Graphs and Reports Guide

Gatedefender

Contents

1. Introduction

The aim of this guide is to offer a detailed description of the reports and graphs generated by Panda Gatedefender, and which can be accessed through the product's Web console.

The system of reports and graphs in the Gatedefender series has two basic objectives relating to security management and the performance of computers on the network:

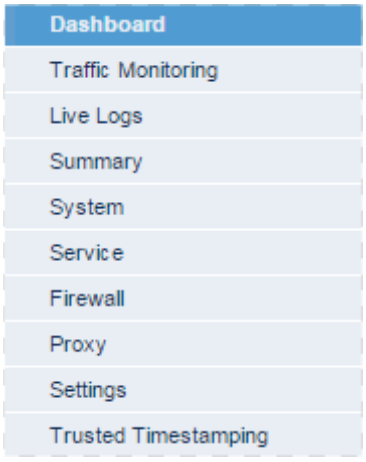
- To provide detailed information about the network security status in order that any appropriate measures can be taken through the various traffic protection modules in the Gatedefender device.
- To give a clear, real-time picture of network resources consumed through Internet access. This then makes it easy to pinpoint computers that are inappropriately using resources and take any necessary action. The Gatedefender series devices include mechanisms for such purposes, including bandwidth restrictions (QoS), Web filtering and application filtering, among others.

The reports and graphs service is delivered with all Gatedefender models, including software, virtual or hardware/appliance solutions. This feature does not therefore require a separate license.

2. General overview of graphs and reports

All the report and graph functions can be accessed through the Logs and Reports tab in the top Menu bar, split into two sections: Dashboard and Traffic Monitoring.

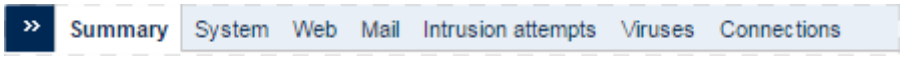
2.1. Dashboard



In the Dashboard menu, there are seven tabs related to the network protection activity of the Gatedefender device. Different types of graphs are available (line, bar, pie…) to illustrate this activity, as well as groups of data displayed in tables. Some of these are timeline graphs displaying how the activity has varied over time.

2.1.1. Available modules

Each tab in the Dashboard menu refers to a module in the Gatedefender device. Below is a brief summary of each tab:



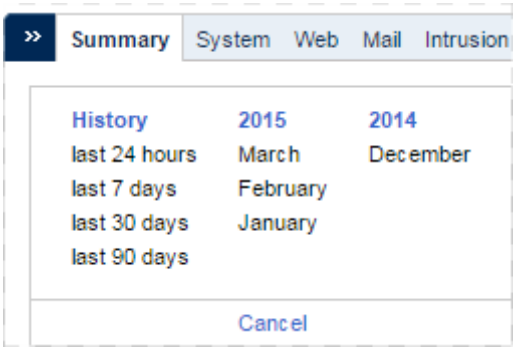
- Summary: This contains a summary of the Gatedefender device activity, mainly focused on network security.
- System: This reflects the internal status of the Gatedefender device at an operational level.
- Web: This shows the activity of the filter of the Web content accessed by users.
- Mail: This displays the activity of the spam filter.
- Intrusion attempts: This shows the activity of the protection against intrusion attempts.
- Viruses: This displays the detections of any threats.
- Connections: Here you can see the number of connections made by computers on the network, organized by type of connection (local, VPN, HotSpot).

2.1.2. Common features

All the graphs in the Dashboard section have several controls for defining the amount of data displayed, printing the data or selecting the data series that will be included in the graphs.

Time filters

By selecting the  icon in the top left of the graph you will see a panel that lets you filter the data to include in the graph. By default the graphs will display data for the last 24 hours.

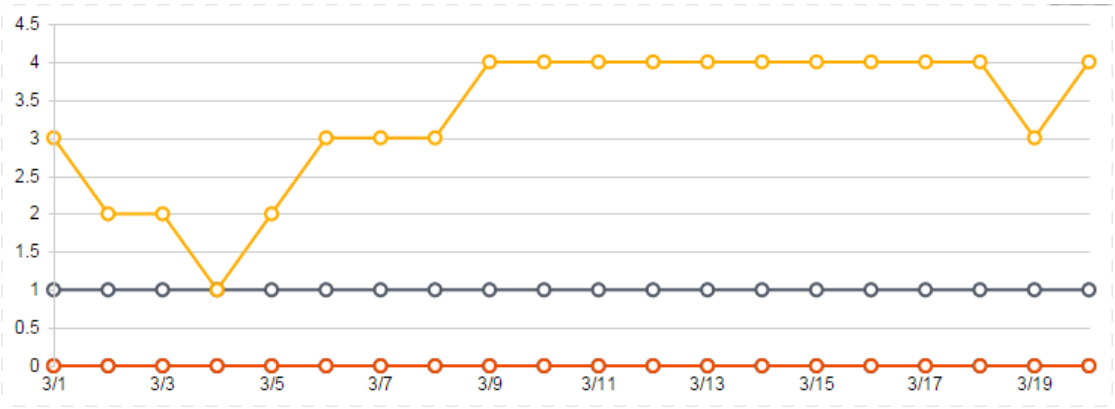


This is a dynamic panel that displays different time periods depending on the information available in the Gatedefender device for specific dates. The options available are:

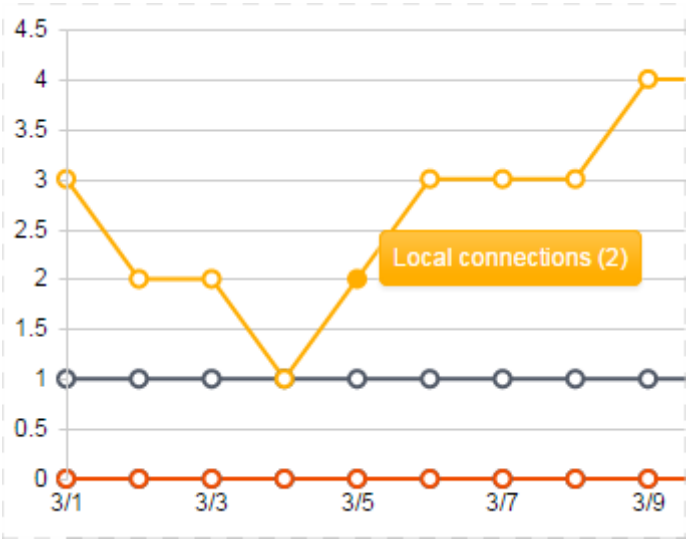
- Last 24 hours
- Last 7 days
- Last 30 days
- Last 90 days
- The months of each year that Gatedefender has been active.

Line graphs

The line graphs or histograms represent the fundamental information in each section of the Dashboard. These graphs reflect the activity of the Gatedefender device for a specific module, with the x axis indicating the time period and the y axis the number of events for the module in question.

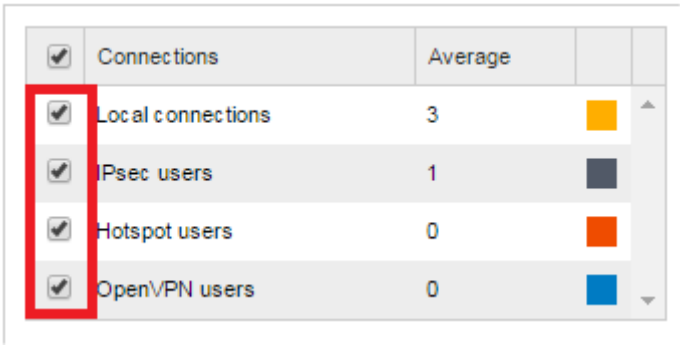


Moving the mouse pointer across the points in the graph will display an explanatory text with the data series name and the value at this point. This makes it easier to interpret the graph.



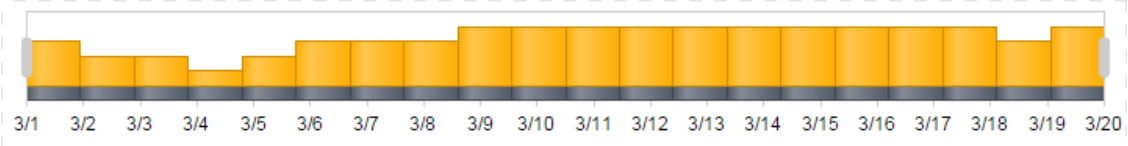
Selecting the data series displayed

Below some of the graphs there is a table with the data series that are represented. Each series has a different color and a checkbox to include it or omit it from the graph. There is also a field (Average or Count) highlighting the average data for the selected period for each data series or a counter with the number of events.



Stacked column charts

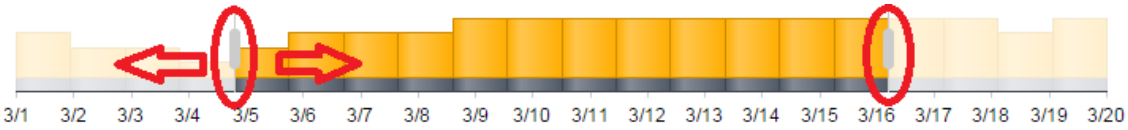
Immediately below the line graphs there is an equivalent graph in the form of a stacked column chart, using the same color codes.



This graph displays the same information as the line graph but in a different way, in order to help interpret the data.

Selecting the time period displayed

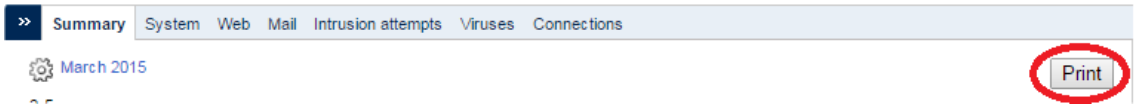
For greater accuracy in selecting the time period for the items displayed, there are two sliding markers to help select the data more precisely.



When you move these markers, the rest of the items in the tab are automatically updated to display data corresponding to the selected period.

Printing graphs

The Print button opens the browser's print dialog box, in order to print the data displayed on screen.



Data table

In some graphs there is a table with the data from which the graph has been generated. These tables can be useful for getting greater detail from each graph.

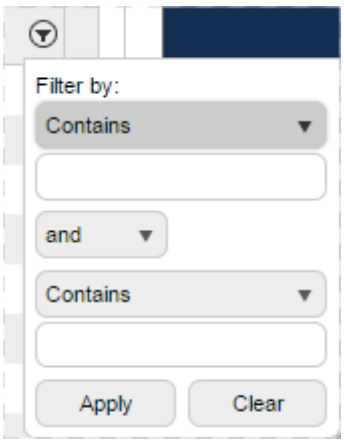
Given the amount of data displayed, there are data filter tools in these tables.

- Building filters

Filters are text-based searches in the data tables. A filter is constructed on the basis of two blocks of conditions inter-related by a logical operation.

Each filter block contains a condition (Contains or Doesn't contain) and the text field. The text field is compared against the data recorded in the Gatedefender device and, depending on the condition selected, will be included –or not- in the data displayed.

The text fields are flexible and allow parts of words to be searched for directly, without having to use wildcards.

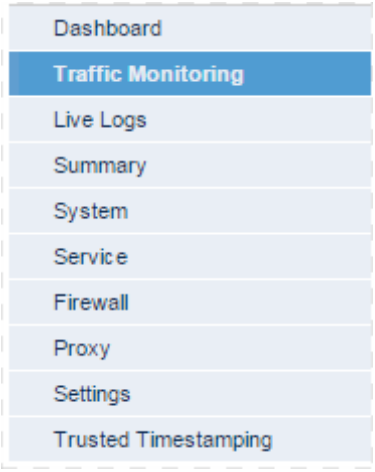


- Page layout

The bottom line includes the page layout controls, page refresh and the number of lines displayed and the total number.

2.2. Traffic Monitoring

In the Traffic Monitoring menu there are four tabs that include graphs and tables for displaying the data traffic in the Gatedefender device.



These graphs display data usage statistics generated in real time, to enable you to locate Internet access bottlenecks, users that consume most, and with which protocols and applications, etc.

2.2.1. Available modules

Below you can see the various Traffic Monitoring modules, organized in tabs:

- Dashboard: General graphs summarizing the volume and type of traffic generated on the network.
- Flows: This displays a table with real-time data on the Gatedefender device traffic flow.
- Hosts list: This displays information on the data consumption and connections for each network computer.
- Top Host (local): This displays information on the data consumption and connections for the network computers requiring most bandwidth.
- Host: By clicking the IP addresses displayed in the Traffic Monitoring diagrams or using the computer search tool described in point 2.2.2, you can obtain detailed information of the bandwidth consumption of an individual computer.
- Interfaces: This displays statistics of the use of the active interfaces on each Gatedefender device.

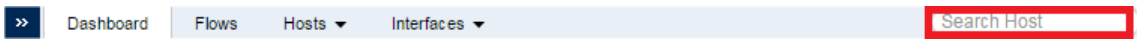
2.2.2. Common features

All tabs in the Traffic Monitoring section include the computer search feature and consumption summary.

Also, the data tables in this section can be organized in columns, clicking on the title of each one in ascending or descending order.

Computer search

By entering part of the name of the computer in the tool, a drop-down list appears with all partial matches found on the network.

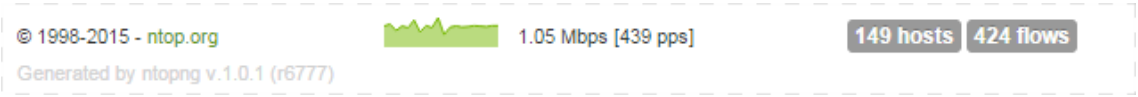


Once the computer has been selected, a new tab opens with detailed information about its activity.

See section 4.4 for more information

Consumption summary

At the bottom of the screen there is a small activity graph providing a high-level image of the volume of data received by the Gatedefender device either to or from the Internet. It also indicates the number of computers discovered since Gatedefender started operating and the number of active data flows at that moment.



3. Dashboard reports

The reports in the Dashboard section reflect the security status of network computers, although they also include information about user access to the Gatedefender device through resources such as VPN or HotSpot.

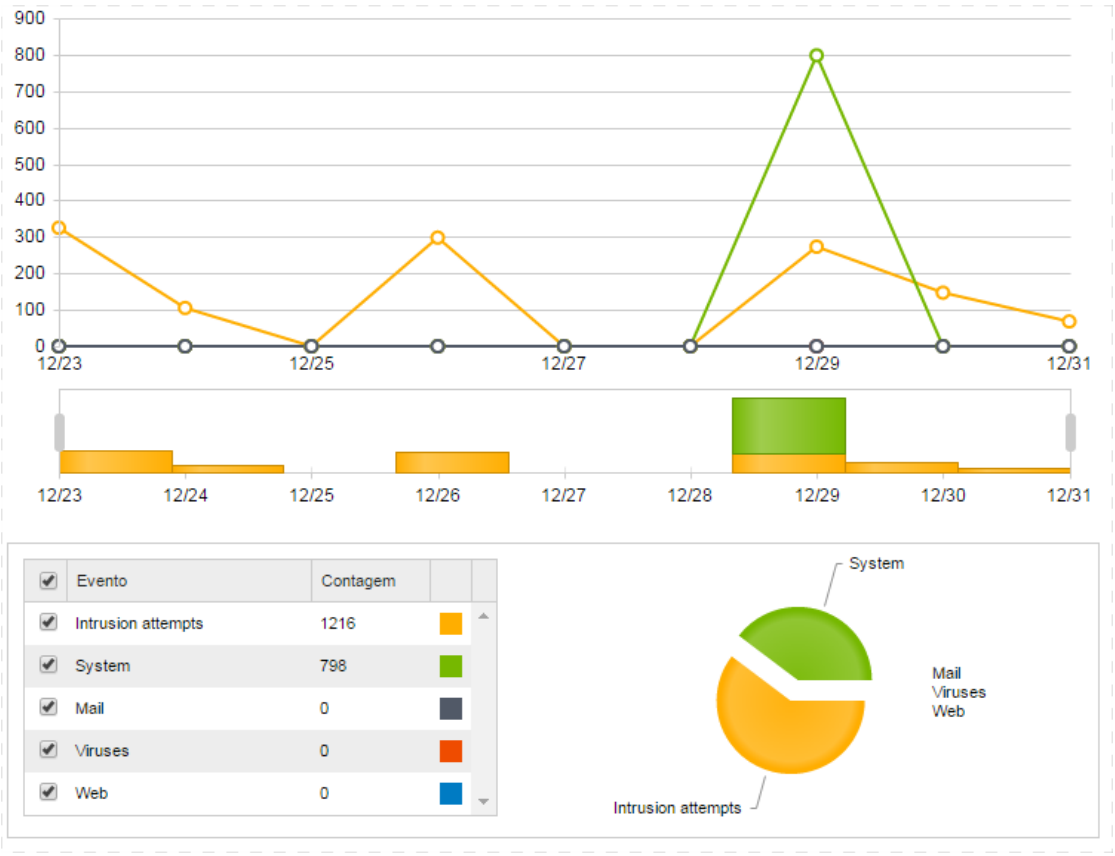
This chapter explains the significance of the graphs displayed in each of the tabs in the Dashboard menu.

3.1. Summary

The purpose of this graph is to show a summary of the Gatedefender device activity with respect to protection for the network against external threats and inbound access attempts.

The information displayed is divided into five categories, which offer more in-depth detail in independent tabs.

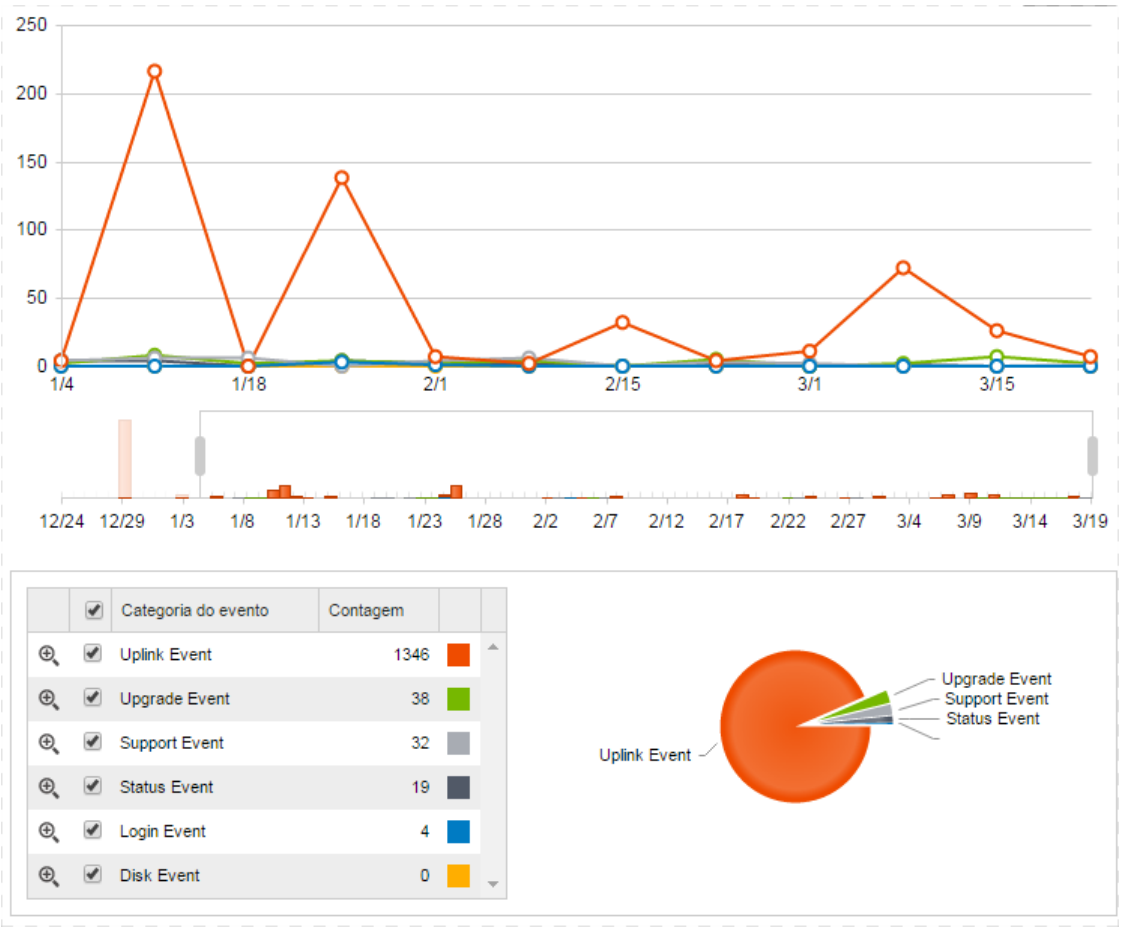
In the Summary report, each category is represented as a data series on the graph which shows a summary of all recorded activity.



By using the time filters and selecting the time period with the sliding controls, any given period can be selected to see at a glance the relevant network security activity.

3.2. System

The system line graph displays the internal activity of the Gatedefender device regarding performance and service management.

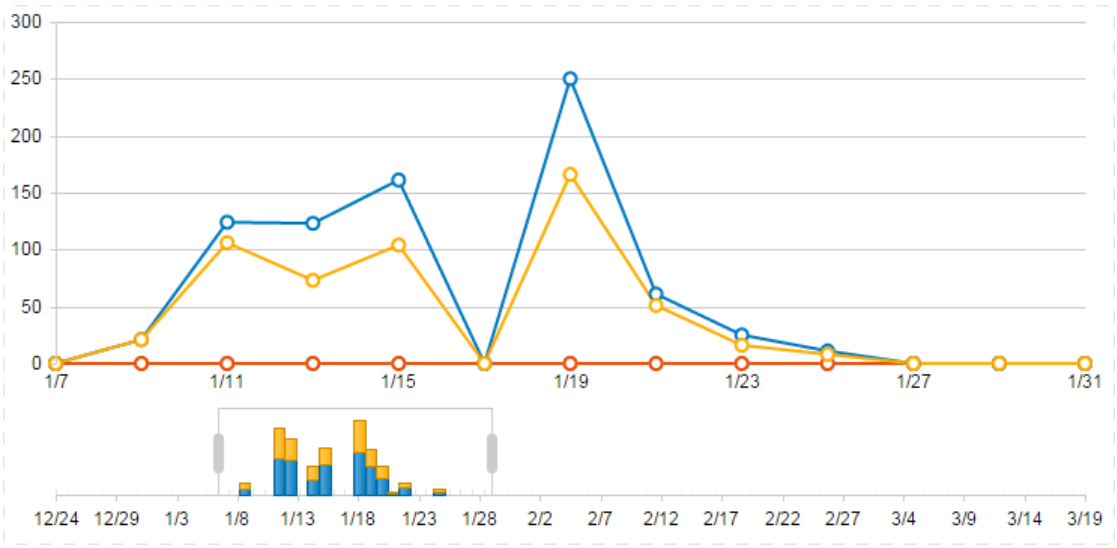


The events displayed are divided into six categories:

- Upgrade event: Events generated as a consequence of system upgrades or any of the corresponding upgrade packets.
- Disk event: Events related with the I/O activity of the internal disk on the Gatedefender device.
- Login event: Number of system logins by SSH, both successful and failed.
- Status Event: Changes to system status (startups, restarts, shutdowns).
- Support Event: Permitted or rejected access attempts to the Gatedefender device by the Support user used by the Panda Security Support department.
- Uplink event: Events associated with the outbound Internet interfaces (uplink interfaces). Possible status are: online, offline, dead, alive.

3.3. Web

This tab displays the network activity related to access to Web services, showing the number of pages accessed by users and, out of these, the number blocked by the URL filter engine.



At the bottom there are two tabs that offer this information as tables: Access report and Filter report.

3.3.1. Access report

This tab shows information about the Web traffic generated on the network and allowed by the security policies configured in the Gatedefender device.

The following three tables are included:

- Source IP address: This helps locate the network computers that require the highest volume of Web resources. The table displays the number of requests for Web services grouped by the IP address of the network computers.
- Domain: This identifies the domains most requested by users. The table displays the number of Web requests on the network, grouped by domain.
- User: This helps locate the network users that require the highest volume of Web resources. The table shows Web service requests grouped by network users.

Integration with LDAP has to be enabled in the Web filter module in order to identify network users.

For each of the tables there is a pie chart to help interpret the data.

3.3.2. Filter report

This tab displays information on the Web traffic filtered by the Gatedefender device and blocked in line with the security policies configured.

The following three tables are included:

- Blocked category: This identifies the most frequently requested categories for which access is not allowed. The table displays the number of blocked Web requests grouped

into the five first-level categories included in the Gatedefender Web filter: General use, Parental control, Productivity, Security, Uncategorized Sites

- Source IP address: This helps locate network computers that try to access Web resources that are not permitted by the organization. The table displays the number of blocked Web service requests grouped by the IP addresses of network computers.
- Domain: This identifies the domains most requested by users for which access is not allowed by the organization. The table displays the number of blocked Web service requests grouped by domain.

3.4. Mail

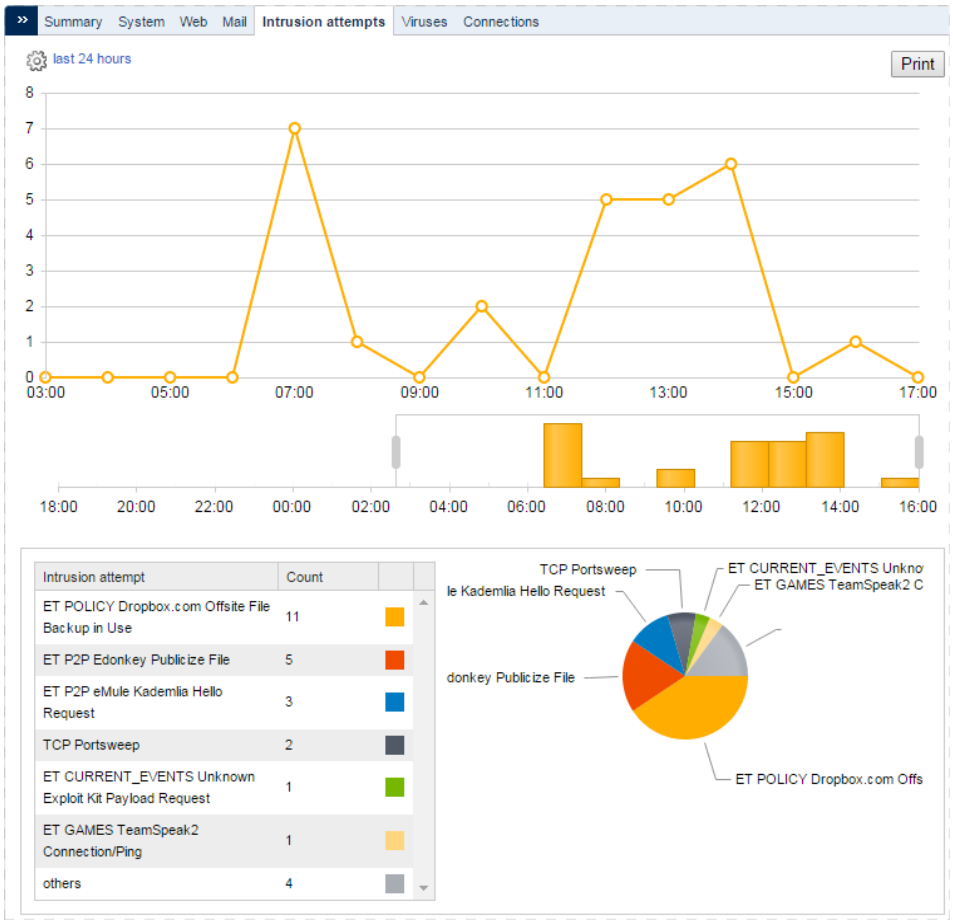
The Mail tab shows the activity of the Gatedefender spam filter.

At the bottom there are three tables that offer in-depth information:

- From: This helps locate the most frequent spammers. The table shows the number of spam messages grouped by sender.
- To: This helps identify the users that receive most spam. The table shows the number of spam messages grouped by recipient.
- Source IP address: This helps identify the mail servers used by the most frequent spammers. The table shows the number of spam messages grouped by the source IP address.

3.5. Intrusion attempts

The Intrusion Attempts tab displays all the intrusion attempts detected on the network by the IPS module.



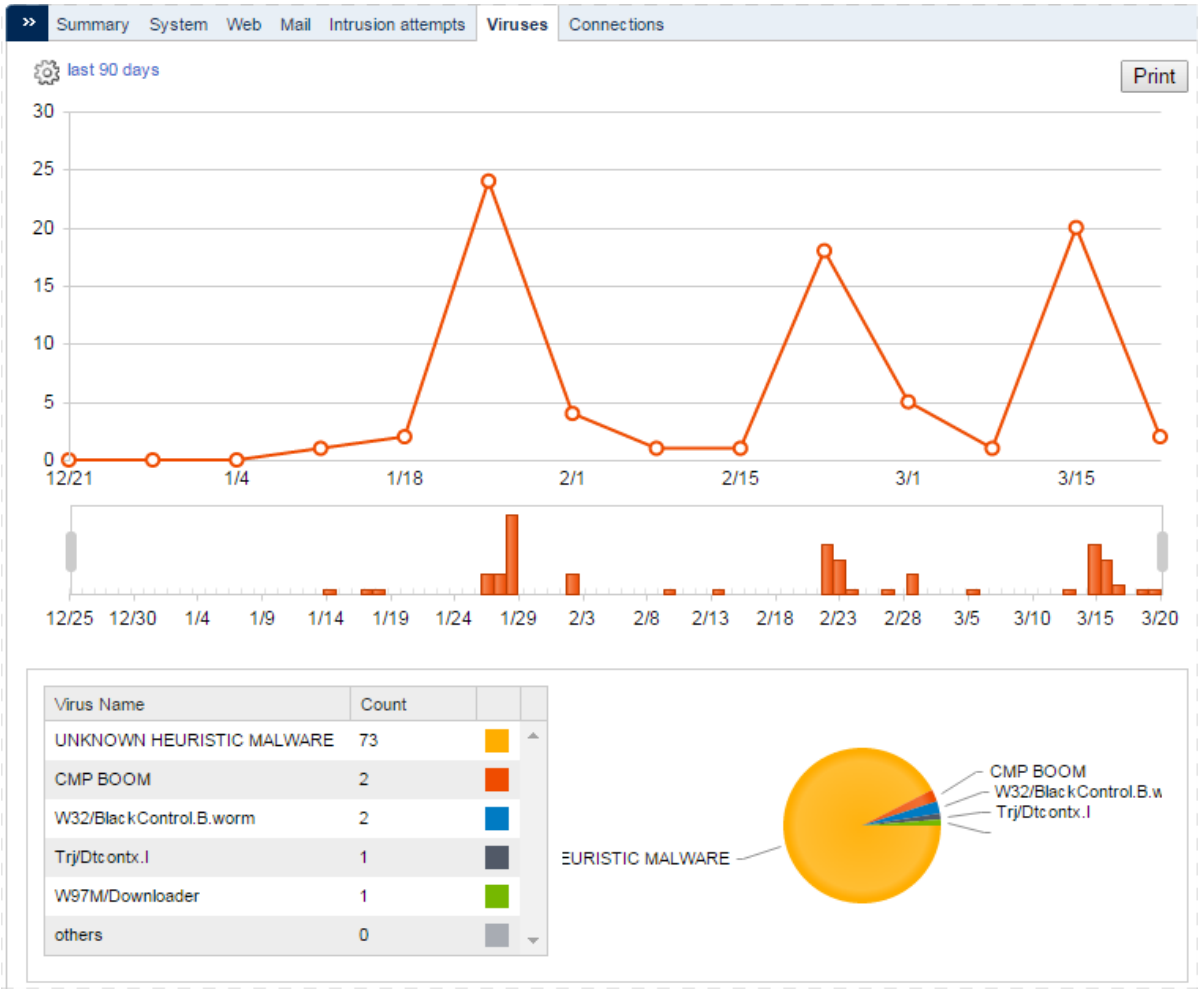
At the bottom of the screen there are three tables with more information:

- Intrusion attempts: This helps identify the attacks used by hackers. The table displays the number of intrusion attempts grouped by type/signature.
- Source IP address: This helps locate the IP addresses used by hackers to launch attacks against the network. The table displays the number of intrusion attempts grouped by the attacker's IP address.
- Target IP address: This helps locate the most frequently attacked computers on the network. The table displays the number of intrusion attempts grouped by the target IP address.

For each of the tables there is a pie chart to help interpret the data.

3.6. Viruses

The Viruses tab shows all the malware intercepted by the antivirus engine in the Gatedefender device, highlighting the source and the target.



At the bottom of the screen there are three tables with more information:

- Virus Name: This helps identify the malware that most frequently affects the network. The table displays the number of viruses detected, grouped according to the name of the malware.
- Source IP address: This helps identify the source of malware targeting the network. The table displays the number of viruses detected grouped according to the IP addresses of the computers from which they were sent.
- Target IP address: This helps identify the network computers that receive most malware. The table displays the number of viruses detected grouped according to the IP addresses of the computers to which they were sent.

3.7. Connections

The Connections tab displays the activity of users' computers and the Gatedefender device with respect to VPN or HotSpot connections.

The diagram includes four series representing the following information:

- Local Connections: Average number of computers connected to the Gatedefender device. This series displays as a graph the Gatedefender ARP tables in relation to the MAC addresses discovered on the customer's LAN.
- IPSec users: Average number of users connected to remote networks via IPSec.
- Hotspot users: Average number of users connected to the network via Hotspot.
- OpenVPN users: Average number of users connected to remote networks via VPN.

4. Data Traffic Monitoring

The Traffic Monitoring menu presents a set of reports that help accurately identify network bottlenecks with respect to Internet access.

All the graphs displayed in this section are calculated in real time.

4.1. Dashboard

The Dashboard tab contains several diagrams that display, in real time, the Gatedefender traffic flow.

4.1.1. Top Flow Talkers

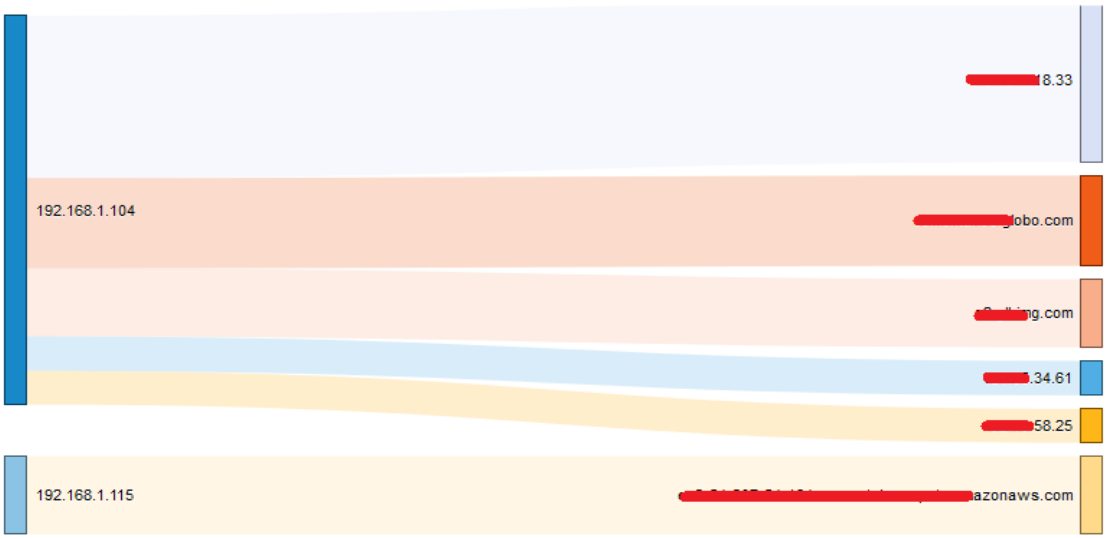
The Top flow Talkers is a Sankey diagram that uses horizontal bars to illustrate the system pairs exchanging data at any moment.

The left side of the diagram represents network computers, and on the right are the servers or external computers with which some kind of data exchange has been established.

By double-clicking a computer in the Sankey diagram you can see details of the activity and consumption of the specific computer. Refer to point 4.4 for more information.

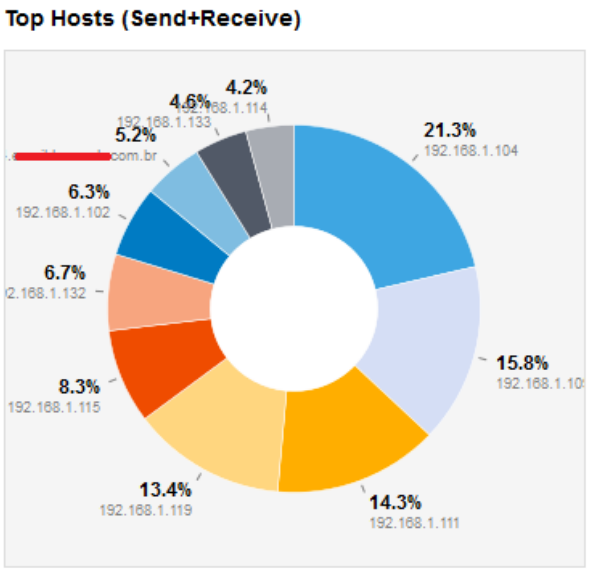
The size of each bar reflects the data flow consumption of a specific computer as a percentage of the total consumption of all data flow connections established by all network computers.

As you can see in the diagram, one computer can have simultaneous connections with several remote systems. For example, a local computer with a data transfer established with five different remote systems will be represented with five bars, each with a width proportional to the consumption of that system.



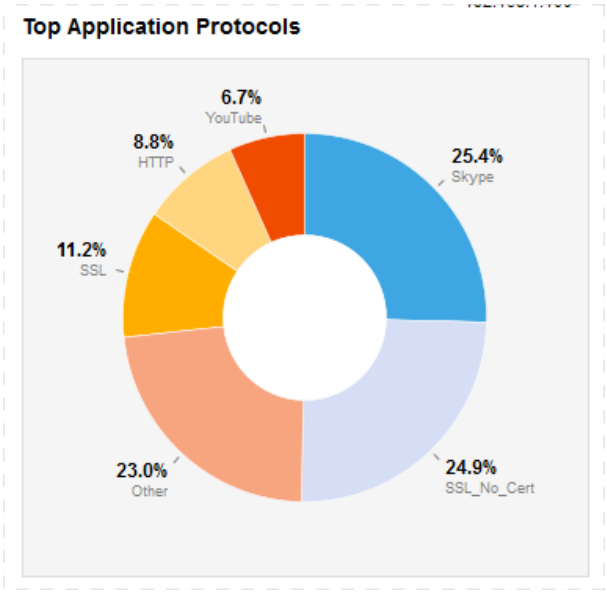
4.1.2. Top Hosts (Send+Receive)

This diagram lets you locate the computers that consume most Internet resources.
This is a pie chart that represents the bandwidth consumed by network computers.



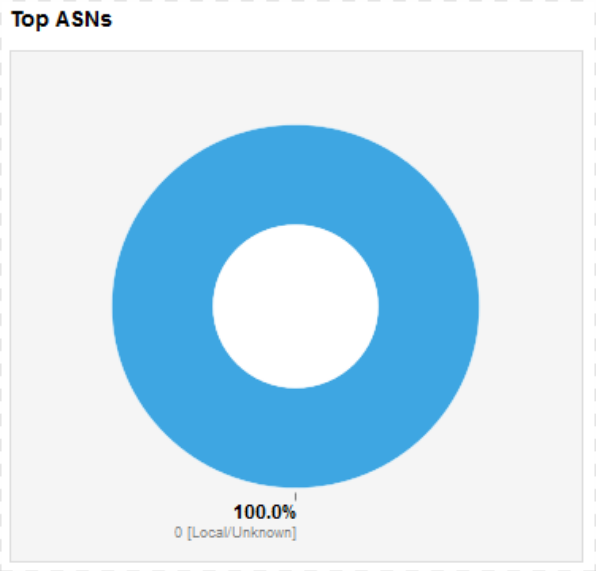
4.1.3. Top Application Protocols

This diagram lets you locate the applications that consume most Internet bandwidth.
This is a pie chart that represents the percentage of bandwidth consumed by applications.



4.1.4. Top ASN

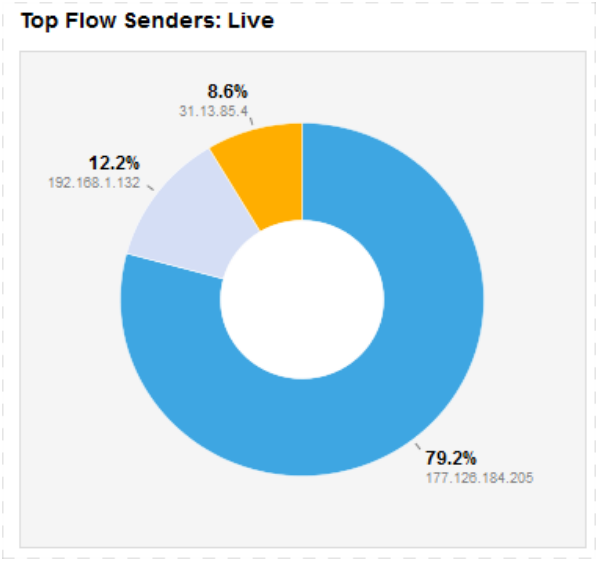
This diagram lets you locate the Internet networks that exchange most traffic with the local network. Each IP address on the Internet represents a network managed by a single administrative entity, and the ASN (Autonomous System Number) identifies this network.



4.1.5. Top Flow Senders: Live

This is a pie chart that represents the percentage of bandwidth consumed by the transmission of data across the customer's network.

On networks with asymmetric inbound and outbound lines, it is possible that the performance of the download line is affected by computers rapidly sending data externally, saturating the outbound line. Because of the nature of the Internet protocols used, the download performance depends largely on the free outbound bandwidth, so it is necessary to know at all times which computers are over-using these network resources.



4.2. Flows

The Flows table lets you view all the data exchanges at any given moment between computers on the internal network and external connections. The table can be ordered (ascending/descending) in columns by clicking the title.

The fields are explained below:

- Info: Clicking the Info icon displays more detailed information about the specific flow.
- Application: The name of the application exchanging data within the flow. There may be a certain delay before the correct application is displayed. In this case, the message 'Too early' appears instead of the application name.
- L4 Proto: Transport protocol used by the flow, which is usually TCP or UDP.
- Client: Name of the client side computer and port used by the flow. By clicking the computer or port name, more information about network traffic on this computer or port is displayed.
- Server: Name of the server side computer and port used by the flow. Similarly, more information can be displayed by clicking on the name of the computer or port.
- Duration: Duration of the flow.
- Breakdown: Percentage of traffic generated by the client and by the server.
- Throughput: Amount of data actually exchanged between the client (on the left, in black) and the server (on the right, in green).
- Total bytes: Total amount of data exchanged since the connection was established.

Only ten lines are displayed in the table, so at the bottom a page layout system has been added to enable the user to browse through all connections.

Clicking the Info icon displays detailed information about the specific flow. Below you will find a description of the contents of the Info table.

- Client: Name of the client side computer and port used by the flow.
- Server: Name of the server side computer and port used by the flow.
- Application Protocol: Name of the application exchanging data within the flow.
- First Seen: Time the connection was established, along with the time that has passed since then.
- Last Seen: Time the connection was last active, along with the time that has passed since then.
- Total Traffic Volume: Total traffic transferred in the flow.
- Client vs Server Traffic Breakdown: Percentage of traffic generated by the client and by the server.
- Client to Server Traffic: Number of packets and bytes sent from the client to the server.
- Server to Client Traffic: Number of packets and bytes sent from the server to the client.
- Actual Throughput: Consumed bandwidth, measured in megabits per second.
- TCP Flags: Active bits reflecting the TCP status of the current flow.

4.3. Hosts List

This tab displays information about the computers exchanging data with the Gatedefender device. Below you will find the fields included in the table.

- IP Address: IP or MAC address of the computer. The latter is displayed if the DHCP assignment for the computer has expired.
- Location: Specifies whether the computer belongs to a local or remote network.
- Symbolic Name: Name of the computer.
- Seen Since: Time the first connection was established.
- ASN: Autonomous System Number of the network to which the computer's IP address belongs.
- Breakdown: Diagram of the percentage of traffic sent and received.
- Throughput: Speed with which the computer sends and receives data.

4.4. Host

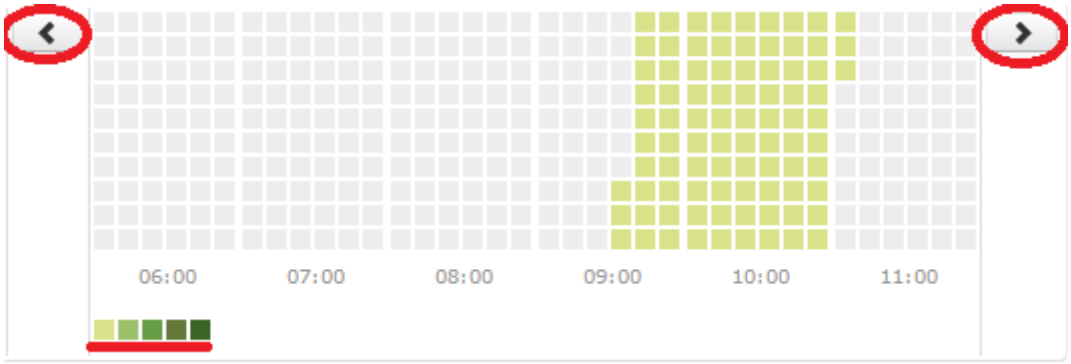
In the Traffic Monitoring section, clicking any IP address in the graphs or tables will open a new tab with more detailed information about the computer across eight tabs.

4.4.1. Overview

This gives a general description of the selected computer.

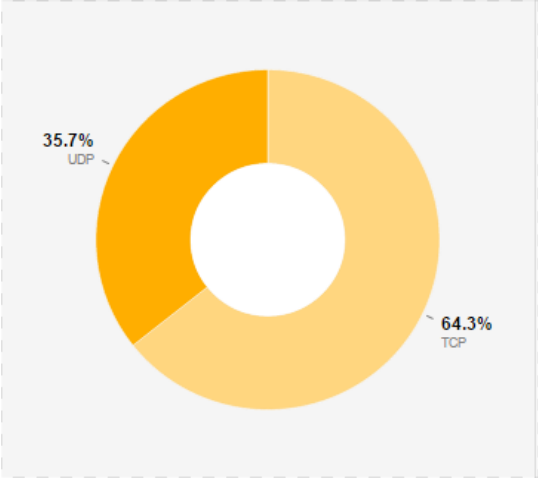
- (Router) Mac Address: MAC address of the computer. If there are no routing devices between the computer and Gatedefender, the MAC address of the computer is displayed. If there are routers, the MAC address of the router directly accessible to Gatedefender is shown.
- IP Address: IP or MAC address of the computer. The latter is displayed if the DHCP assignment for the computer has expired.
- Name: Name of the computer if available. In addition, the Local tag is indicated if the computer is on the customer's LAN and the Private IP tag appears if the computer has an address from a private range.
- First Seen: Time the connection was first established.
- Last Seen: Time the connection was last active, along with the time that has passed since then.
- Sent vs Received Traffic Breakdown: Traffic generated or received by the computer.
- Traffic Sent: Number of packets and bytes sent from the client to the server.
- Traffic Received: Number of packets and bytes sent from the client to the server.

- JSON: Information about the computer in JSON format.
- Activity Map: This illustrates the number of flows from/to a computer over a certain period of time. Each square represents one minute. The darker the color, the more flows have occurred in this minute in line with the key at the bottom. To the right and left are buttons for adjusting the time period.



4.4.2. Traffic

This tab shows a breakdown of the level 4 protocol traffic (TCP / UDP). It includes the Protocol Overview pie chart showing the percentage of UDP and TCP data handled by the computer.

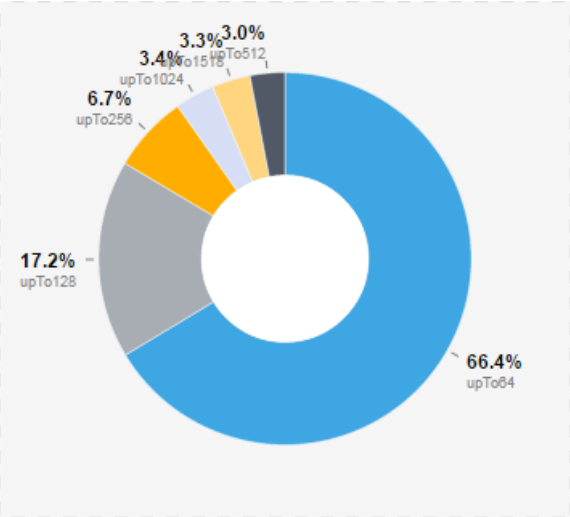


The same information is presented in the form of a table with the following fields:

- Protocol: TCP or UDP.
- Sent: Data sent by the computer.
- Received: Data received by the computer.
- Breakdown: Diagram of the percentage of traffic sent and received.
- Total: Total volume of data sent and received by the computer in Kbytes and as a percentage of the total of the two protocols.

4.4.3. Packet

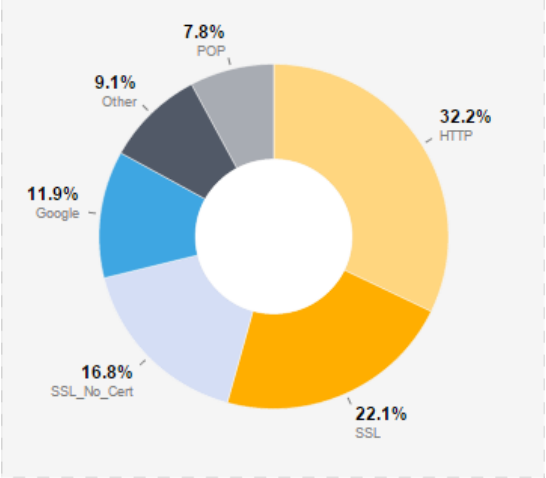
This pie chart breaks down the Gatedefender packets according to size.



4.4.4. Protocols

This tab helps identify the applications run on users' computers which use the most bandwidth.

The pie chart shows the distribution of application layer protocols used by network users.



The content of the pie chart is also displayed through a table listing all the protocols discovered along with other complementary data. The fields are as follows:

- Application protocol: Application layer protocol.
- Sent: Data sent by the computer using the selected protocol.
- Received: Data received by the computer using the selected protocol.
- Breakdown: Diagram of the percentage of consumption by the selected protocol.

- Total: Total volume of data sent and received by the computer (measured in bytes and as a percentage of the total for all protocols).

4.4.5. Flows

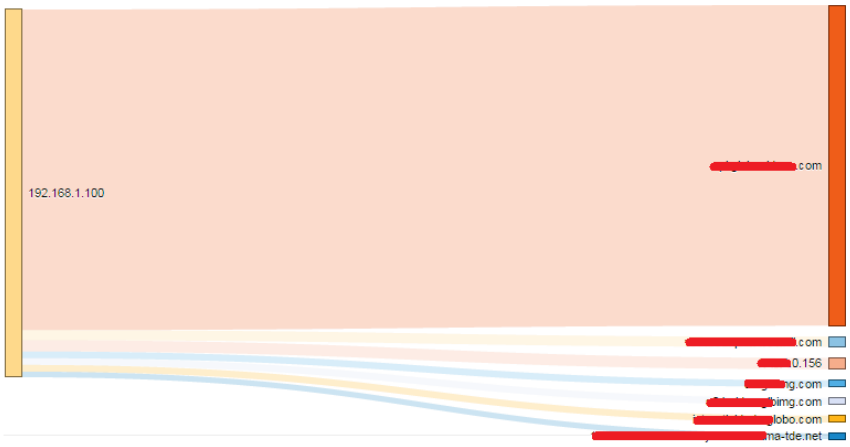
This shows as a table the data flows in real time established by users' computers. For each flow there is a line in the table with the following information:

- Info: Click to see the Flows tab (see point 4.2).
- Application: Application layer protocol of the data flow.
- L4 Proto: Transport layer protocol used by the data flow.
- Client: Name of the client side computer and the port used by the flow.
- Server: Name of the server side computer and the port used by the flow.
- Duration: Duration of the connection.
- Breakdown: Amount of data actually exchanged between the client (on the left, in black) and the server (on the right, in blue).
- Throughput: Speed with which the computer sends and receives data.
- Total Bytes: Total amount of data exchanged since the connection was established.

4.4.6. Talkers

This tab has a Sankey diagram similar to that mentioned in point 4.1.1, but only referring to the selected computer.

The diagram represents the data flow established by the selected computer, with bars of colors, along with the bandwidth for each pair. The bandwidth displayed is proportional to the amount of data exchanged.

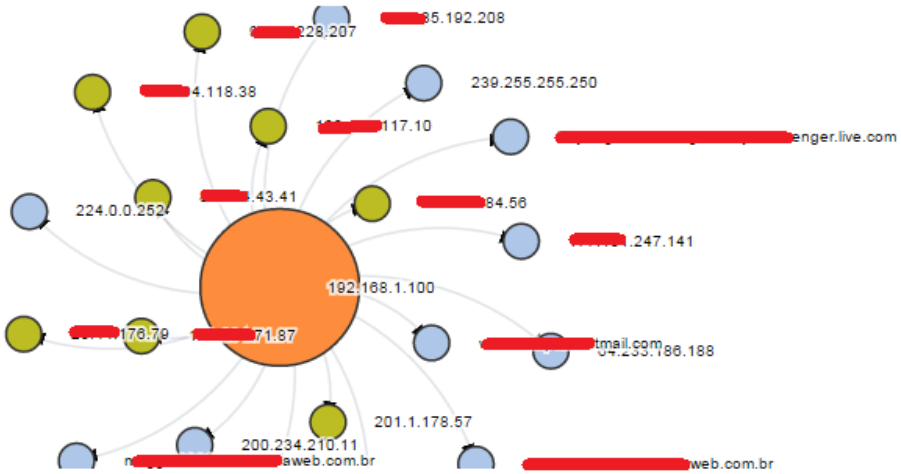


4.4.7. Contacts

This tab details all the computers that have initiated or received a connection with the selected computer.

This information is represented by means of an interactive graph with three color codes:

- Orange: For the selected computer
- Blue: Identifies local computers
- Green: For remote computers



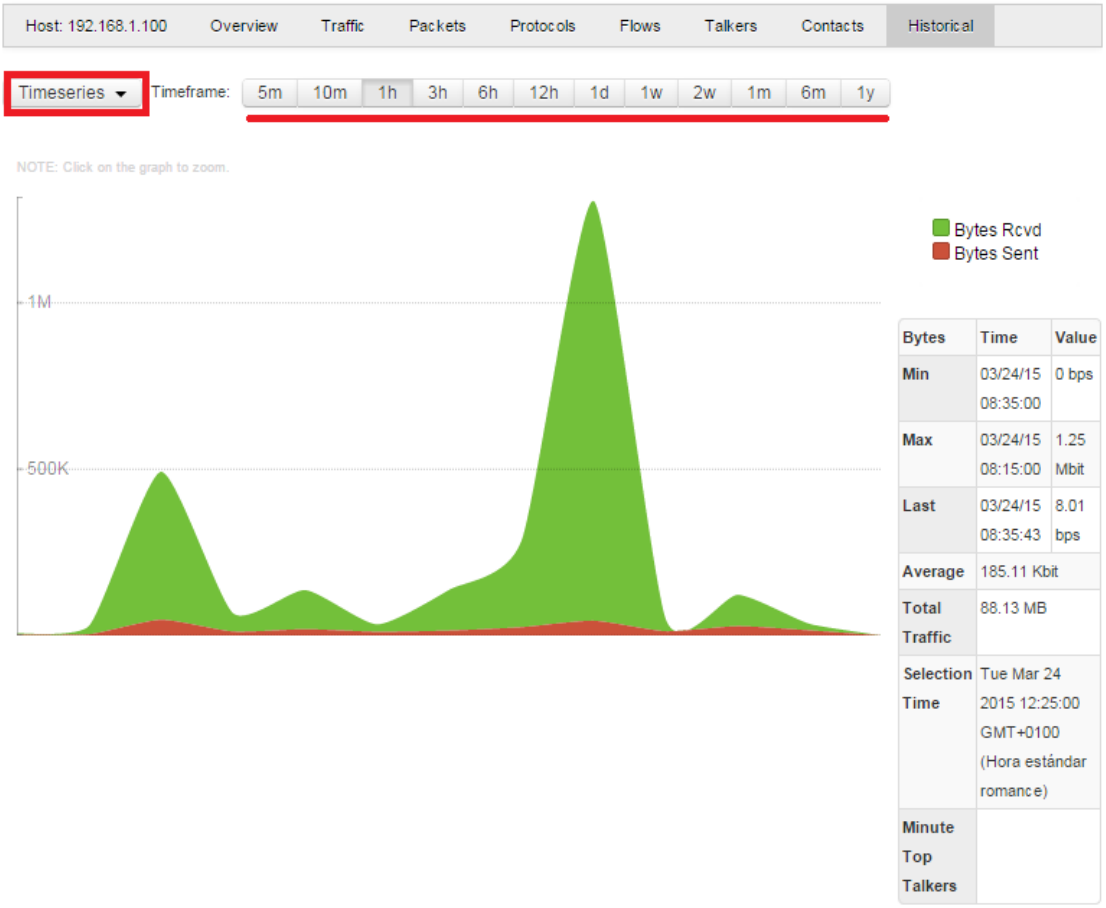
There is also a table divided into two areas:

- Client Contacts (Initiator): List of the remote computers that initiated a communication with the selected computer. Below is the information displayed for each contacted client:
  - Server Address: IP address or FQDN
  - Contacts: Number of established connections
- Client Address (Receiver): List of the remote computers that received communication from the selected computer. Below is the information displayed for each contacted client:
  - Client Address: IP address or FQDN
  - Contacts: Number of established connections

4.4.8. Historical

This tab has an interactive diagram with the history of the data flow from and to the computer over a given period. The y axis represents the volume of data and the x axis the time period.

The default period selected is one hour, and all protocols are displayed together divided into two series: traffic sent (green) and traffic received (red).



Below you can see the controls available to filter traffic and get more information.

- Timeseries: This allows you to expand a list of application layer protocols to filter the graph by the protocol you choose.
- Timeframe: This lets you adjust the time period (from five minutes to one year).
- Zoom: By clicking any part of the graph you can zoom in on the point, changing the current Timeframe to the previous period. If, say, the select period was one day, by clicking the graph you can zoom in on the selected area to a timeframe of ten minutes.
- Node information: By moving the mouse pointer over the graph you can see the values for the *y* ordinate (data sent or received, depending on the selected data series).

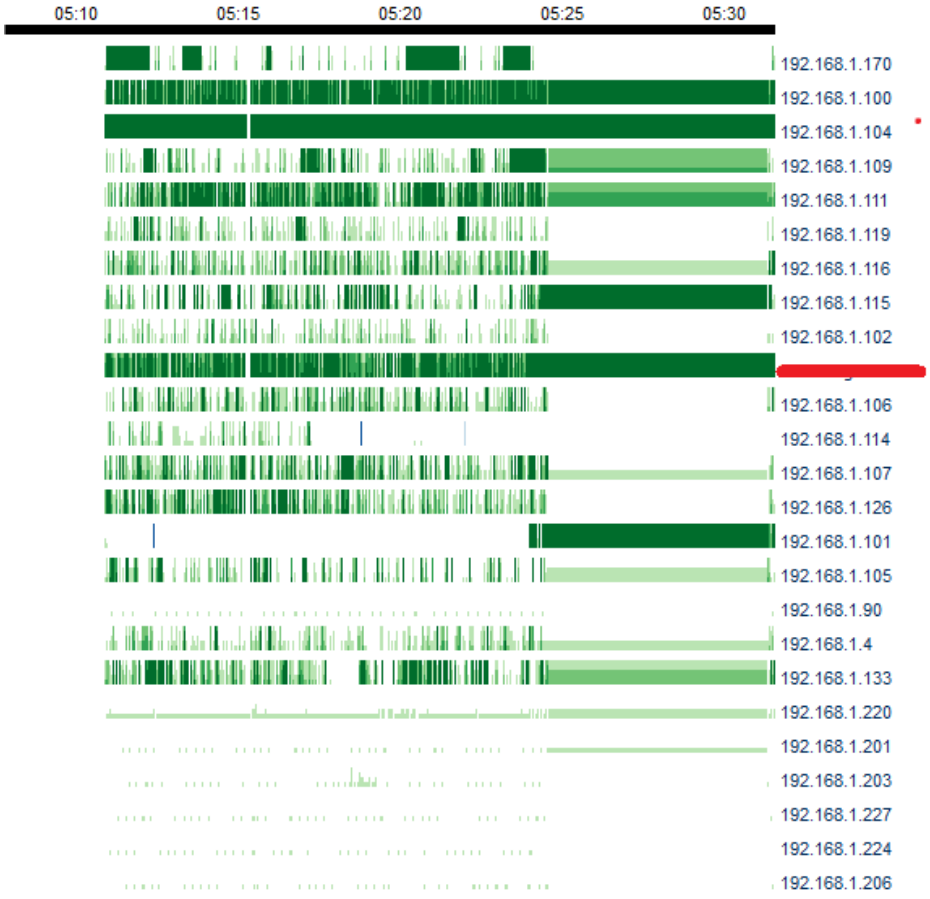
There is also a table with statistical information about the data exchanged and other useful information:

- Min: Exact time within the selected period when least data was exchanged, and the amount.
- Max: Exact time within the selected period when most data was exchanged, and the amount.

- Last: Exact time within the selected period when data was last transferred and the amount.
- Average: Average data transferred during the selected period.
- Total Traffic: Total amount of traffic transferred during the selected period.
- Selection Time: Time period displayed in the graph.
- Minute Top Talkers: Minute with the greatest number of pairs exchanging information.

4.5. Top hosts

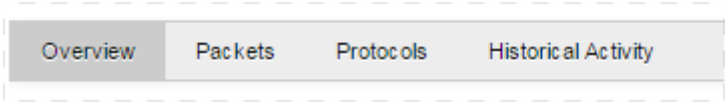
This shows a real-time diagram of the network computers with active connections. The graph shows the last 30 minutes.



4.6. Interfaces

The Interfaces tab shows the traffic on each independently configured network area.

Clicking the Interfaces menu displays a drop-down list of active interfaces. Selecting one of them reveals four tabs.



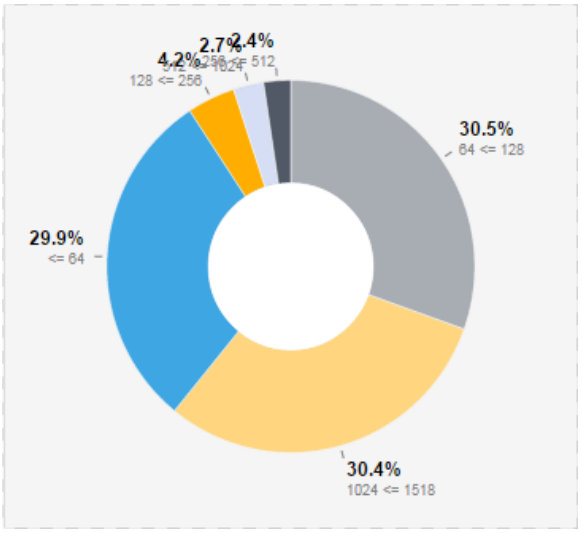
4.6.1. Overview

This offers a table with general information about the interface:

- Name: Name of the logical bridge interface assigned by the operating system.
- Bytes: Traffic on the selected interface. The traffic count displayed includes the 24 bytes of the headers of each Ethernet frame sent or received. These headers are not included in the calculations of the data traffic between the pairs displayed in other sections of this guide, as they are calculated at network level.
- Received Packets: Number of packets/frames received.
- Dropped Packets: Number of packets rejected because of corrupt format, bottlenecks, network driver failure, network hardware failure, etc. and the percentage of failures with respect to the volume of successfully handled packets.

4.6.2. Packets

This tab displays packets handled by the interface distributed according to size. There is a pie chart to illustrate this.



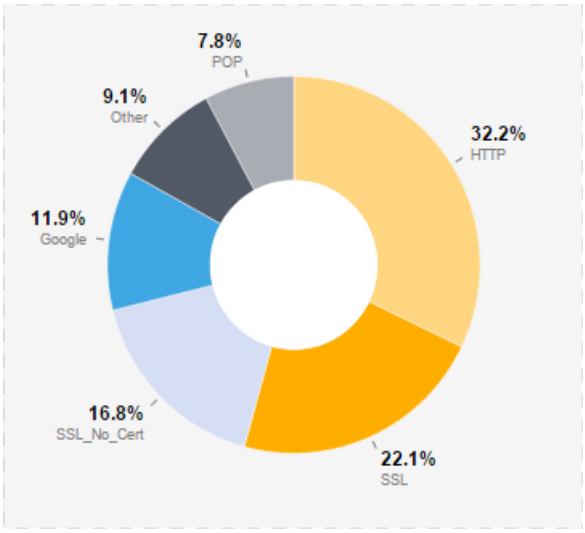
On Ethernet 802-3-2012 networks the maximum frame size is 1518 bits, and the intervals displayed in the graph are:

- x < 64
- 64 < x > 128
- 128 < x > 256
- 256 < x > 512
- 512 < x > 1024
- 1024 < x > 1518

With other network topologies, such as Gigabit Ethernet, maximum frame sizes can be much larger, such as jumbo frames. In this case the intervals and maximum and minimum sizes may vary.

4.6.3. Protocols

This tab displays the distribution of application layer protocols managed by the selected Gatedefender interface. There is a pie chart with most frequently used protocols and the corresponding percentages.



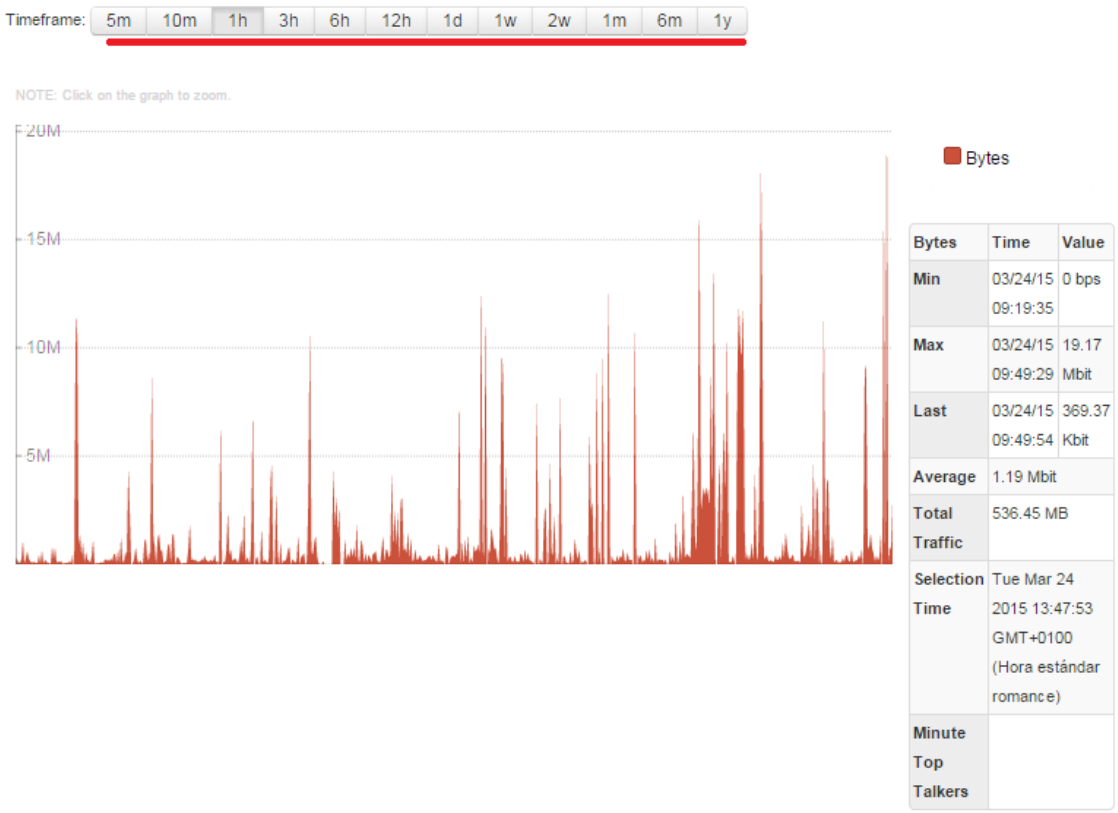
There is also a table with more detailed information:

- Application Protocol: Application layer protocol.
- Total: Total volume of data transferred via the selected interface since the Gatedefender device was started.
- Percentage: Data transferred by the selected interface, displayed in a graph as a percentage of the total amount of data transferred.

4.6.4. Historical Activity

This tab includes an interactive graph showing the history of the data flow of the selected interface in a given time period. The *y* axis represents the volume of data and the *x* axis the selected time period.

The default period is one hour.



Below you can see the traffic filters available and further information about them:

- Timeframe: This lets you choose the time period (from five minutes to one year).
- Zoom: By clicking any part of the graph you can zoom in on the point, changing the current Timeframe to the previous period. If, say, the selected period was one day, by clicking the graph you can zoom in on the selected area to a timeframe of ten minutes.
- Node information: By moving the mouse pointer over the graph you can see the values for the Y ordinate (data handled by the interface).

There is also a table with statistical information about the data handled and other useful information:

- Min: Exact time within the selected period when least data was exchanged, and the amount.
- Max: Exact time within the selected period when most data was exchanged, and the amount.
- Last: Exact time within the selected period when data was last handled and the amount.
- Average: Average data transferred during the selected period.
- Total Traffic: Total amount of traffic transferred during the selected period.
- Selection Time: Time period displayed in the graph.
- Minute Top Talkers: Minute with the greatest number of pairs exchanging information


Gatedefender