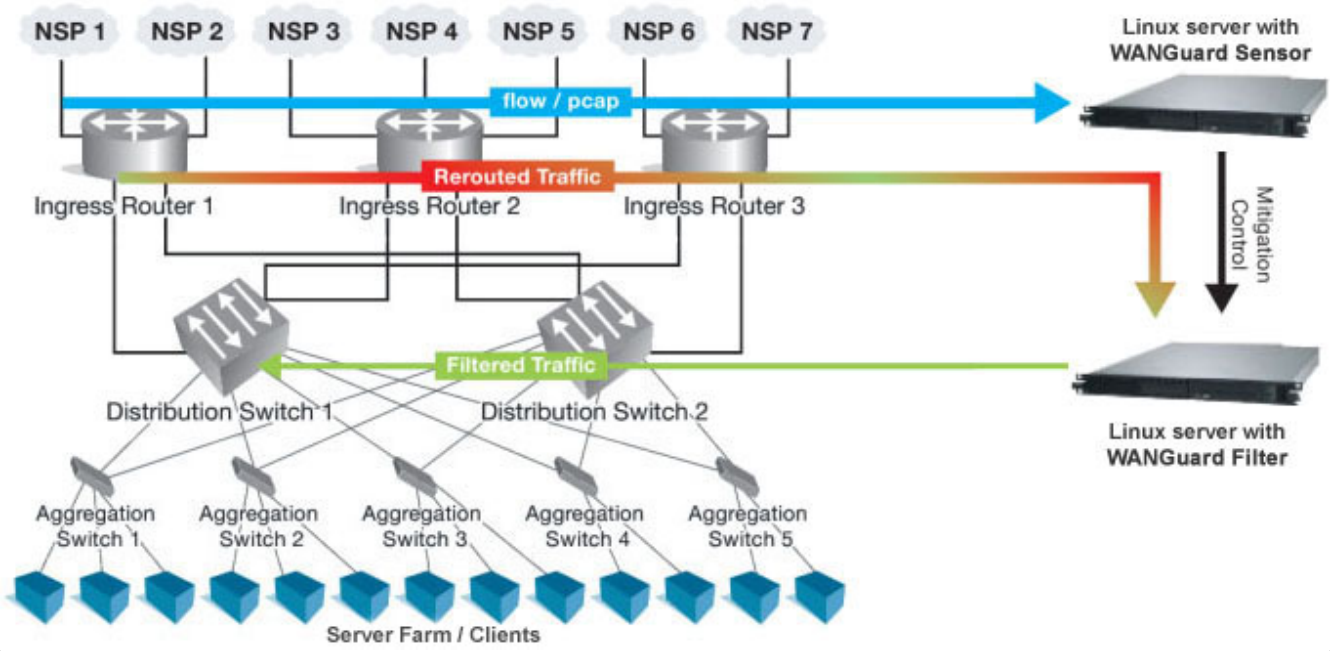
Understanding the BGP Diversion Method

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 63) with the Outbound Interface set to the virtual network interface created by the tunnel.