streamcore

STREAMVIEW GUIDE

Table des matières

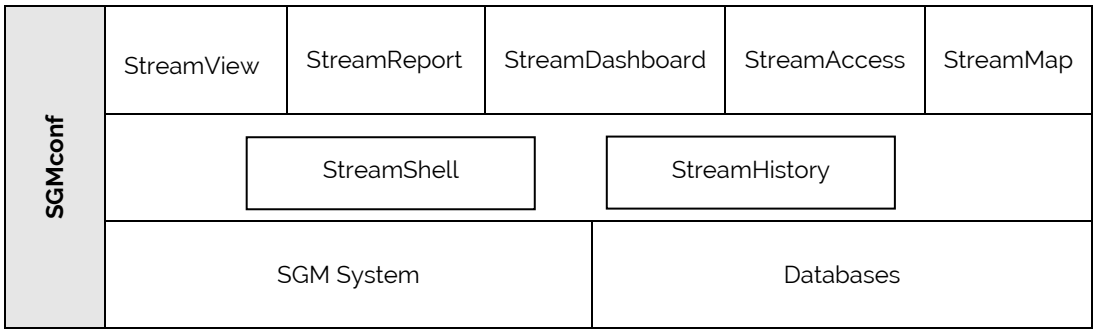
1 Introduction

1.1 STREAMGROOMER MANAGER (SGM)

StreamGroomer Manager (SGM) is a specific hardware platform, which hosts the following software applications:

- SGMconf: SGM management application
- SGM System: SGM operating system
- Databases: coherent sets of data associated with one or several StreamGroomers
- StreamShell: command mode (cli) on which all the applications are interfaced
- StreamHistory: access module to long-term data and graph generation
- StreamView: configuration and supervision application in graphic mode
- StreamReport: application for editing PDF reports
- StreamDashboard: application for managing personalized Web dashboards
- StreamAccess: application for managing flexible access rights to the Web applications
- StreamMap: application for alarms and performance summary display in a geographic map

This software suite can be represented as follows:



The SGM "Databases" groups' parameters and statistics associated with one or more StreamGroomers into a coherent whole. Management of these databases (i.e., creation, deletion, back up, and restoration) is handled through the SGMconf application.

A database is used through the middleware (StreamShell, StreamHistory) by the applications (StreamView, StreamReport, StreamDashboard, StreamAccess and StreamMap) in order to configure and manage all Streamcore solution features.

2 Launching StreamView

2.1 LOGGING INTO THE DATABASE

After launching a browser, a database can be logged into via the following methods:

1. Direct Access: http://<@IP-SGM>/streamview/<database_name>/

   <@IP-SGM>: the SGM IP address (the name assigned by DNS can also be used)

   <database_name>: database name, as defined when it was created with the SGMconf application

   Access via the Welcome Screen: `http://<@IP-SGM>/`

   <@IP-SGM>: the SGM IP address (the name assigned by DNS can also be used).

   The SGM welcome page then presents links for launching various applications. To access a database click a displayed database name.

Note: To provide a secure connection between a browser and an SGM replace "http" with "https".

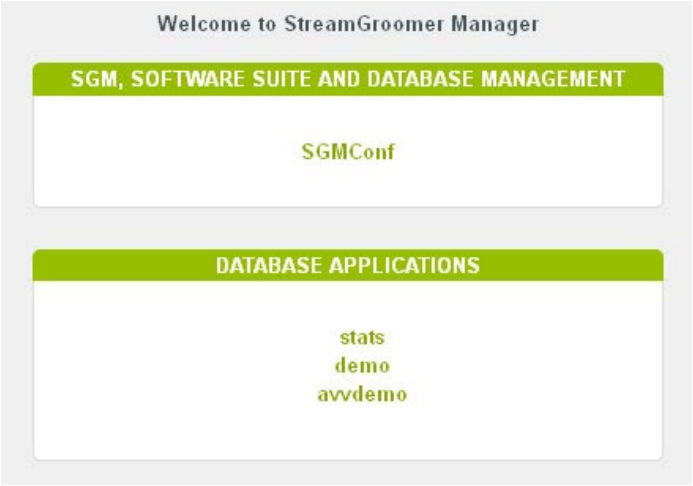


Figure 1 – Access via the SGM welcome screen

2. From the welcome screen, enter your user name and password. If you have created a new database and accessing it for the first time, use the user name **global** and no password.

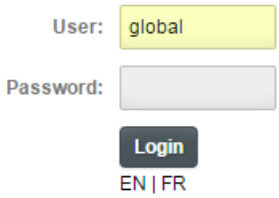


Figure 2 – First time login to newly created database

Note: The default language for all Streamcore applications can be set via the SGMconf application.

2.2 UNDERSTANDING THE INTERFACE

The diagram below outlines the various sections displayed in StreamView.

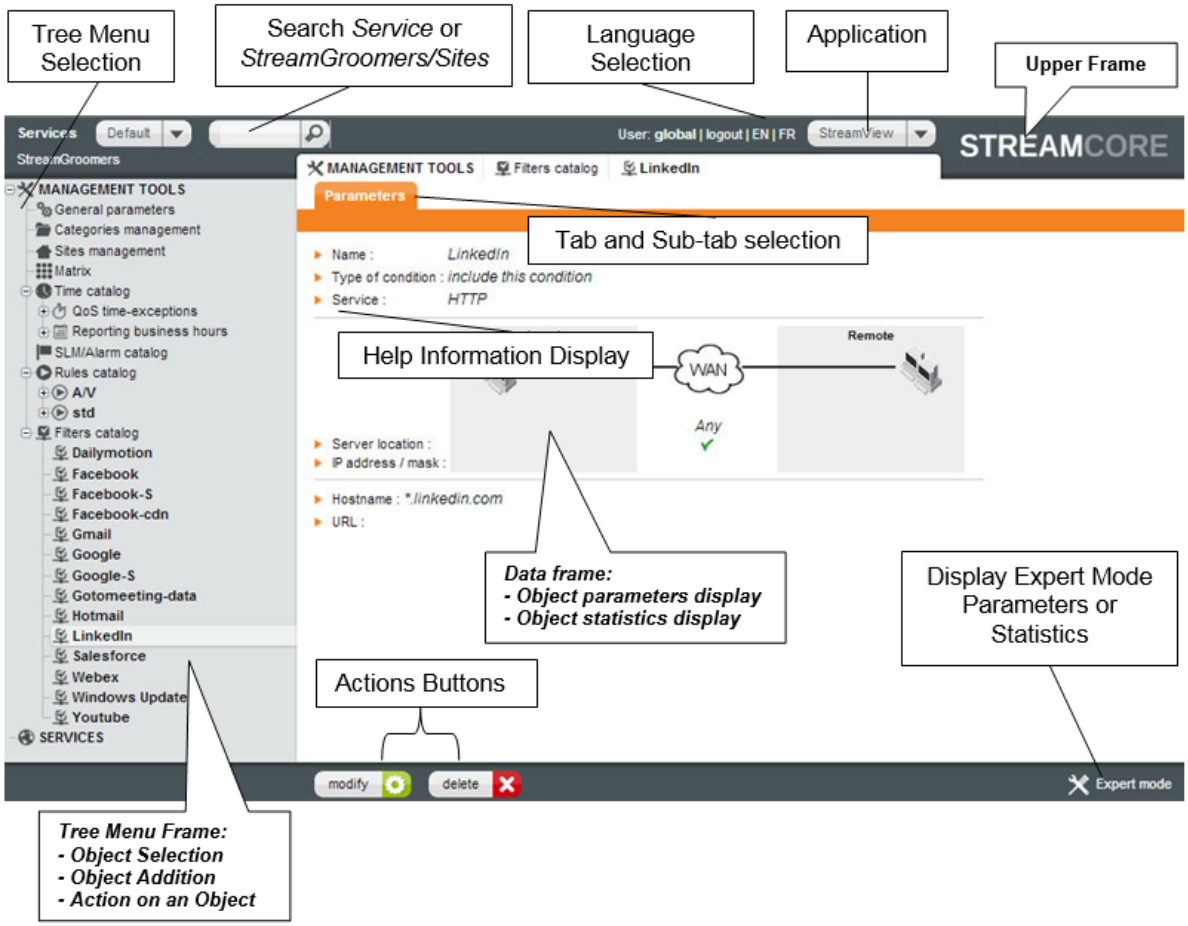


Figure 3 – StreamView frames at a glance

In the "Upper Frame", the "Application" menu gives you direct access to various Streamcore applications including StreamView.

The "Data frame" enables the configuration and display of database objects.

To navigate in StreamView use the "Tree Menu Frame" located on the left-side of the screen. There are two tree menus which are associated with:

- **Services**: categories, sites and rules management the Unified Mapping Tree (UMT).
- **StreamGroomers**: used for StreamGroomer management.

3 Configuration Methodology

With Streamcore solutions, administration is done on a site-to-site basis and not by equipment.

Service management is performed via the Unified Mapping Tree (UMT) and uses the same approach for:

- A site with a single StreamGroomer
- A site with dual / tandem StreamGroomers (high availability architectures)
- A site without a StreamGroomer

The configuration and deployment steps are:

1. **StreamGroomer Configuration**

   Define your StreamGroomer operational and boot parameters.

2. **Unified Mapping Tree (UMT) Configuration**

   Define all characteristics that relate to your organization along with what sites need to be managed by the Streamcore solution:

- Categories matching entities such as Business Units or Geographical locations
- Per site characteristics:
  - Categories to which the site belongs
  - Access link characteristics
  - Subnets characteristics

  Definition of characteristics related to "Rules tree" per site:

- Access links management
- Site-to-site traffic management:
  - Shaping rules (for remote sites without StreamGroomer)
  - Grooming rules (for sites with StreamGroomer)
  - WAN Optimization (for sites with WAN Optimized StreamGroomers)
- VoIP/Video and application traffic classification

3. **Services Configuration**

   Once the UMT has been defined, it provides a unified access to a set of visibility, performance control and optimization services. Many of these services are ready-to-use, but some of them require some additional provisioning:

- Visibility services configuration
  - Real-time/Long-term Stats
  - Alarms
  - Troubleshooting tools
- Performance control services configuration (traffic shaping/QoS)
  - Network congestion control
  - QoS policies
- Optimization services configuration
  - Compression and WAN load balancing
  - Web caching

4 StreamGroomer Management

4.1 INTRODUCTION

This chapter describes how to provision and manage your StreamGroomers. All the following operations are performed after having selected the "StreamGroomers" tree menu.

Figure 4 – Select StreamGroomers from the top-left in the interface

4.1.1 Single StreamGroomer Deployment

In most cases a single StreamGroomer is deployed between a LAN and a WAN router. A single StreamGroomer has a dedicated administration port and can have either 2 or 4 LAN/WAN traffic management ports. The required information per StreamGroomer is:

- Management IP address and default gateway
- Ethernet ports speed/duplex mode

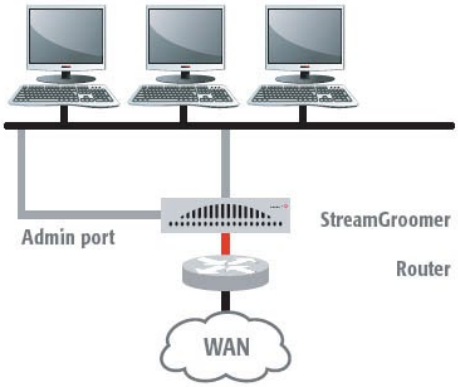


Figure 5 – Single StreamGroomer

4.1.2 Dual/Tandem Deployment of StreamGroomers

In case high availability is required, two types of paired StreamGroomers are available:

- Dual StreamGroomers
- Tandem StreamGroomers

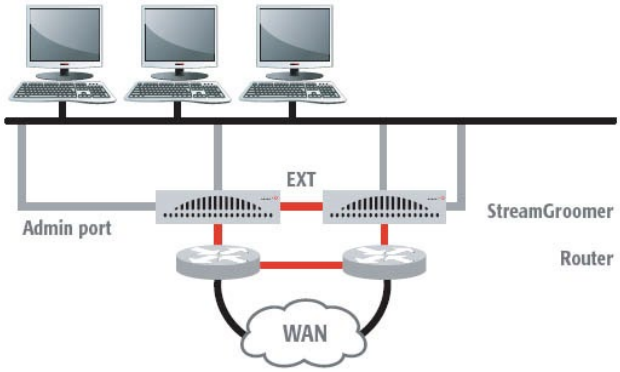


Figure 6 – Dual/Tandem Deployment

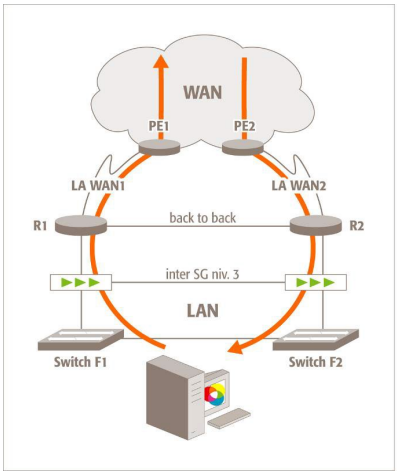
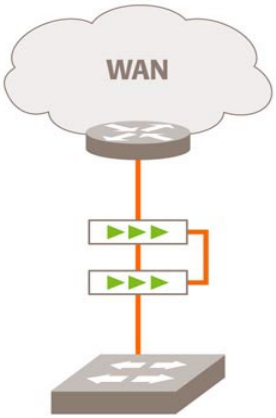
Dual/tandem StreamGroomers require three management IP addresses in the same subnet:

- Master IP address
- Slave IP address
- Shared IP address (statistics), used by the active StreamGroomer

The SGM uses the following addresses depending on the performed operation:

	SERVICES Configuration	SERVICES Monitoring / Reporting	STREAMGROOMERS Configuration	STREAMGROOMERS Monitoring / Reporting
Master IP address	X		X	X (port, maintenance)
Slave IP address			X	X (port, maintenance)
Shared IP address		X		X (IP router, stats polling)

The following diagrams show the deployment differences between a set of Dual and Tandem StreamGroomers:

DUAL STREAMGROOMERS	TANDEM STREAMGROOMERS
Advantage: • Real-time processing of asymmetrical traffic • High availability traffic management 	Advantage: • High availability traffic management 

Note: Tandem StreamGroomers can have 2 or 4 LAN/WAN traffic management ports.

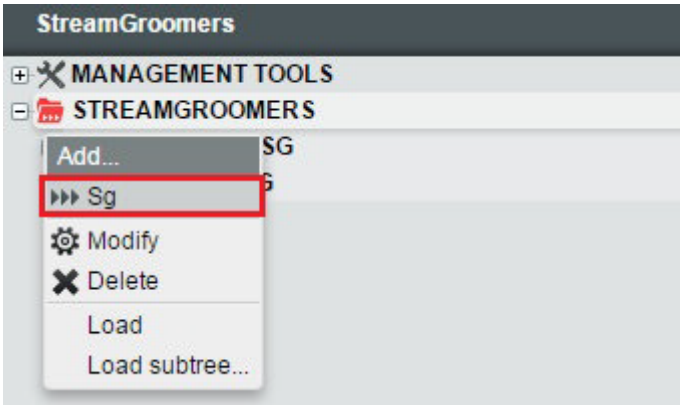
Note: A transparent migration from Single StreamGroomer to Dual/Tandem StreamGroomers (and vice-versa) is possible. See the insertion mode parameter in 4.2.3.

4.2 STREAMGROOMER PROVISIONING

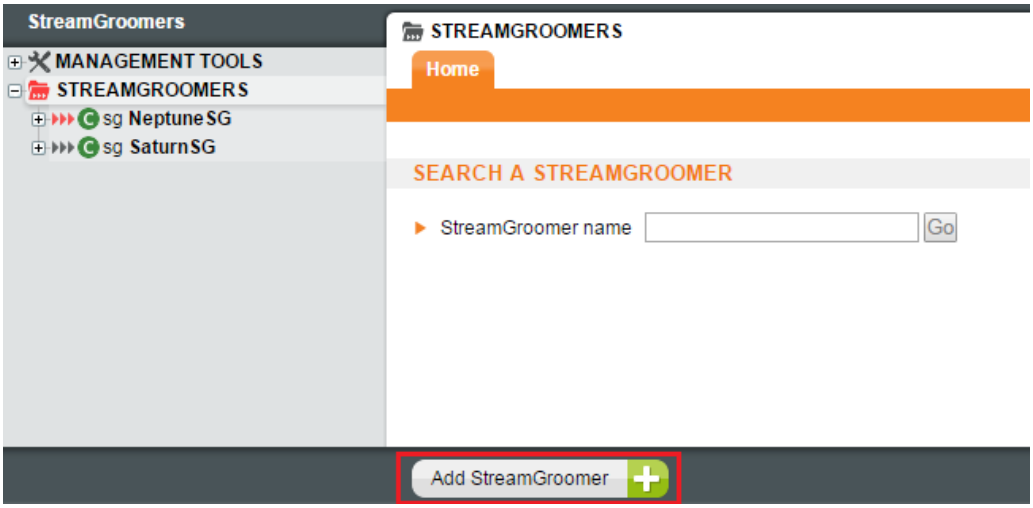
1 ADDING A NEW STREAMGROOMER

To add a new StreamGroomer:

1. Right-click on **STREAMGROOMERS** in the tree menu then select **Add...Sg**.

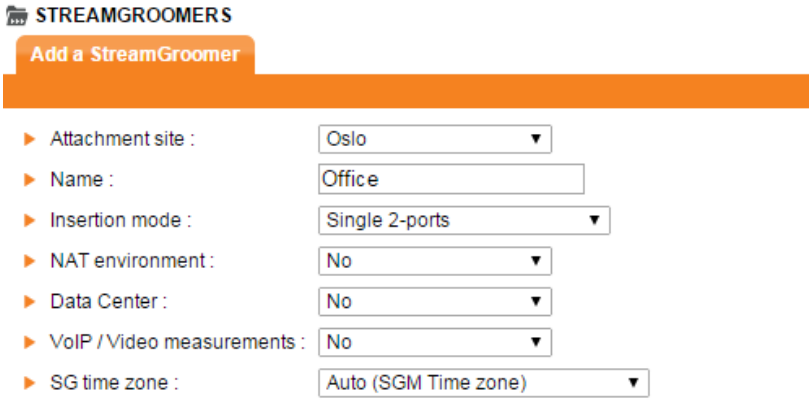


Alternatively click on **STREAMGROOMERS** in the tree menu then click the **Add StreamGroomer** button.



Note: You must always add a site before adding a StreamGroomer.

2. Next, enter the required parameters then click the **Next** button.

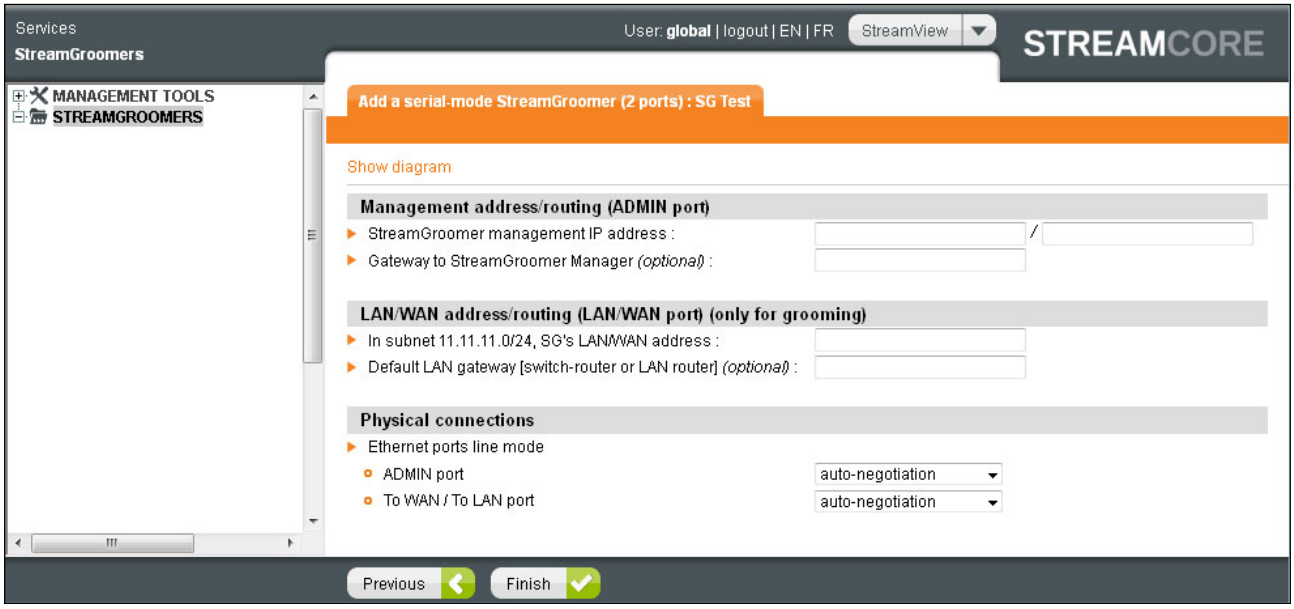


Parameter	Description / Values
Attachment site	Select the site where the StreamGroomer will be created (see 6.3 for configuring sites).
Name	StreamGroomer name
Insertion mode	Select one of the following choices: **Single 2-ports (default):** a single StreamGroomer is deployed inline with 2 LAN/WAN ports connected on a single LAN segment. **Single 4-ports:** a single StreamGroomer is deployed inline with 4 LAN/WAN ports connected on two LAN segments. **Dual (2 SG):** two StreamGroomers are deployed inline in front of two separate WAN access routers, and are interconnected together through the EXT port to interact. **Tandem 2-ports:** two StreamGroomers are deployed inline with 2 LAN/WAN ports connected on a single LAN segment, and are interconnected together through the EXT port to interact. **Tandem 4-ports:** two StreamGroomers are deployed inline with 4 LAN/WAN ports connected on two LAN segments, and are interconnected together through the EXT port to interact.
NAT environment	The default value is set to "No". This must be set to "Yes" if the SG administration address is seen by the SGM as NATed. Public IP addresses will be provisioned in addition to the private IP addresses.

Data Center	The default value is set to "No". This must be set to "Yes" if the site is a Data Center. (see 6.3.2 for more information)
VoIP/Video measurements	The default value is set to "No". The "VoIP/Video measurements" parameter is available per site with a SG, see 6.3.
SG time zone	The default parameter is set to **Auto – SGM timezone**. This parameter is used by time-based QoS policies.

Note: If the site was managed by shaping rules from another StreamGroomer, then the shaping rules will be automatically transformed into grooming rules (statistics will be preserved).

3. Next enter the StreamGroomer network information:
    a. For a **Single 2-ports** and **Single 4-ports** insertion mode



Parameter	Description / Values
Management address/routing (ADMIN port)	
StreamGroomer management IP address	This refers to the StreamGroomer administration IP address. The mask can be entered in the following form: 24 or 255.255.255.0
Gateway to SGM (Optional)	Enter the gateway address used to reach the SGM. This parameter is required only if the SGM is located on a different subnet than the StreamGroomer.
LAN/WAN address/routing (LAN/WAN port) only for **Grooming** and **WAN Optimization**	
In subnet x.x.x.x, SG's LAN/WAN address	LAN/WAN IP address of the StreamGroomer. Required if Grooming network rules are configured. Required for WAN Optimization. The mask can be entered in the following form: 24 or 255.255.255.0
Default LAN gateway	LAN gateway. Required if Grooming network rules are configured, as well as tunnel mode. Required for WAN Optimization.
Physical connections	
ADMIN port	The default is set to **auto-negotiation**. StreamGroomer Ethernet ports can adapt to half-duplex and full-duplex modes as well as to speeds of 10 Mbps, 100 Mbps and 1 Gbps.
To WAN / To LAN port	

	Configuration recommendations: if the opposing device is in auto-negotiation or half-duplex 10 Mbps mode, use auto-negotiation, otherwise, force the same mode as that of the opposing device.

Note: If the WAN access type of the site is set to redundant active/active, the management of the access links can be defined as aggregated or independent when adding the StreamGroomer. See chapter 7.3 for more information on managing 2 WAN access links in active/active mode.

b. For a **Dual, Tandem 2-ports, Tandem 4-ports** insertion mode

Parameter	Description / Values
Terminology	
Master suffix	Suffix added to the name of the SG.
Slave suffix	
Management address/routing (ADMIN port)	
Shared IP address (statistics)	Shared IP address between the StreamGroomers used by the SGM to poll statistics. See chapter 4.1.2. The mask can be entered in the following form: 24 or 255.255.255.0
Master IP address	IP address of the Master StreamGroomer (Administration).
Slave IP address	IP address of the Slave StreamGroomer (Administration).
Gateway to SGM	Address of the gateway used to reach the SGM. This parameter is required only if the SGM is located on a different subnet than the StreamGroomer.
LAN/WAN address/routing (LAN/WAN port) only for **Grooming** and **WAN Optimization**	
In subnet x.x.x.x, SG's LAN/WAN address	LAN/WAN IP address of the StreamGroomer. Required if Grooming network rules are configured. Required for WAN Optimization is being used. The mask can be entered in the following form: 24 or 255.255.255.0
Default LAN gateway	LAN gateway. Required if Grooming network rules are configured, as well as tunnel mode. Required for WAN Optimization.
InterSG address/routing (EXT port)	
Master InterSG IP address	IP addresses used by the dual StreamGroomers to exchange packets in the InterSG link. Any IP addresses can be chosen, whether the Master and Slave StreamGroomers EXT ports are connected directly or via a VLAN trunk.
Slave InterSG IP address	
Physical connections	
ADMIN port	The StreamGroomers Ethernet ports can adapt to half-duplex and full-duplex modes as well as to speeds of 10 Mbps, 100 Mbps and 1 Gbps. Configuration recommendations: if the opposing device is in auto-negotiation or half-duplex 10 Mbps mode, use auto-negotiation, otherwise, force the same mode as that of the opposing device.
To WAN / To LAN port	
EXT port	

Note: If the WAN access type of the site is set to redundant active/active, the management of the access links can be defined as aggregated or independent when adding the StreamGroomer. See chapter 7.3 for more information.

4. Click **Finish**.

4.2.1 Deleting a StreamGroomer

To delete a StreamGroomer:

1. In the **StreamGroomers** branch, click on **STREAMGROOMERS>xx** and right-click and select **Delete** from the menu. Validate the confirmation message.

Note: If Grooming rules were defined on the StreamGroomer, then they will be transformed automatically into shaping rules on the remote StreamGroomer (statistics will be preserved).

4.2.2 StreamGroomer Operational Modes and Parameters

There are 2 ways to modify a StreamGroomer's parameters:

1. Click on **STREAMGROOMERS>xx** from the tree menu. Then from the bottom of the page click the **Modify** button. Select the operational mode you require from the combo box and any additional parameters. Click the **Submit** button to finish.
2. Click on **STREAMGROOMERS>xx** in the tree menu. Right-click the SG and then select "Modify" from the sub-menu.

Parameter	Description / Values
Name	StreamGroomer name.
Operational mode	**Bypass (default):** Traffic management is inactive. The mechanical bypass is closed, and therefore the LAN and WAN ports are deactivated. However, the management ADMIN port remains active. **Monitoring:** Traffic management is passive. Only the Monitoring & Reporting features are available. **Monitoring+Control:** Traffic management is active. The following features are made available with this mode: Monitoring & Reporting UCP engine / Advanced QoS Compression / Web caching / WAN Load balancing **Monitoring+Tagging+Control:** Traffic management is active. The following features are made available with mode: Monitoring & Reporting UCP engine / Advanced QoS Compression / Web caching / WAN Load balancing Streamcore QoS management WAN Optimization is also activated
SGM-SG dialog type	**RSH – Not secured (default):** the SGM uses the RSH protocol to communicate with the StreamGroomer. **SSH – Secured with weak authentication:** the SGM uses the SSH protocol to communicate with the StreamGroomer (with certificates exchange over the network). **SSH – Secured with strong authentication:** the SGM uses the SSH protocol to communicate with the StreamGroomer (with certificates exchange through USB key). See chapter 15 (Annex A) for more information to use SSH instead of RSH.
SG time zone	The default parameter is set to **Auto – SGM timezone**. This parameter is used by time-based QoS policies.

To configure additional parameters select **Expert Mode** located at the bottom of the page.

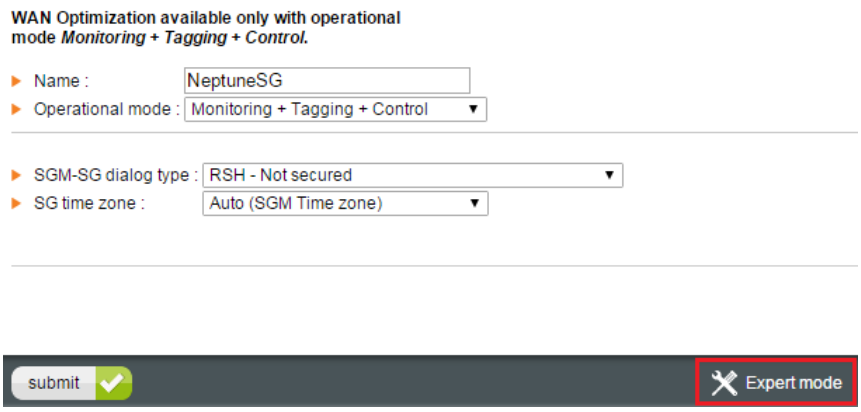


Figure 7 – Selecting expert mode provides additional configurable parameters

Parameter	Description / Values
Insertion mode	The insertion mode displayed is one chosen by you at setup. This option lets you change the StreamGroomer insertion mode, the options are as follows: Single (2 ports) Single (4 ports) Dual Tandem (2 ports) and Tandem (4 ports)
Secured administration port	The default value is set to 22. This option allows you to change the port used by SSH communications between the SGM and the SG.
Statistics polling by the SGM	The default parameter is set to "Yes". This option lets you enable or disable statistics polling by the SGM.
Automated reinit sending	The default parameter is set to "Yes". This options lets you enable or disable the automated sending of parameter modifications by the SGM. **Note:** If you set this option to "No", then you will have to reboot the StreamGroomer for it to take into account any parameter modifications.
Status mirroring between LAN and WAN ports	The default parameter is set to "Yes". This option lets you enable or disable the automatic mirroring of the LAN port state to the WAN port (up/down), and vice-versa.
Bypass state when SG down (Dual / Tandem SG only)	The default parameter is set to "Closed". This parameter can only be set to "Open" by experts from Streamcore professional services.
Switch WAN side (Dual / Tandem SG only)	The default parameter is set to "No". This parameter must be set to "Yes" for Dual StreamGroomers in case there is a switching layer on the WAN side of the StreamGroomers.
HTTP DPI tracking	Up to 2 additional ports (in addition to 80 and 8080) can be defined.
Activate WAN Optimization Expert tab	**Important:** If you active this tab, **do not modify** any parameters in the "Configuration" menu without Customer Service acknowledgment. Activating this tab enables you to view the "Reports" menu. This menu includes information concerning live traffic, accelerated clients, bandwidth savings and more. 
Global cache size	Use this setting to control your WAN optimization cache size.
HTTP specific tracking ports	Up to 3 additional ports (in addition to 80) can be defined.
HTTPS specific tracking ports	Up to 2 additional ports (in addition to 443) can be defined.

2 STREAMGROOMER IN MULTI-GIGABIT MODE

Multi-Gigabit traffic relates to traffic rates that are above 1-Gbps (Gigabit/second). The SG3200e series can operate on serial traffic rates up to 6-Gbps.

If the SG operational mode is set to "**Monitoring + Tagging + Control**" and the traffic throughput is under 1-Gbps, the SG can perform traffic control. However, if the traffic throughput goes over 1-Gbps, the SG processing capacity would not be enough to process a high number of packets.

Note: Multi-Gigabit Mode is available from Streamcore v6.2 and above only.

3 SUPPORTED FEATURES IN MULTI-GIGABIT MODE

The following table indicates the features available when Multi-Gigabit mode is activated on StreamGroomer.

Supported Features in v6.2	Standard Mode	Multi-Gigabit Mode	Comment
SG Tandem deployment mode **(2 x Single mode, inline in the same LAN segment)**	Yes	No	
SG Single mode deployment	Yes	Yes	Only for 3200e series
SG Dual deployment mode **(2 x Single mode, back to back)**	Yes	No	
SG 4 port deployment	Yes	Yes	
Monitoring + Tagging + Control	Yes	Yes	Control is possible when traffic is less than 1 Gbps.
Grooming (compression, web caching, load balancing)	Yes	No	
Monitoring + Tagging	Yes	Yes	
Monitoring	Yes	Yes	
Local Traffic Management (Fast Bridging)	No	Yes	
LAN/WAN port status mirroring	Yes	Yes	When the status of the LAN interface is down, the SG sets automatically the status of the associated WAN interface to down, and vice-versa.

4 LOCAL TRAFFIC MANAGEMENT (FAST BRIDGING) IN MULTI-GIGABIT MODE

Local Traffic Management is optimized when using Multi-Gigabit mode; QoS is applied for LAN/WAN traffic only, and not for packets exchanged between hosts belonging to LAN or VLAN segments behind the switch, therefore making traffic management highly efficient.

By checking the source and destination IP address the StreamGroomer is able to identify which packets are locally exchanged. Therefore, when traffic is acknowledged as local, packets read on the VLAN interface are automatically re-directed to the LAN interface.

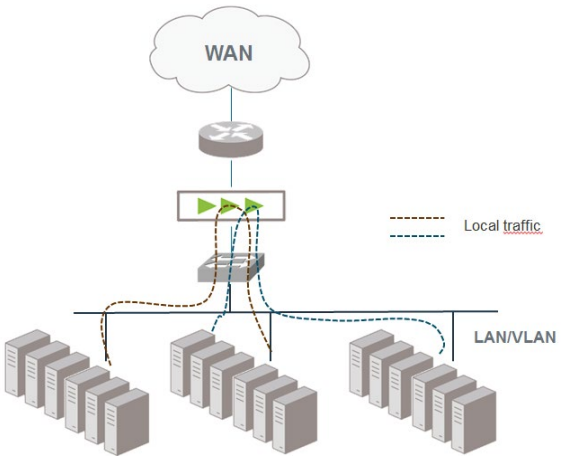


Figure 8 – Local Traffic Management

4.2.3 StreamGroomer Tree Menu (Ports, Routing, System Parameters)

5 STREAMGROOMER TREE

To modify any object in the StreamGroomer tree menu:

- First, select an object from the StreamGroomer tree menu in order to display the Parameters tab.
- Either right-click on the object and select "Modify" from the menu or click "Modify" from the bar at the bottom of the page.
- Enter all necessary updates and then click the "Submit" button.

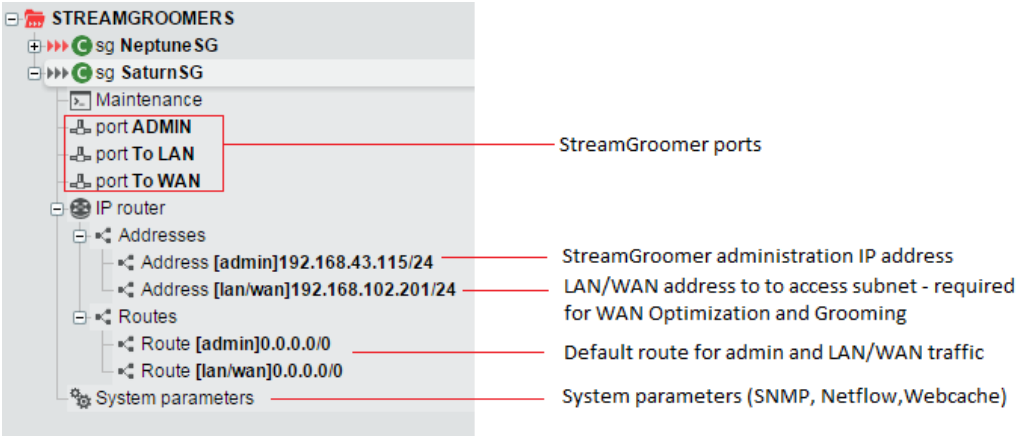


Figure 9 – StreamGroomer Tree Menu

6 PORTS

The Line mode (speed and duplex mode) can be updated directly from the StreamGroomer tree menu.

- Right click on the port (to ADMIN, LAN or WAN) object then select **Modify**.
- Then use the combo box to select line mode you require.
- Finally click the **Submit** button to verify your modification.

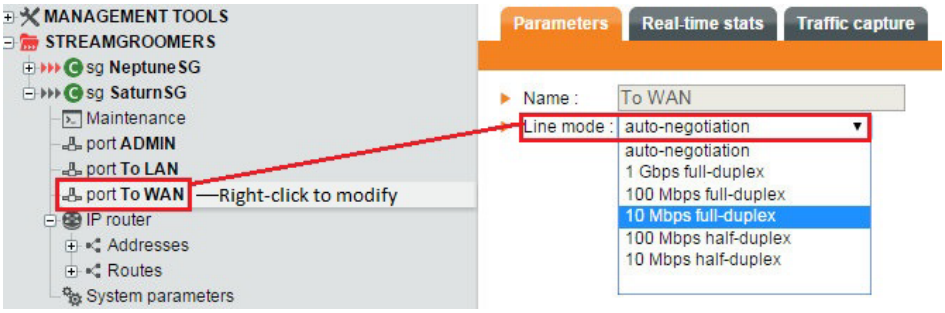


Figure 10 – Line mode modification

Note: For Dual/Tandem StreamGroomers, the "Port EXT" object also provides access to InterSG IP addresses.

7 ROUTING (ADMINISTRATION TRAFFIC)

A StreamGroomer has two fully independent routing instances:

- StreamGroomer administration traffic (ADMIN port)
- LAN/WAN traffic exchanged through grooming rules or through WAN Optimization (LAN/WAN ports). See chapter 12.1.2 on grooming rules for more information.

The IP addresses and default route for administration traffic can be updated directly from the StreamGroomer tree menu.

- Right click on the **Route [admin]** object then select **Modify**.
- Modify the route parameters you require.
- Finally click the **Submit** button to verify your modification.

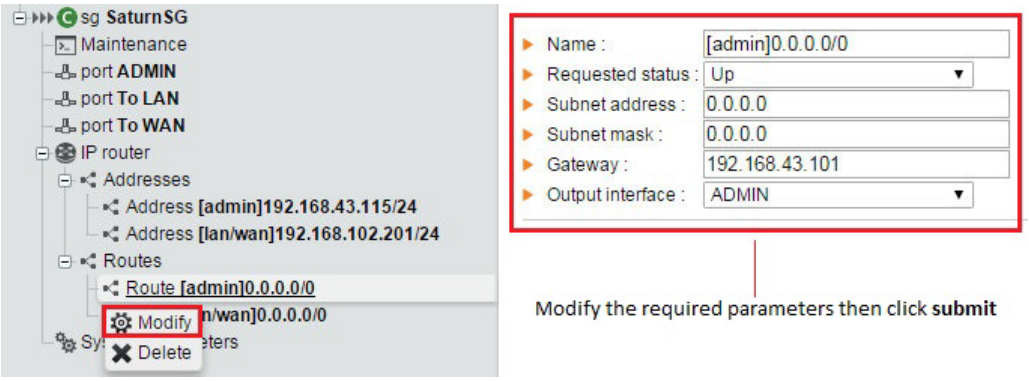


Figure 11 – Admin route modification

Note: For a NAT environment, optional expert parameters are available for ADMIN IP addresses:

Public IP address: the SGM will connect to this address to communicate with the SG.

SSH port associated with the public IP address: the SGM will call this port (and not port TCP 22) to communicate with the SG when using SSH.

8 SYSTEM PARAMETERS (SNMP, NETFLOW, WEBCACHE)

To modify a StreamGroomer's SNMP, NetFlow or Webcache parameters:

- First, select the "System Parameters" object from the StreamGroomer tree menu to display the **SNMP Parameters**, **NetFlow Parameters**, and **Webcache Parameters** tab.
- Either right-click on the object and select "Modify" from the menu or click **Modify** from the bar at the bottom of the page.
- Enter all necessary modifications and then click the **Submit** button.

Parameter	Description / Values
SNMP Parameters	
Community	SNMP community to poll the StreamGroomer.
SysName	Standard MIB II fields. This information will be retrieved when the StreamGroomer is polled with SNMP
SysContact	
SysLocation	
Trap-community	Optional parameters to enable SNMP traps sending by the StreamGroomer.
Trap recipient	
NetFlow Parameters (see chapter 9.2.3.2)	
NetFlow collector	There are 3 NetFlow collector options: • SGM (Integrated - v9 ticket format) • Stream Collector • External Collector **Note:** If you are using a NAT environment check the NAT box.
IP address	IP address towards which NetFlow tickets will be exported. (required for an external collector or a SGM in a NAT environment)
UDP port	The default value is set to 9991. UDP port towards which NetFlow tickets will be exported.
Format (Required when you an external NetFlow collector is selected)	The default value is v9. Defines the NetFlow ticket format (v5 or v9). **Note:** v9 is used by default for the SGM collector.
Export HTTP parameters	When a HTTP traffic is detected by the StreamGroomer, the NetFlow generated ticket will carry the following hostname and URL information: **Hostname:** only the hostname will be exported. **Hostname + URL XX:** the hostname and URL will be exported (up to XX characters).
Maximum number of tickets to export per second	The default value is set to 150 tickets per seconds. This can be manually modified by entering a new value into the box.
Webcache Parameters (see chapter 12.2.2)	
Redirected ports	The default ports are set to 80 and 8080. These are the specified TCP ports that are transparently redirected to the Webcache.
Maximum object size	The default value is set to 50,000KB (50 MB). This option lets you specify the maximum size of objects stored by the cache.
Caching policy	The default caching policy is set to "Nothing except the list below" and the "Network exceptions" are **10.0.0.0/8**, **172.16.0.0/12**, **192.168.0.0/16** only. Set of policies to define what types of traffic should be cached. Two types of caching policies can be implemented: • Nothing except a list of subnets listed below or FQDN (Fully Qualified Domain Name). • All except a list if subnets and FQDN.

Note: Some of these parameters can be modified for a set of StreamGroomers by using the Configuration tools. See chapter 4.5.2.3 for more information.

4.2.4 Alarms

9 PREDEFINED ALARMS FOR STREAMGROOMERS

To display the predefined alarms:

- From the StreamGroomer tree menu select a StreamGroomer.
- Select the **Alarms** tab to display the predefined **Performance Alarms**.

At each polling interval (i.e. every 10 minutes) the SGM checks if conditions defined in alarms are triggered or not. When a threshold is exceeded or specific event occurs, then an alarm is registered in the alarm log and can be exported by email, SNMP trap or syslog (see chapter 4.2.5.3 for exporting alarms). The following alarms are automatically available for each StreamGroomer:

	Trigger criteria	Rearm criteria	Criticality
Threshold alarms			
CPU load	CPU load > 80% (detected by polling)	< 80%	Critical
Dynamic memory usage	dynamic memory < 15% (detected by polling)	> 15%	Critical
Static memory usage	static memory < 15% (detected by polling)	> 15%	Critical
Status alarms			
Mode change	Mode change: Boot, Bypass, Monitoring, Monitoring & Control	-	Minor
	SG cannot be reached by the SGM	SG can be polled	Critical
Webcache status	Web caching service has changed from up to down	Service Up	Info
Port down	Port status has changed from up to down and SG mode different from bypass	Port Up	Critical
Dual/tandem SG issue	Slave SG has become active (detected by polling)	Master SG has become active	Critical

Note: For Dual / Tandem StreamGroomers, alarms are related to the active StreamGroomer, which is the Master StreamGroomer in normal operation.

10 MODIFYING PREDEFINED ALARMS FOR STREAMGROOMERS

To modify alarm thresholds and levels set on a StreamGroomer:

- Click on **STREAMGROOMERS>xx** in the tree menu.
- Select the *Parameters > Alarms* sub-tab to display the Alarms on threshold page. Click one of the links to modify the threshold criteria and level.

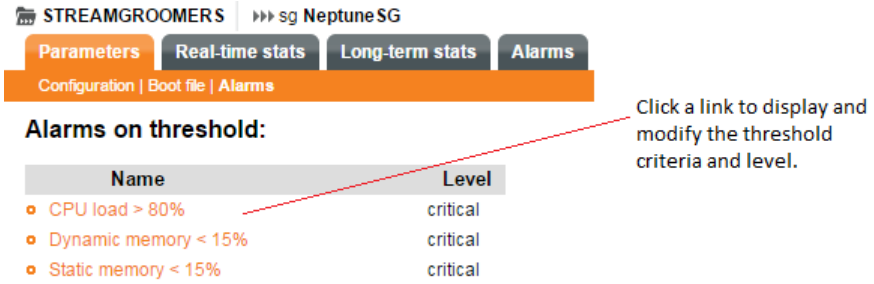


Figure 12 – Modifying the predefined SG alarms

- Click the **Modify** button to begin modifications.

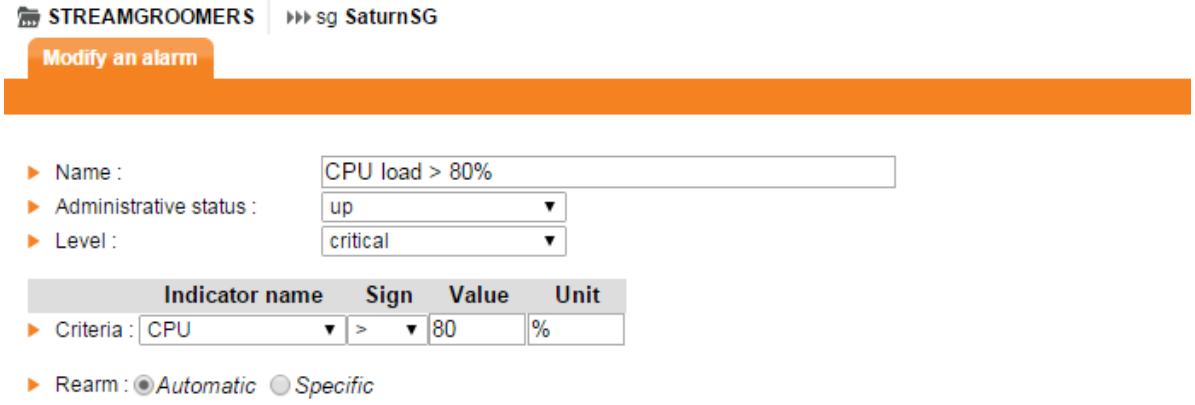


Figure 13 – Alarms modified

- Following your changes, click the **Submit** button.

11 ALARMS EXPORT

Different options can be provisioned to export StreamGroomers alarms:

	Available Perimeters	Provisioning Page
Email	All StreamGroomers	SG tree>Management tools>General parameters Alarm export tab (see chapter 4.5.1.2)
SNMP trap **Syslog**	All StreamGroomers (parameters shared with Services alarms)	Services tree >Management tools>General parameters Alarm export tab (see chapter 0)

Note: Alarms with a rearm criteria (threshold alarms, port down, unreachable SG, Dual/Tandem SG issue), an export will be performed when the alarm is triggered and again when the alarm is rearmed.

4.3 STREAMGROOMER LAUNCH

4.3.1 StreamGroomer Boot and OPE Software

A StreamGroomer has the following embedded software:

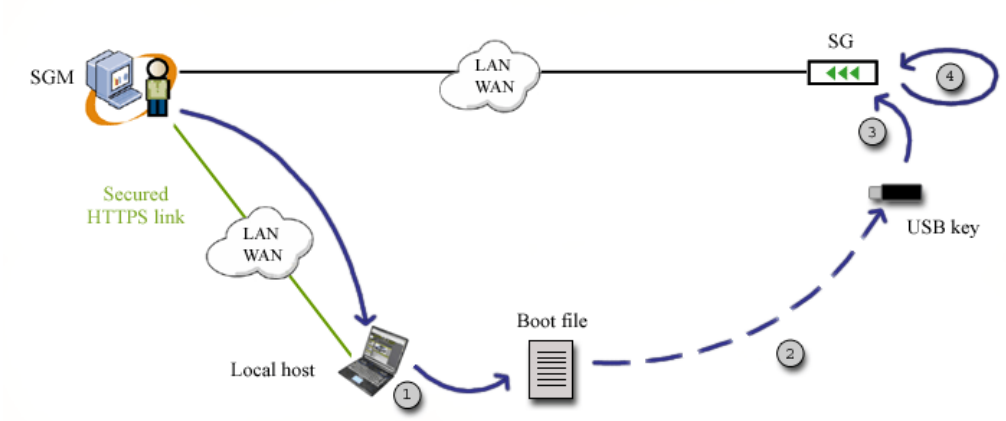
- Boot Software: only the administration service is available (bypass is closed)
- Operating (OPE) Software: all services are available

The default active software on a StreamGroomer is the boot software. In order for the SGM to have access to the StreamGroomer, the boot parameters must be provisioned by one of the following methods:

- **By asynchronous cable:** see the "StreamGroomer Installation Guide" for more details. The defined parameters using this method must be the same as those defined in StreamView.
- **By USB key:** see chapter 4.3.2. This method ensures that boot parameters are the same as those defined in StreamView.

4.3.2 Boot parameters provisioning with a USB Key

Boot parameters can be imported into a StreamGroomer by using a configuration file loaded on a USB key. The process is as follows:



1. Click on **STREAMGROOMERS>xx** in the tree menu, on the ***Parameters>Boot file*** sub-tab. Then click on the **Download the boot file on the local computer** link. Download the boot file to a local PC.

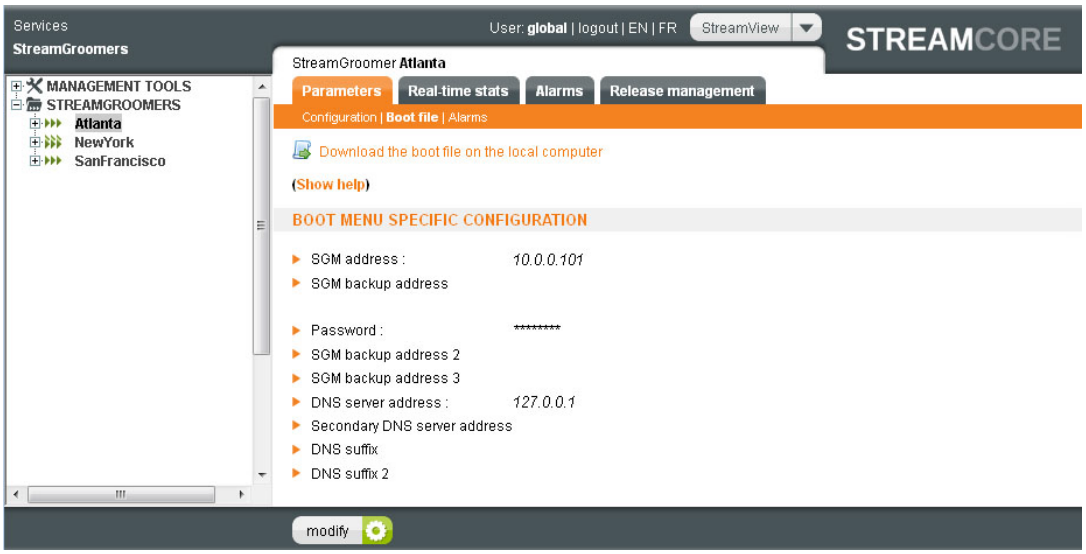


Figure 14 – Download a boot file

2. Copy the boot file onto a USB key.

3. Insert the USB key into the StreamGroomer.
4. Power down and up. Wait for a few minutes till the StreamGroomer has booted entirely.
5. When the USB key is plugged in a StreamGroomer and it is rebooted, the following operations are automatically performed:
    - USB key mount + USB key writing check
    - Search for a *sgconfig_<sgname>.txt* file
    - Security parameters checking (password, optional strong SSH authentication…)
    - Boot file parameters import
    - Status file push on the USB key

A StreamGroomer will make different kinds of "beep" sounds at the end of these operations:

Beep	Event
Double short high-pitched beep and then deep beep	The 5 steps described above have been successful. A status file summarizing the configuration has been pushed on the USB key.
Several short high-pitched beeps	A strong SSH authentication has been required and the StreamGroomer is generating its pair of public/private RSA keys during step 4.
Several long deep beeps	Step 1 has failed (USB key mount)
Single long deep beep	Step 2, 3 or 4 has failed. If step 2 has failed, then a *sgstatus_ERROR.txt* file is pushed on the key (for instance if the StreamGroomer has found several file starting with sgconfig). If step 3 or 4 has failed, then a *sgstatus_<sgname>.txt* is pushed on the key and contains a message explaining the failure.

6. Remove the USB key and check the *sgstatus_<sgname>.txt* file.

Important: If a file named *sgstatus_<sgname>.txt* is present on the USB key, the configuration file will not be taken into account.

Note: (Optional) The boot password can be defined and changed before downloading the boot file. Additional boot parameters can be defined as well.

Note: In case SSH administration with strong authentication is enabled, then the last step is to import the SG public-key into the SGM. See chapter 15.1 for more details.

After approximately two minutes, the StreamGroomer should be reachable by the SGM (assuming its administration port is plugged on the network).

4.3.3 Launching a StreamGroomer in Operating Software

To launch a single StreamGroomer xx:

1. Click on **STREAMGROOMERS>xx** in the tree menu, and then on the *Release Management > Read Status* sub-tab to check the availability of the StreamGroomer. To install the OPE software you must use the installation sub-tab.

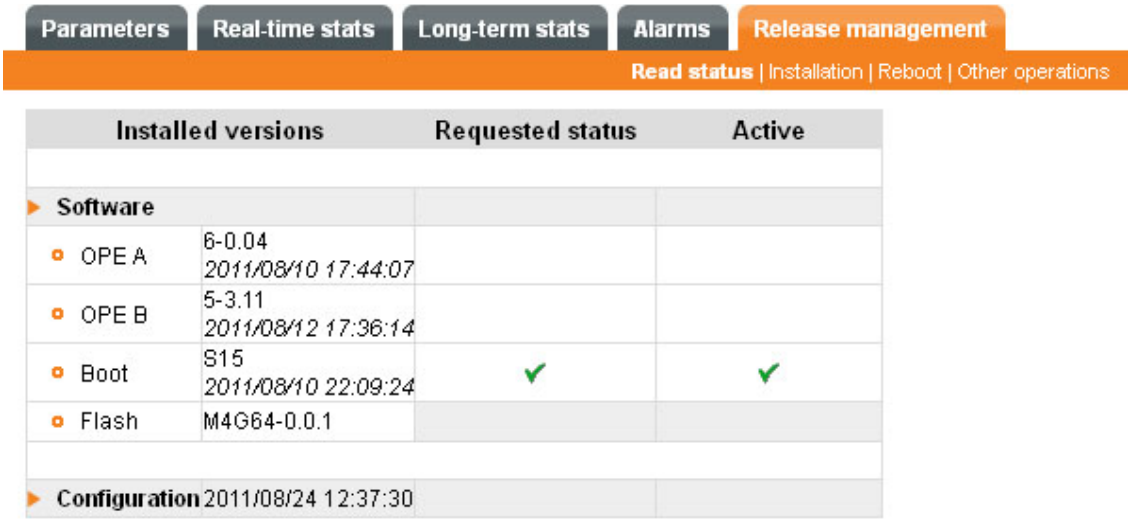


Figure 15 – Reading the StreamGroomer status

2. Next click on the **Installation** sub-tab. Use the "Available releases" and "Destination" combo box to select a release and partition to install the OPE software.

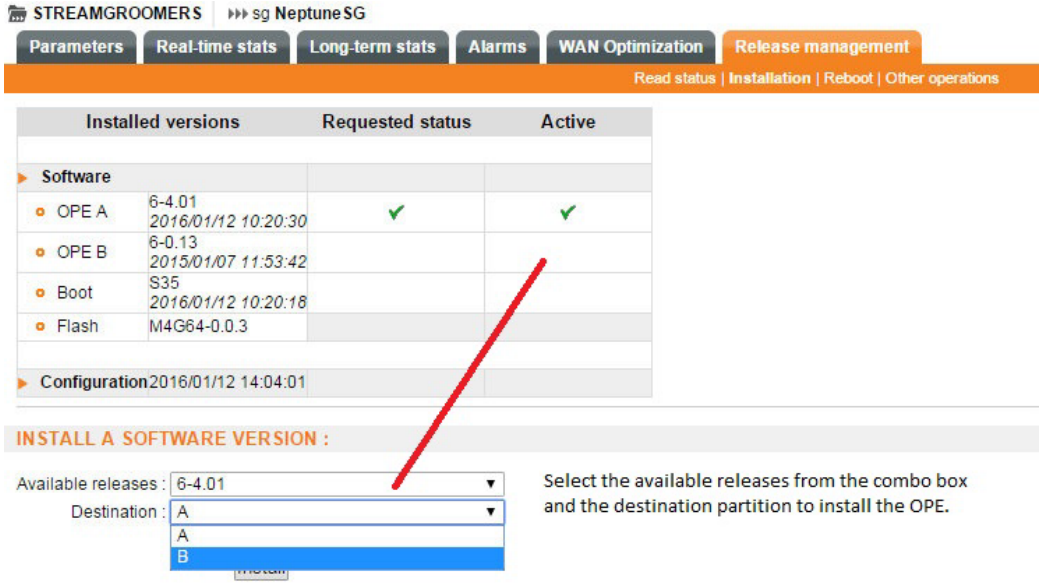


Figure 16 – Activating the OPE Software

3. After clicking the **Install** button, the software should be visible in the "Installed versions" column.

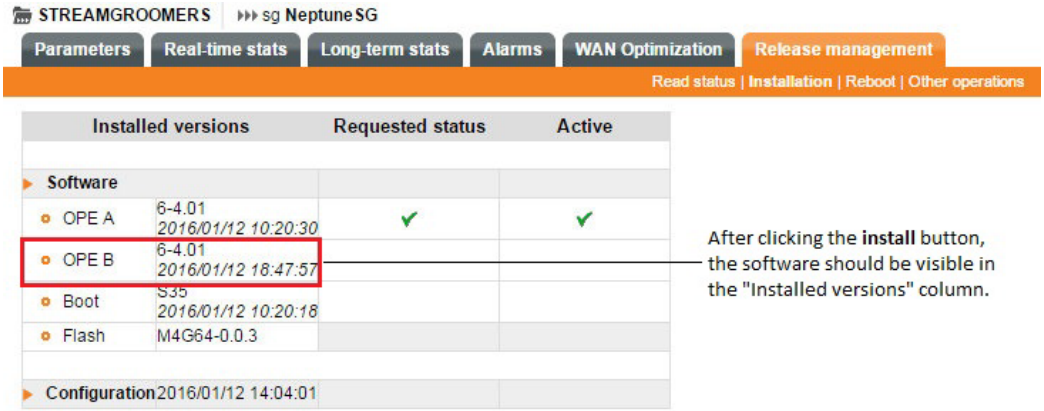


Figure 17 – Installed OPE Software on partition B

4. In order to activate the Software click on the **Reboot** sub-tab and click the **Activate** button. If the activation is successful you will notice a green check in the "Active" column.

   Warning: That this will affect your organizations current SG setup, especially if you do not have failsafe SGs in place (i.e. Duel/Tandem mode)

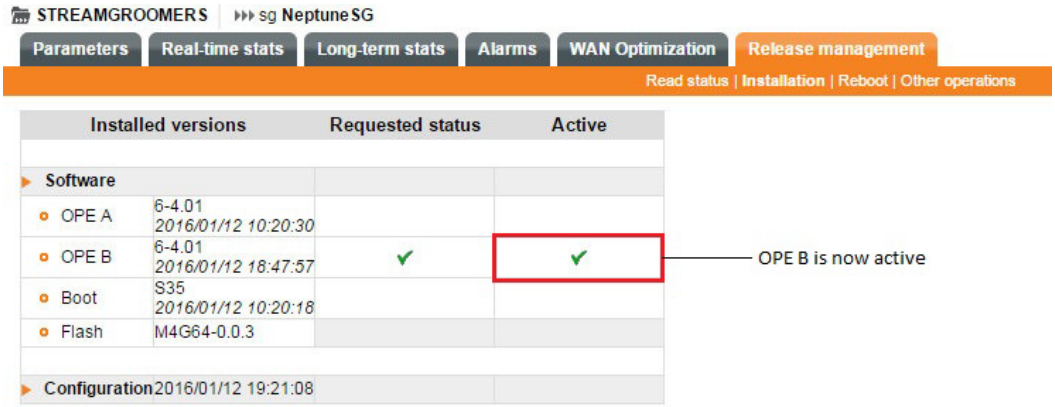


Figure 18 – Activating OPE software

5. After a restart confirm that the StreamGroomer is accessible and that it is in the operating software, by clicking again on the *Release Management – Read Status* sub-tab.

12 CONFIGURING HIGH PERFORMANCE MODE

It is possible to configure some StreamGroomers in high performance processing mode, enabling Multi-Gigabit traffic rates that are above 1-Gbps (Gigabit/second). The SG3200e series can operate using high performance mode. However, there are some limitations refer to Supported features in Multi-Gigabit Mode on p19 for a full list.

If you upgrade from v6.1 to v6.2 and your StreamGroomer supports high performance processing you will be presented with a drop-down list that offers you a choice to active it. By default high performance processing is not activated.

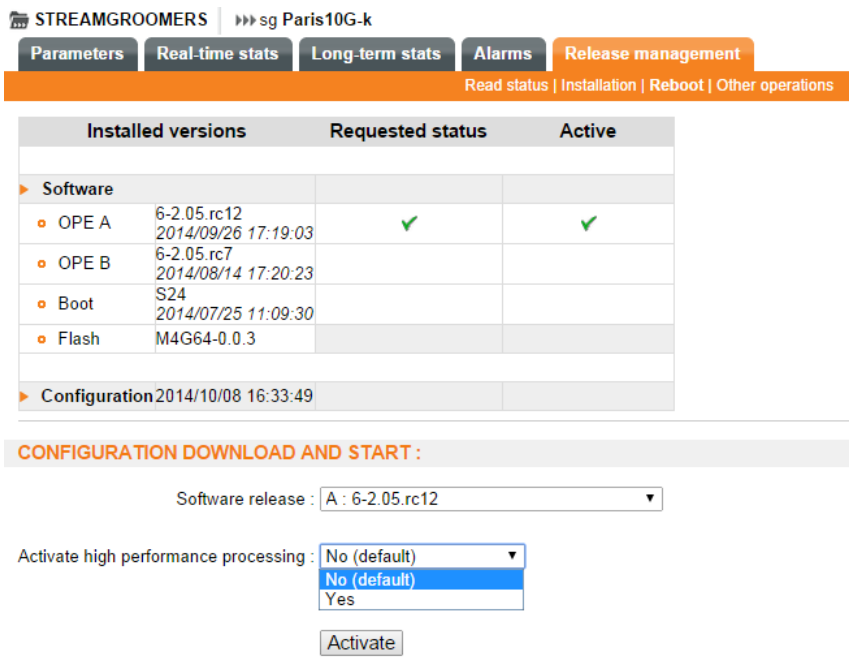


Figure 19 – High Performance Processing

To launch Dual / Tandem StreamGroomers, the operations are the same, except that each task must be performed for the Master and the Slave StreamGroomer. Two "*Release management*" tabs are therefore available when selecting a Dual / Tandem StreamGroomers in the tree menu.

4.4 STREAMGROOMER MONITORING

4.4.1 Real-time Statistics

Streamcore provides a set of information that is on-demand in real-time:

- Check StreamGroomer mode and performance: click on **STREAMGROOMERS>xx** in the tree menu, and then on the *Real-time stats* tab:

  The type of StreamGroomer is then displayed, along with the following color codes:

  - **Green:** Operational software, "Monitoring + Control" or, "Monitoring + Tagging +Control" mode.
  - **Orange:** Operational software, "Monitoring or Bypass" mode.
  - **Red:** Boot software mode.

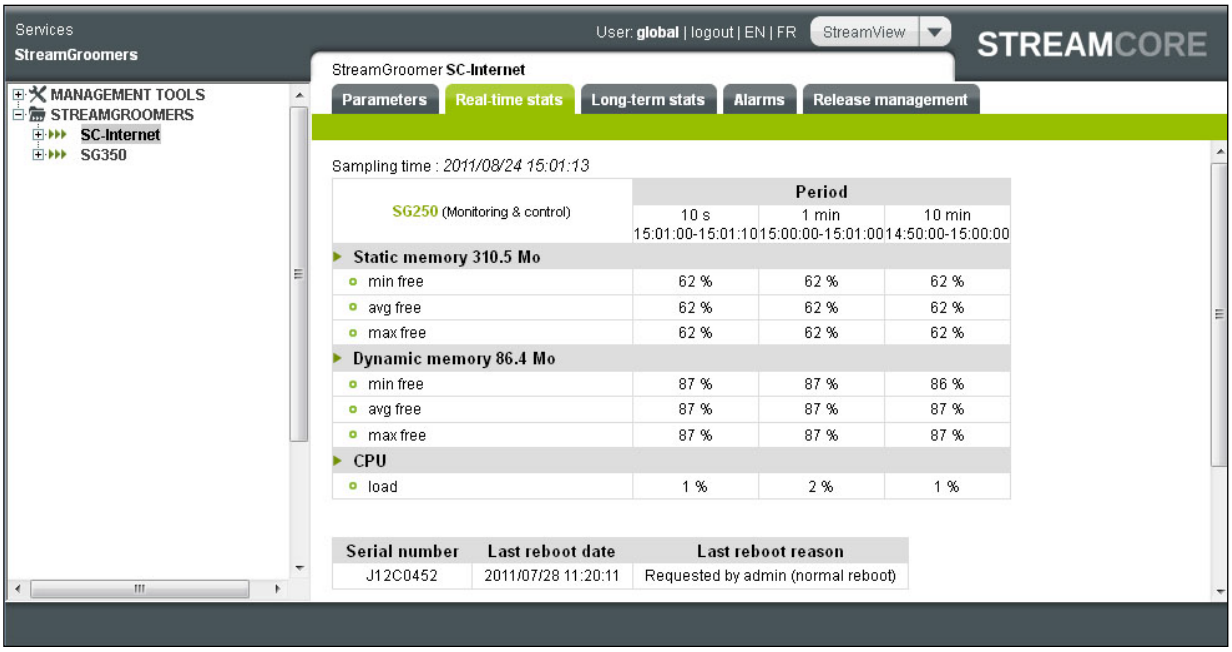


Figure 20 – Real-time statistics on a StreamGroomer

Note: For Dual/Tandem StreamGroomers, check as well the state of each StreamGroomer on this page. The Master should be ACTIF_SYNC and the Slave PASSIF_SYNC.

- If auto-negotiation was selected for the LAN and WAN ports, check the speed and duplex mode. Click on the port and then on the *Real-time stats* tab:

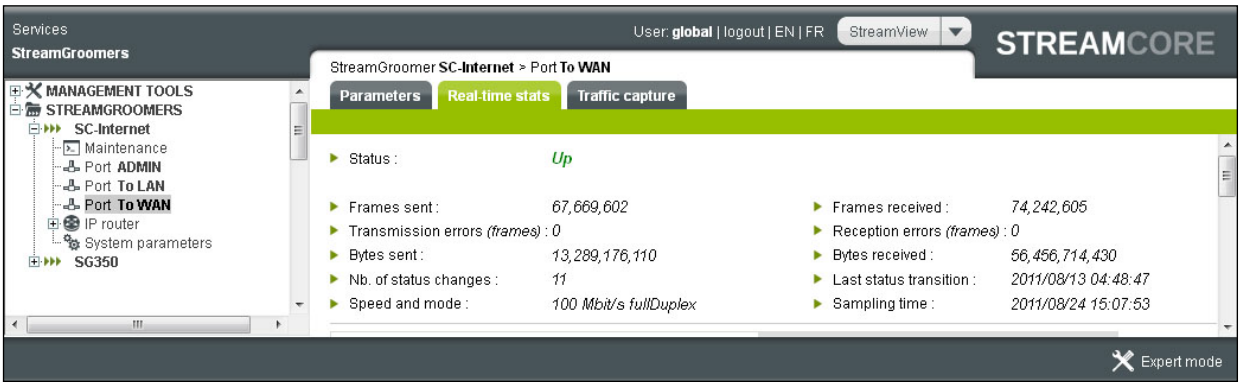


Figure 21 – Port speed and duplex mode

4.4.2 Long-Term Statistics

In order to check over the long-term the performance of a StreamGroomer xx, click on **STREAMGROOMERS > xx** in the tree menu and then on the *Long-term stats* tab.

Figure 22 – Long-term statistics of a StreamGroomer

4.4.3 Alarms

In order to check all alarms related to a StreamGroomer xx, click on **STREAMGROOMERS > xx** in the tree menu and then on the *Alarms* tab (Open or Log).

4.4.4 Traffic Capture

In order to check traffic capture (tcp dump) packets from **ADMIN**, **LAN** and **WAN** ports related to a StreamGroomer xx, click on **STREAMGROOMERS > xx** in the tree menu, port ADMIN, Port to LAN or WAN; then the *Traffic Capture* tab.

It is also possible to make a traffic capture in a rule see troubleshooting Traffic Capture.

Note: The **status** area below the start button displays the traffic capture state. If a capture is running on another LAN/WAN interface or rule, it will displayed with a link to the running capture.

Selection Parameters (Traffic Capture)	Description
IP address	Used to filter packets based on IP addresses
Other IP address	Used if you want filter from another IP address
Port	Used to filter packets on a particular port
Data length	To select the packet size being captured for each packet (max = 1500). The default value is set to 200 per packet
Packets nb.	The default packet capture value is 1000
Capture for	The default duration of traffic capture packet is set to 5 minutes. However you can change this by selecting another value in the combo box. Durations available: **Unlimited time** **Seconds:** 5,10 or 15 **Minutes:** 1,5,10 or 30 **Hours:** 1h or 2hr
Interactive Mode and Decode ASCII and use colors	This mode enables you to view traffic capture directly in StreamView. Use the ascii decoding + color checkbox to enhance the displayed results
File Size	You can specify the traffic capture file size you want to download. If you specify a large file size, it is advised that you use the **Check** button to verify that your SG can handle the files size in compliance to the number of files.
Number of files	You can specify the number of files you want to store on the SG. However you should be aware that there is a file storage size limited. If you specify a large amount of files to keep, it is advised that you use the **Check** button. This is to verify that your SG will be in compliance to the file size. The file size will change accordingly and vice-versa.
Check	The **Check** button allows verifies that your SG can store an adequate number of files according to your file size.
Run in background	This mode lets you configure and run the traffic capture tool in the background. It is possible to by specify the maximum file size (packets being transmitted or received) and the number of files to keep. This is particularly helpful if you want to finish other tasks in the interface and come back at a later stage to download a collection of traffic captures. If you want to download multiple traffic captures from the interface, they will be download in a zip format. It is also possible to specify the run in background mode for a specified duration of time using the "capture for" combo box.. Files are stored in a cyclical way meaning that when the file size has reached its limit, old files will be deleted to make way for new files. After the Traffic Capture process has finished the result will be displayed in a table with the following information: • Name of ".pcap" file • Traffic capture date • Capture file size

	• Download checkbox and Download button See Figure 23 - Traffic Capture tool using run in background mode A traffic capture is complete when one of the two parameters (packets nb or max.duration) has been satisfied. **Note:** If you download the ".pcap" file, it will only be viewable when imported into a packet analyzer (for example Wireshark) for further analysis. **Note:** It is only possible to make one traffic capture at a time and therefore you can only capture the traffic for 1 rule at a time.
More options	Options and Filters See Traffic Capture Options and Filters in the Appendix.
Start (Button)	Start traffic capture according to your set parameters.
Stop (Button)	Let's you stop a traffic capture if you need to change a parameter or cancel.

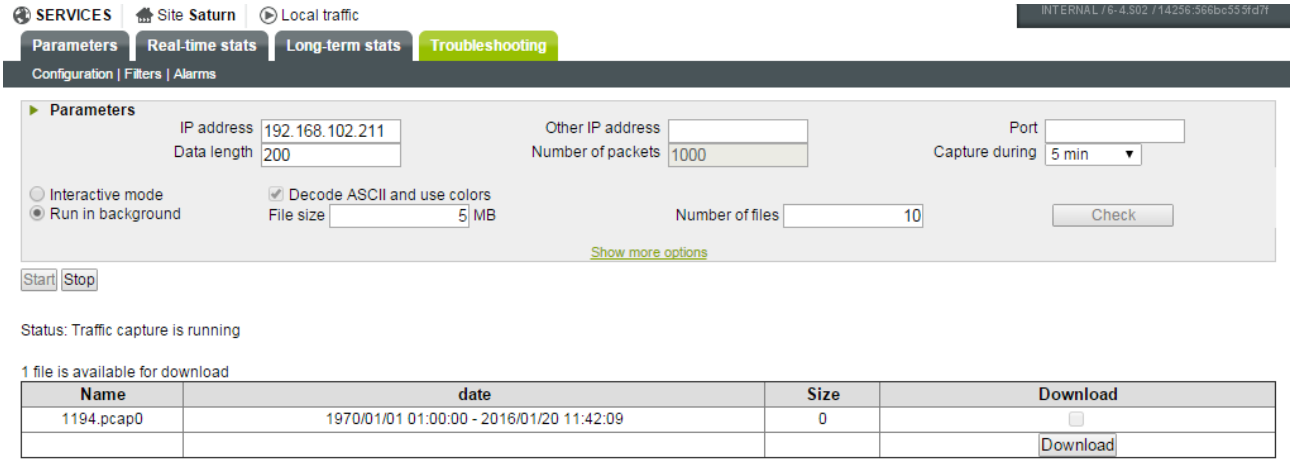


Figure 23 - Traffic Capture tool using run in background mode

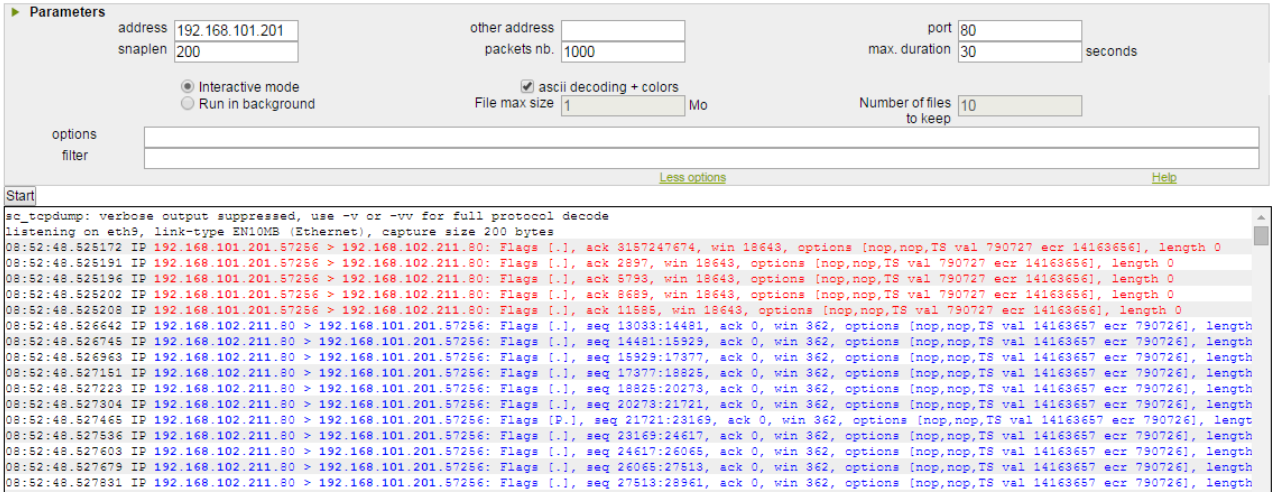


Figure 24 - Traffic Capture tool using run in interactive mode

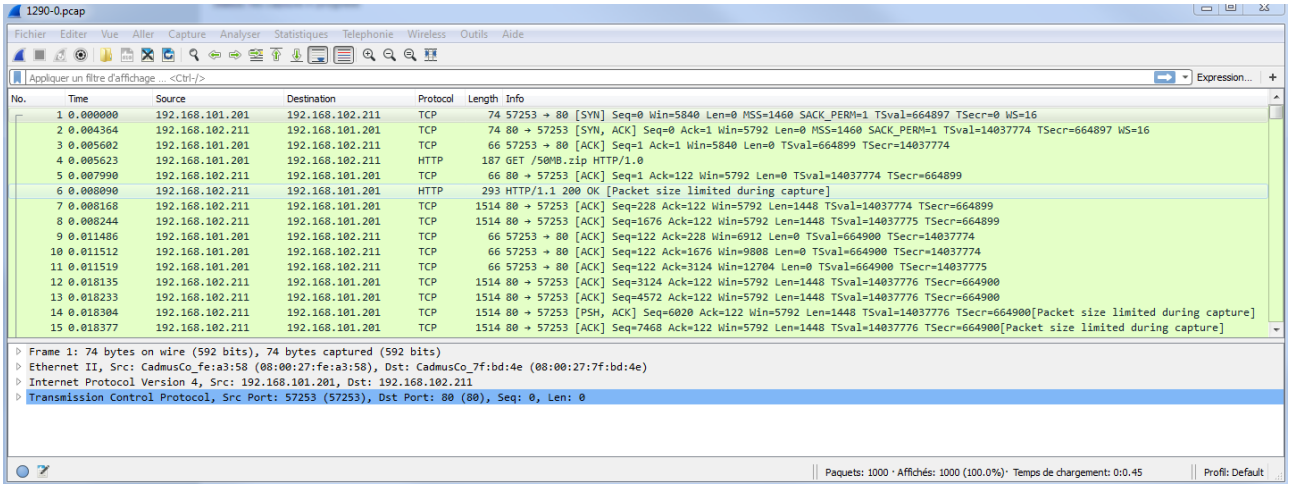


Figure 25 - Download "pcap" file and import into a packet analyzer for further analysis

4.5 MANAGEMENT TOOLS

4.5.1 General Parameters

13 CATEGORIES MANAGEMENT

To classify StreamGroomers into categories, expand the **MANAGEMENT TOOLS** in the tree menu, and click on **General parameters**. Any of the category type defined in the Services can be used to classify the StreamGroomers (see chapter 6.2 for categories management).

Once a category type has been selected for the StreamGroomers, the benefits are:

- StreamGroomers are classified into category folders in the tree menu
- A category of StreamGroomers can be directly selected when using other management tools

14 ALARMS EXPORT

StreamGroomers alarms export by SNMP trap or Syslog needs to be configured in the Services tree (in **Management Tools > General Parameters**, *Alarms Export* tab, see chapter 14.1).

To define email export parameters for StreamGroomer alarms, expand the **MANAGEMENT TOOLS** tree menu, click on **General Parameters**, then select the *Alarms Export* tab. The following modifications are available in the section related to StreamGroomers alarms export by email:

- **Modifying a recipient:** Click on the recipient in the right-hand operating window; click the "Modify" button, enter the modifications, and then click the "Submit" button.
- **Adding a recipient:** Click on **+ Add** in the right-hand operating window; enter the recipient parameters, and then click on the "Submit" button.
- **Deleting a recipient:** Click on the recipient and then on the "Delete" button.

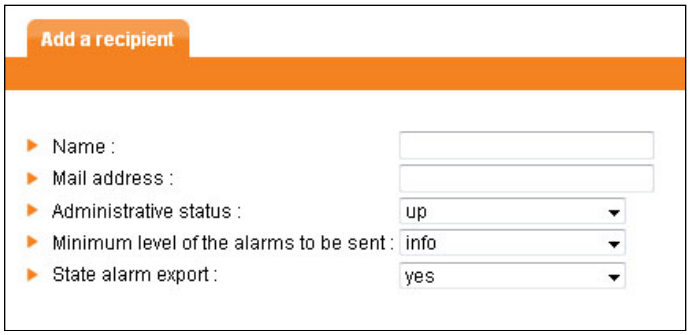


Figure 26 – Add and Modify an email recipient

Note: Sending emails is effective only if a SMTP gateway has been defined in SGMconf system parameters (See SGMconf user guide for more details).

4.5.2 StreamGroomers Configuration

15 INTRODUCTION

To display a summary of StreamGroomers configuration or make mass configuration changes, expand the **MANAGEMENT TOOLS** tree menu, click on **StreamGroomers configuration**. The following parameters can be displayed or updated:

StreamGroomer Parameters		"Summary" Tool	Mass Configuration Change Tools	
			"Set parameters" Tool	"Change mode" Tool
Main parameters (See chapter 4.2.3 for more information)	*Mode*	Yes	-	Yes
	Dialog type	Yes	-	-
	Insertion mode	Yes	-	-
Expert parameters (See chapter 4.2.3 for more information)	*Statistics polling*	Yes	Yes	-
	Reinit sending	Yes	Yes	-
	Ports status mirroring	Yes	-	-
Ports/Routing/System parameters (See chapter 4.2.4 for more information	*Ports*	Yes	-	-
	Admin IP address	Yes	-	-
	SNMP	Yes	Yes	-
	NetFlow	Yes	Yes	-

16 SUMMARY

A summary of the StreamGroomers' configuration can be displayed automatically (and exported in a CSV file if required). The information displayed is retrieved directly in the configuration database (without any interaction with the StreamGroomers).

17 SET PARAMETERS

Mass configuration changes can be performed on a set of StreamGroomers for the following parameters:

- SNMP configuration
- Webcache parameters
- NetFlow configuration
- SGM-SG configuration (statistics polling, reinit sending)

The steps to follow:

- Click on the **Launch** sub-tab
- Select StreamGroomers or a Category (if a category type has been defined in Categories management)
- Select a parameter from the combo box
- Click on the **Apply** button
- The result will be displayed in the **Results** tab

18 CHANGE MODE

In order to change the mode of a set of StreamGroomers, follow these steps:

- Click on the **Launch** sub-tab
- Select StreamGroomers or a Category (if a category type has been defined in Categories management)
- Select the mode
- Click on the **Apply** button
- Click on the **Results** sub-tab to view results

4.5.3 StreamGroomers Inventory

19 INTRODUCTION

To get an inventory of the StreamGroomers, expand the **MANAGEMENT TOOLS** tree menu, click on **StreamGroomers Inventory** in the tree menu. The following information is available depending on the tool being used:

Retrieved Information		Status Summary (Polling based)	On-demand Inventory	Configuration Synchronization	Alarms
Mode and Status	SG Mode / Status	Yes	Yes	-	Yes (history)
	Last reboot	Yes	Yes	-	-
	Ports status	Yes	Yes	-	Yes (history)
	Performance	-	-		Yes (history)
HW and SW Information	SG type	Yes	Yes	-	-
	Site name	Yes	Yes		
	Installed and activated software	-	Yes	-	-
	Serial number	-	Yes	-	-
Configuration synchronization	Automated reinit parameter	-	-	Yes	-
	Reinit state	-	-	Yes	-
	Last reinit report	-	-	Yes	-

20 STATUS SUMMARY

An administrator can check the state of all StreamGroomers by using the "Status Summary" tool. This data is based on information automatically retrieved every 10 minutes (StreamGroomer statistics polling) by the SGM. A list of deployed StreamGroomers is displayed with the following information for each StreamGroomer:

- SG name / Site name
- SG type
- Mode/Status. Possible values are:
  - Unreachable
  - Boot
  - Bypass
  - Monitoring
  - Monitoring + Control
  - Monitoring + Tagging + Control
  - Polling disabled
- Time since Mode/Status change
- Port state (ETH, LAN, WAN) and the time since last state modification

Note: The information displayed is updated every 10 minutes after each polling. Dual/Tandem StreamGroomers are displayed in a single line since the polling uses the shared statistics IP address.

21 ON-DEMAND INVENTORY

For a more detailed StreamGroomer on-demand inventory, the "On-demand inventory" tool can be used. The steps to follow are:

- Click on the **Launch** sub-tab
- Select StreamGroomers or a category (if a category type has been defined in Categories management)
- Click the **Activate** button
- Click on the **Results** sub-tab to display results

The following information is available per StreamGroomer in the inventory:

- Site name
- SG name
- Administration IP address
- SG type
- Mode
- Activated software
- Installed software
- Serial number
- Last reboot date
- Ports configuration and status

22 CONFIGURATION SYNCHRONIZATION

All modifications in "Services" that impact StreamGroomer traffic management are sent to them by the SGM (except if the "Automated reinit sending" expert parameter is set to "No"). If the volume of reinits is very high, then it may take some time: an administrator can check the state of all StreamGroomers reinits by using the "Configuration Synchronization" tool.

The list of deployed StreamGroomers is displayed with the following information for each StreamGroomer:

- Automated reinit parameter: yes/no
- Reinit state. Possible values are:
  - Not executed yet (for instance when the SGM is preparing the updates to be sent)
  - In progress
  - None (when all reinits have been sent)
  - Error
- Error report, with a detailed message when the "Reinit state" is "Error"
- Retry: a button to send again the renits when the "Reinit state" is "Not executed yet" or "Error"

Note: Dual / Tandem StreamGroomers are displayed in 2 separate lines since the reinits sending uses the 2 independent Master and Slave IP addresses.

23 ALARMS

See chapter 4.2.5 for more information on the different types of StreamGroomers alarms.

The available alarm summaries are:

Open sub-tab: an administrator can view if alarms are currently triggered for all StreamGroomers.

Summary sub-tab: an administrator can view if alarms have been triggered in the past for all StreamGroomers.

The "Period" combo box allows you to select and display all StreamGroomer alarms for a predefined period. If at least one alarm has been triggered, then the StreamGroomer with the longest alarm duration will be displayed.

Log sub-tab: an administrator can check all alarms triggered for all StreamGroomers.

4.5.4 Install Software

To download new software into a set of StreamGroomers, expand the **MANAGEMENT TOOLS** tree menu, and click on **Install software** in the tree menu.

- Click on the **Launch** tab
- Select StreamGroomers or a Category (if a category type has been defined in Categories management)
- Select the OPE software version to install from the combo box
- Click on the **Install** button
- Click the **Results** tab to displayed installation results

4.5.5 Reboot

To reboot a set of StreamGroomers, open the **MANAGEMENT TOOLS** in the tree menu, and click on **Reboot** in the tree menu.

- Click on the **Launch** tab
- Select the target StreamGroomers or a Category (if a category type has been defined in Categories management)
- Select to reboot now or at a specific date and time
- Select the software version activation from the combo box
- Click on the **Activate** button
- Click the **Results** tab to displayed reboot results

5 UMT – Application Performance Scorecards (APS)

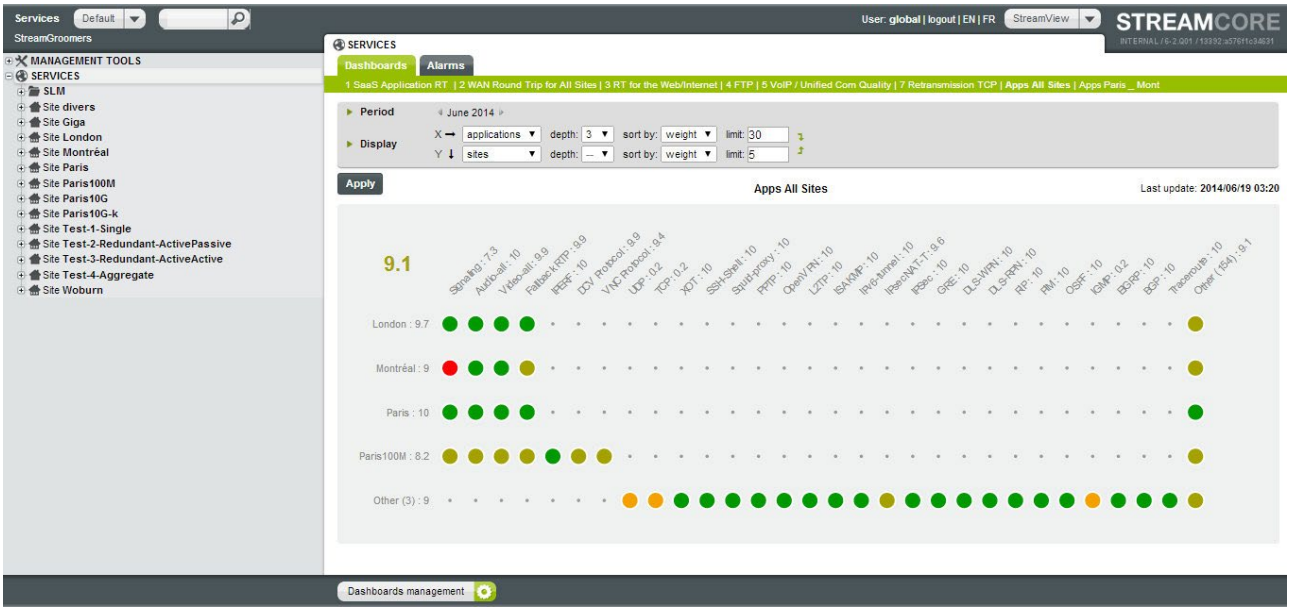
5.1 INTRODUCTION

Streamcore's Application Performance Scorecard (APS) is a simple, but powerful tool designed to assist users evaluate the network performance of their Business Applications, VoIP and network protocols. Network managers can configure KPIs based on application terminal rules and VoIP data, as well as manage Service Level Agreements, for both internal Business Units (BUs) in addition and external.

Evaluation is based on metrics (defined as indicators in scorecard configuration) measured by StreamGroomers and computed by the SGM. The user selects an indicator and two thresholds. The metric is compared against the thresholds and the result leads to a score out of 10, 10 being the best score and 0 the worst. The thresholds represent the areas of good and bad performances as decided by the user.

For example, a network administrator would like to evaluate the VoIP service performance by using the Mean Opinion Score (MOS) indicator. MOS indicates how end-users perceive communications quality. Measurements are based on a score between 1 and 5. In terms of classification, 5 represents very good and 1 represents extremely poor VoIP communication. If the MOS is equal or greater than 4, the VoIP application receives a high score (9 or 10) in the APS. If the MOS value is less than 2.9 this performance would be regarded as not acceptable; therefore, its score will be low (2, 1 or even 0). Based on this example, a user should enter the following thresholds when configuring a scorecard, 4 (good performance area) and 2.9 (bad performance area). The score is evaluated every 10 minutes for the selected VoIP application and sites.

Scores are displayed in a matrix displaying the performance of a specific indicator associated to an application and site, or the evolution of the indicator for applications or sites. A scorecard layout can be customized.



Application Performance Scorecard (APS)

5.2 APPLICATION PERFORMANCE SCORECARD (APS) MANAGEMENT

To configure scorecards:

1. Select **SERVICES**. The scorecard tab is displayed automatically.
2. Click the **Configure** button located on the bottom of the page.
3. Select **Add scorecard**.

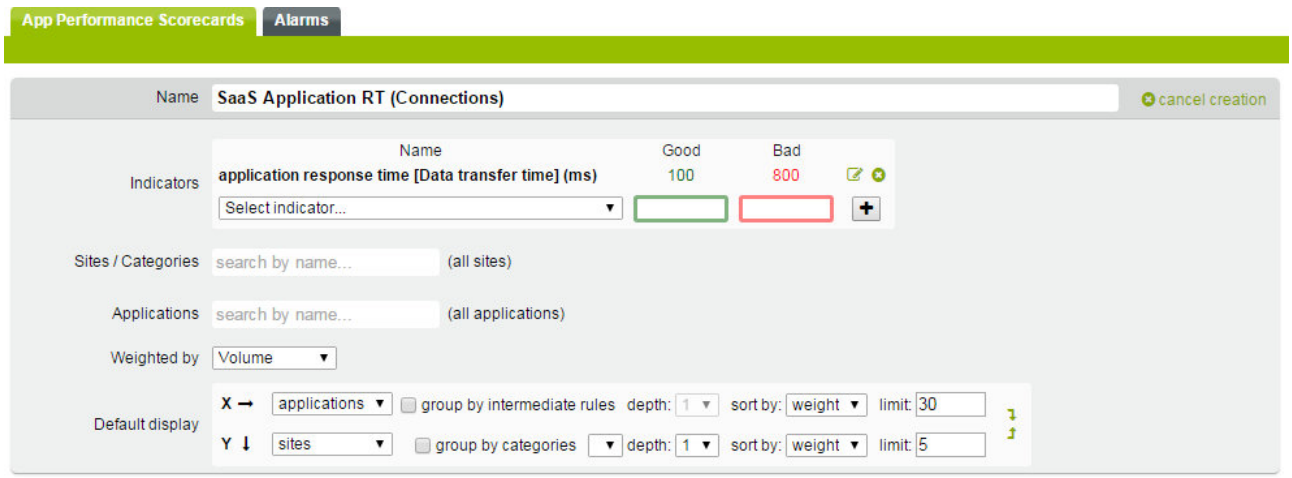
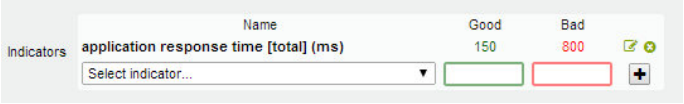


Figure 28 – Application Performance Scorecard creation

5.2.1 Scorecard Parameters

Scorecard parameters, actions, and descriptions are outlined in the following table:

Parameter/Label	Description / Values	
Name	The "name" text box is used to enter a scorecard name. It is recommended that you create a name that is closely associated with the collected objects or sites. For example, SaaS Applications for Streamcore or WAN round trips for all sites.	Not applicable
Indicators		
Good and Bad Indicators	The Good/Bad Indicator boxes allow you to enter a set of benchmarks that correspond with your (or your customers) considered good and degraded application performance, VoIP or network service.  The good quality (**green**) value appears as a green circle in a scorecard and a bad quality (**red**) value appears a red circle. In addition, two other colors also feature in a scorecard and they represent performance quality states that lie between "Good" and "Bad" values. **brown/green** represents a "Slightly degraded" quality and **orange** represents a "Severely degraded" quality.	
Applications	Application response time [Total] (ms) Application response time [Data transfer time] (ms) TCP calls (cal/mn) TCP retransmission throughput [local to remote] (%) TCP retransmission throughput [remote to local] (%) Average number of connections WAN round-trip time (ms) Average throughput [local to remote] (bps) Average throughput [remote to local] (bps) Maximum throughput [local to remote] (bps) Maximum throughput [remote to local] (bps)	
VoIP	VoIP burst density	

	VoIP number of communications VoIP network delay (ms) VoIP average discard throughput (%) VoIP max discard throughput (%) VoIP jitter [avg] (ms) VoIP jitter [max] (ms) VoIP network loss [avg] (%) VoIP network loss [max] (%) VoIP MOS-CQ VoIP MOS-LQ	
Site/Categories	The default setting is "all sites" however; it is also possible to customize by adding individual sites or categories ad hoc. Enter the first letters of the site or category and the autocomplete feature will help you complete the site/category name.	Not applicable
Applications	The default is set to "all applications" however; it is also possible to customize by adding individual applications ad hoc. Enter the first letters of the application and the autocomplete feature will help you complete the application name.	
Weighted by	Use this feature to determine your scorecard weight. It permits you to select a method to evaluate your displayed results. The three options are: None (No weight is applied to scorecard result) Connections – displays results by number of connections Volume – displays results by volume See Interpreting Scorecards on p44	
Display		

Default Display
(x and y-axis)
	This section allows you to personalize your displayed scorecard. It can be changed at a later stage.
	The available options are
	• **Sites**
	  ○ Group by categories (for example sites by countries or organizational type)
	• **Application**
	  ○ Group by intermediate rules (check box)
	• **Time**
	Each display option has an associated depth (associated with terminal rules), sort by (weight or score), and limit (number of sites or applications).
	
	Available display settings to select from:
	
	1. X and Y display can be set to "applications" and "sites" (or vice versa); and a period is defined using the "Period" drop down list or calendar picker.
	
	2. X and Y display can be used and one of the axis is set to "time".	

5.2.2 Pre-filling a Scorecard

The scorecard pre-fill option is useful when you require initial values perhaps to evaluate good and bad benchmarks. The check boxes on the top of the scorecard panel allow you to populate a scorecard based on historical data.

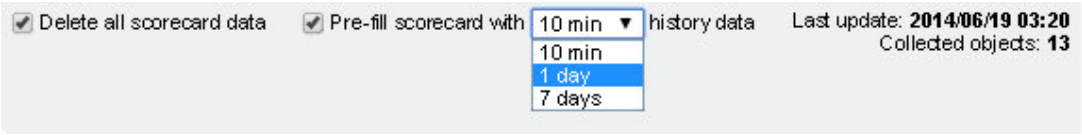


Figure 29 – Scorecard Pre-fill

Label	Description	
Delete (active when scorecard has been created)	Used to delete the selected APS. To delete multiple scorecard's select scorecard then click **Apply**.	Not applicable
Cancel creation	Closes current scorecard creation. All scorecard information is lost.	Not applicable
Delete all scorecard data (check box) & Pre-fill scorecard (time period) with history day (check box)	By selecting the "delete all scorecard data" the "Pre-fill scorecard (period) with history data" is activated.	The following time periods are available from the "Pre-fill scorecard (time period) with history day" drop-down list: **10 minutes** **1 day** **7 Days**
Last updated (text)	The information displayed here shows when the scorecard (objects in the scorecard) was last updated.	yyyy/mm/dd hh:mm
Collected objects (text)	The collected objects number is associated with the number of terminal rules used. The greater objects collected; the greater impact it will have on SGM performance. It may also take longer to display your scorecard results, as a greater number of calculations have are taken into account. If this is the case, try to either limit or selected sites or applications.	

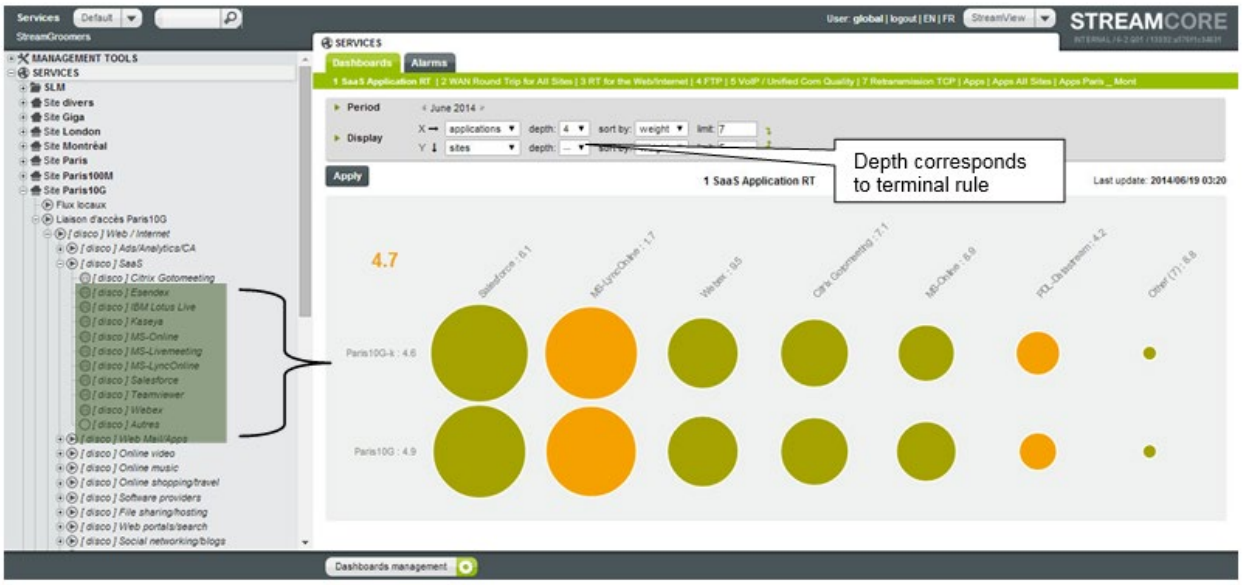


Figure 30 – Application terminal rules at depth 4 as seen in the menu tree.

5.2.3 Add/Modify/Delete Operations

24 ADD A SCORECARD

To add a scorecard:

1. Select **SERVICES**. The scorecard tab displays automatically.
2. Click the **Configure** button located on the bottom of the page.
3. Click "Add scorecard …"
4. Enter required information.
5. Click the **Apply** button to activate the new scorecard.

25 MODIFY A SCORECARD

To modify a scorecard:

1. Select **SERVICES**. The scorecard tab displays automatically.
2. Click the **Configure** button located on the bottom of the page.
3. Select and modify the scorecard.
4. Click the **Apply** button.

26 DELETE A SCORECARD

To delete one or several scorecards:

1. Select **SERVICES**. The scorecard tab displays automatically.
2. Click the **Configure** button located on the bottom of the page.
3. Scroll to reach the scorecards to be deleted and click "delete" for every scorecard.
4. Click the **Apply** button.

5.3 INTERPRETING SCORECARDS

There are many ways to view scorecard results; interpreting data requires the right skills and understanding of performance data for VoIP and applications. This section aims to provide you with some examples and useful tips, to help you make sense of your scorecard result.

5.3.1 Determining results based on points of failure (score)

For the majority of cases, you will need to have a good overview of severely degraded or bad application/VoIP performance on your network. The simplest method of determining this is by selecting the "score" display option from the "sort by" drop-down list. Refer to Figure 31 – Applications sorted by score on p45.

Depending on how you configure the X and Y-axis to display *applications*, the "bad quality" (red circles) will appear either on the *far left* or at the *top* of the scorecard. This feature permits you to interpret results fast, allowing you to focus on critical problems.

Figure 31 – Applications sorted by score over 1 hour period

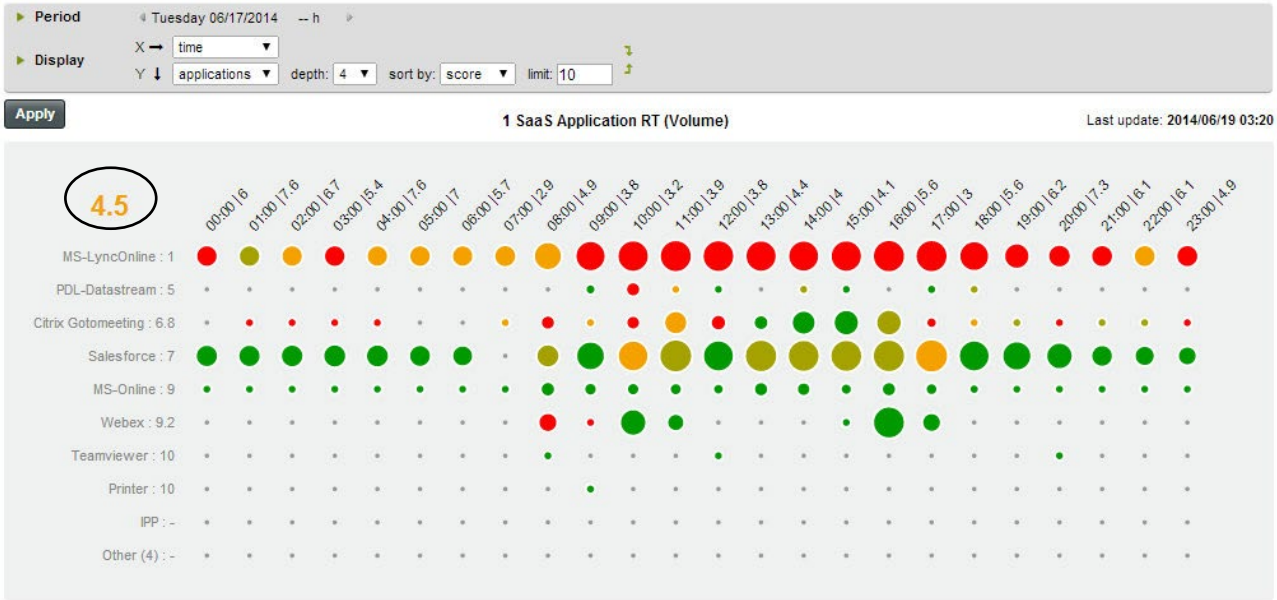


Figure 32 – Applications sorted by score over a 24-hour period

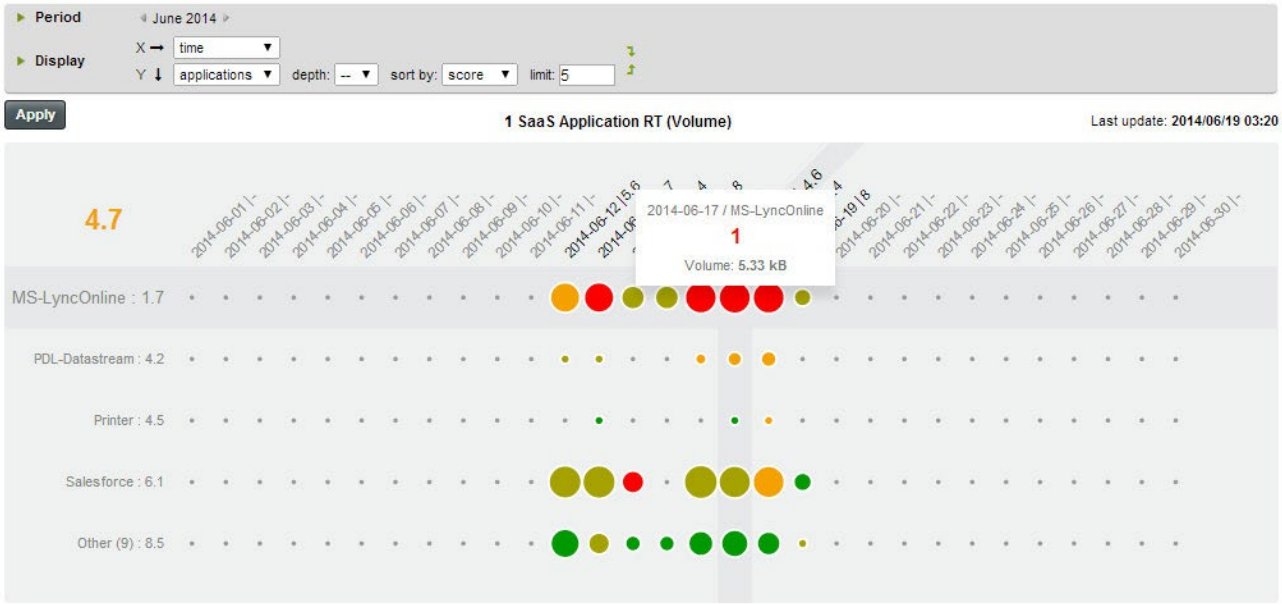


Figure 33– Applications sorted by score over 1 month

5.3.2 Determining results based on weight (volume or connection)

27 INTRODUCTION

The *weight* display option is linked to the initial scorecard configuration parameter "Weighted by". A weighted average score can be by Volume or Connection; *each* option takes into consideration several elements, which are interdependent. Described below are these elements and their functions.

Figure 34 – scorecard configuration weighted by Volume

28 WEIGHTED AVERAGE

There are two types of weighted average used to identify application or VoIP problems:

- Weighted volume
- Weighted connection

Tip: Irrespective of the selected weight used at scorecard configuration stage, your results are largely based on the "Good" and "Bad" quality indicator figures/benchmark entered. Therefore, if you are unsure of what figures/benchmark to enter, use the prefill data option when creating a scorecard. It helps you to discover good and bad quality for your scorecard. Refer to Scorecard Parameters on p41

29 CALCULATION AND METHODOLOGY FOR WEIGHTED SCORE

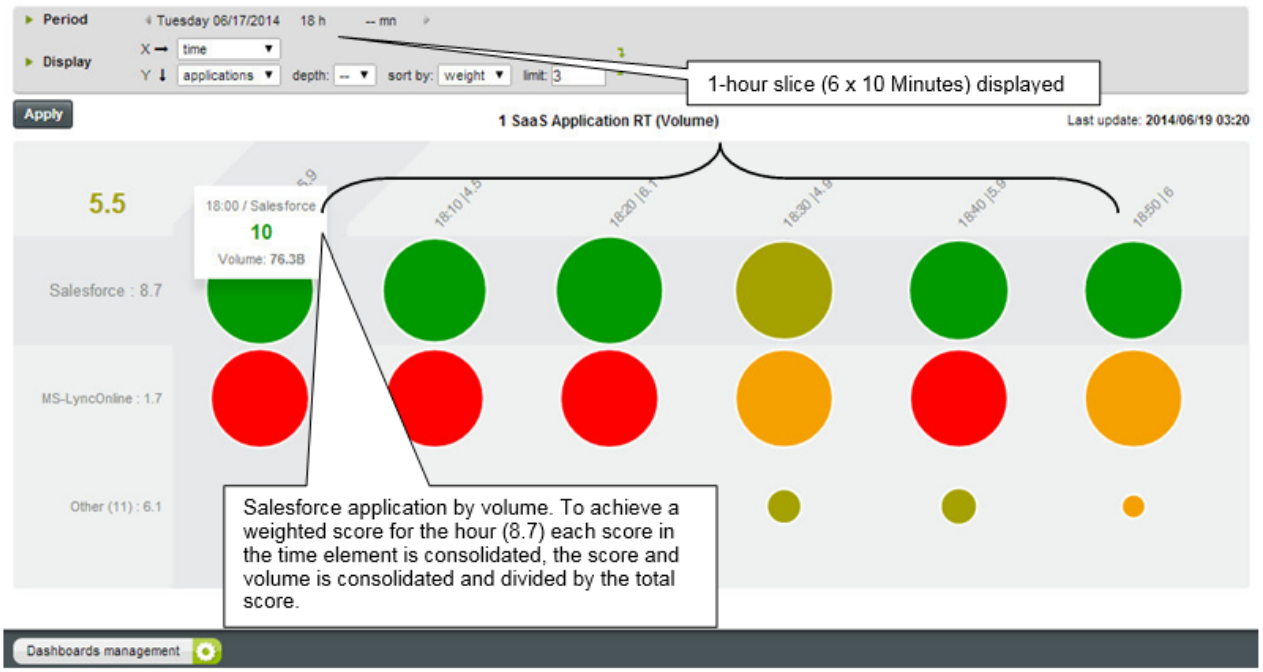


Figure 35 the X-*axis* displays *time* and the Y-*axis* displays *applications*.

From 18:00 to 19:00, the Salesforce application was given an overall weighted score of 8.7. This score is calculated by taking each 10 minute weighted score in an hour, multiplying the scores with the volume for each hour. Then by dividing this number with the total volume over an hour. The calculation is as follows:

$$\frac{\text{Score}_1\ (\text{application}) \times \text{Weight}_1\ (\text{volume or connection1}) + \text{Score}_2\ (\text{application}) \times \text{Weight}_2\ (\text{volume or connection2}) + \text{Score}_3\ (\text{application}) \times \text{Weight}_3\ (\text{volume or connection3}) + \ldots\ \text{Score}_n \times \text{Weight}_n}{\text{Weight1 (volume or connection1)} + \text{Weight2 (volume or connection2)} + \text{Weight3 (volume or connection3)} + \ldots\ \text{Weight}_n}$$

= Application weighted score

Example: The following table lists the Salesforce application scores and volumes obtained over a 1-hour period.

Time Period	Score	Volume (Weight)
1	10	76.3
2	8	65.89
3	9.1	75.76
4	6.3	52.49
5	9.3	55.84
6	9	52.94
Total over 1 hour		379.22

The volume is combined to the score to provide a weighted score:

10 **x** (76.3) + 8 **x** (65.89) + 9.1 **x** (75.76) + 6.3 **x** (52.49) + 9.3 **x** (55.84) + 9 **x** (52.94)

379.22 (total volume over 1 hour)

= 8.7

Important: Irrespective of the weight used, the calculation and methodology described above is the same.

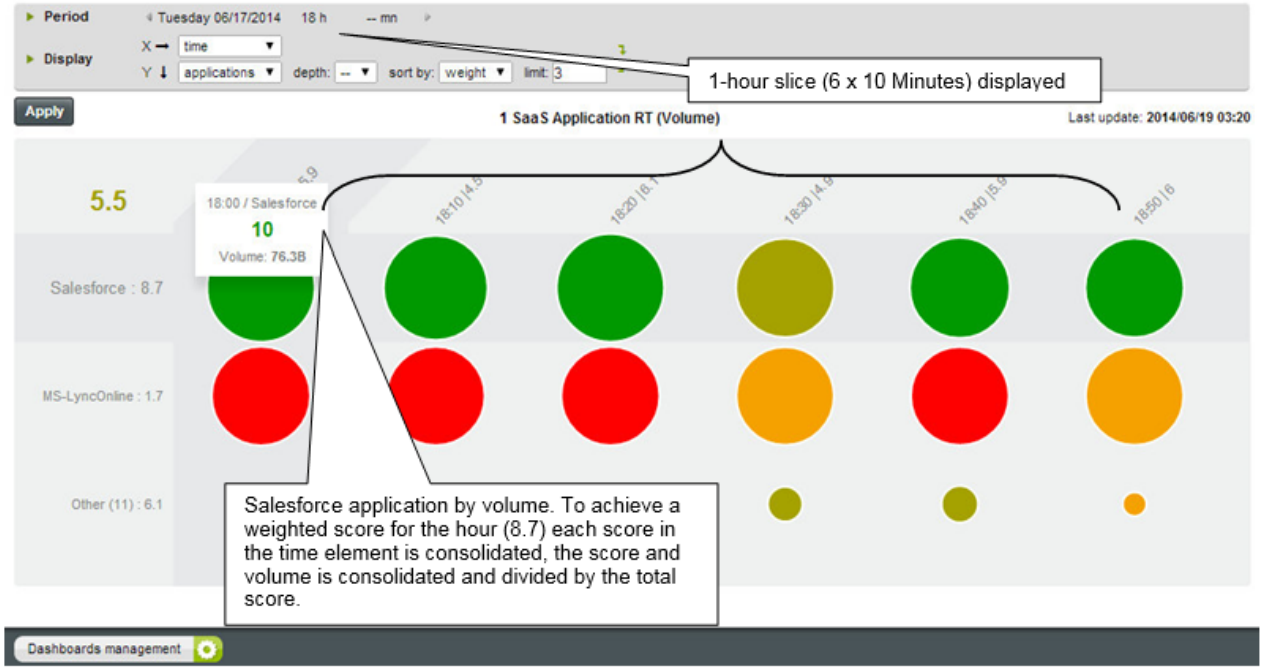


Figure 35 – Example of Application Score over an hour

30 CALCULATION AND METHODOLOGY FOR A SITE

The same calculation method is used as above to attain the weighted score for per site, for example in Figure 36 notice that we have a different display (X and Y) and a different set of results. The scorecard displays application response times, over a 24-hour period for two sites in Paris.

The Paris 10G/K site was given an overall weighted score of 4.5.

- Every applications' weighted score for a 24 hour period was aggregated
- Multiplied by its volume for 24-hours
- Finally this combined total is divided the sites total volume over the 24 hour period

Figure 36 – Applications sorted by weight (volume)

As presented, these elements are aggregated to achieve the result. All calculations take into account three elements regardless of the X and Y display. *Time, Applications and Sites.*

31 DETERMINING THE COMBINED SITE SCORE

The combined site score (displayed in orange) uses the same method of aggregation as shown previously but take into consideration the number of sites used for you scorecard.

32 CIRCLE POSITION RELEVANCE BY WEIGHT VS BY SCORE

Using the "good" and "bad" quality indicators previously mentioned, it is easy to identify between those applications performing smoothly and those with problems. However, in contrast to display by *score*, the display by *weight* circle arrangement is quite different. Notably we can see that an application (circle) position is not relative to its score but comparative to its volume, visible from left to right.

Note: Circles are represented based on a logarithmic scale.

33 WEIGHTED AVERAGE SCORE OVERALL SITE CALCULATION

$$\frac{\text{Score}_1\,(\text{site}_1) \times \text{Weight}_1\,(\text{volume or connection site 1}) + \text{Score}_2\,(\text{site}_2) \times \text{Weight}_2\,(\text{volume or connection site 2}) + \ldots\ \text{Score}_n \times \text{Weight}_n}{\text{Weight1 (volume or connection site 1)} + \text{Weight}_2\,(\text{volume or connection site 2}) + \ldots\ \text{Weight}_n}$$

= Overall combined site weighted score

6 UMT – Sites and Categories

6.1 INTRODUCTION

Streamcore makes service management easy and flexible by providing all information available through a Unified Mapping Tree™ (UMT):

- Whether this information is located on the SGM (statistics or configuration database) or on a StreamGroomer (real-time statistics)
- Whether this information is related to a site equipped with a StreamGroomer appliance or without

Streamcore's unique technology provides a flexible drill-down approach ranging from high-level business-oriented views to very granular troubleshooting statistics. Streamcore solutions present services in a business-oriented, logical view mapped to the IT organization, to make the most relevant information available to users, regardless of how many StreamGroomer appliances are deployed or their locations. For instance, hundreds of sites can be managed and grouped per business unit, even if appliances are only installed at the main corporate and regional data centers.

All the operations on the Unified Mapping Tree are performed after having selected the "Services" tree menu:

The structure of the Unified Mapping Tree can be divided into 3 kinds of objects:

- Category (group of sites)
- Site
- Per site rules tree (network, application, VoIP/Video rules)

This chapter describes:

- how to manage categories (chapter 6.2)
- how to manage sites (chapter 6.3)
- how to search a site or a category (chapter 6.4)

6.2 CATEGORIES PROVISIONING

6.2.1 Introduction

In order to ease the selection of several sites with similar properties (in the tree menu, in StreamReport…) or perform statistics consolidation, it is possible to assign one or several **categories** to a site.

Categories are grouped per **type**, for instance geographic type (country, region…) or organization type (data center, branch office…). Before creating categories in the tree menu, it is therefore first necessary to define all the categories types.

Hierarchical categories can be defined, especially when many categories have to be provisioned within a single type. For instance, geographic categories can be divided into continents types and then sub-divided into countries categories.

In the example below, two types are defined: "organization" type and "geographic" multi-level type.

Type	Categories	
Organization	Data center	
	Branch office	
	Internet access	
Geographic	US	East
		West
	EMEA	France
		Germany
	Asia	Japan

When all types and categories are configured, **a site can be associated with a single category for each type**. In the example above, a site could be a "Branch Office" in "US>East", or a "Data Center" in "EMEA>Germany".

The category type used to classify sites in the tree menu can be selected in the upper frame:

6.2.2 Parameters

To manage categories associated to a category type, select the category type in the upper frame. By default, there is a single category type and therefore the type selector is hidden.

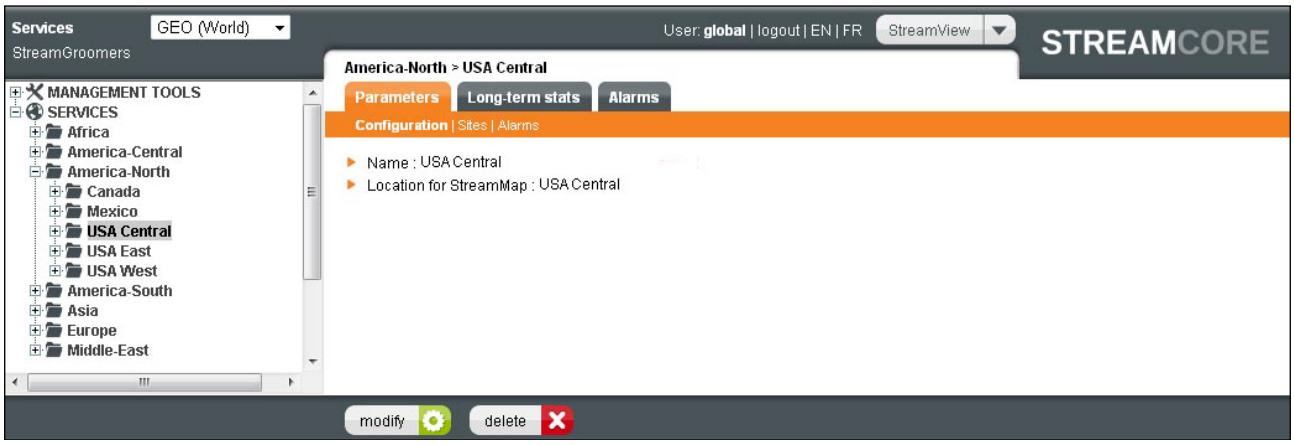


Figure 37 – Category management

The parameters for a category are displayed by clicking on the *Parameters>Configuration* or *Parameters>Sites* tab.

Parameter	Description / Values
Name	Category name. It must be unique (there cannot be two categories with the same name belonging to 2 different category types).
Location for StreamMap	(Optional). This parameter is required to locate a category in StreamMap.
List of sites	Sites related to the category. The list can be displayed directly in the tree, or by clicking on the category and selecting the **Parameters – Sites** sub-tab.

6.2.3 Add/Modify/Delete Operations

34 ADD A CATEGORY

To add a category:

1. Right-click on **SERVICES**. Select "**Add… → Category**"
2. Enter the category name and click on the **Submit** button

Note: In order to add a sub-category, right-click on the upper category and perform the same operations.

35 MODIFY A CATEGORY NAME

To modify a category name:

1. In the tree menu, click on the category and select the *Parameters - Configuration* sub-tab
2. Click on the **Modify** button, enter the new name and click on the **Submit** button

36 DELETE A CATEGORY

To delete a category:

1. In the tree menu, click on the category and select the *Parameters - Configuration* sub-tab
2. Click on the **Delete** button

Note: In order to delete a category, there must not be any site assigned to the category.

37 ASSIGN/REMOVE SEVERAL SITES RELATED TO A CATEGORY

To assign or remove several sites related to a category:

1. In the tree menu, click on the category and select the *Parameters - Sites* sub-tab
2. Assign/remove sites related to a category
3. Click on the **Submit** button

Note: A single site can be directly assigned to a category by modifying its parameters (see chapter 6.3.3).

6.2.4 Summary and Management

38 CATEGORIES SUMMARY

In order to get a summary and to manage category types, open the **MANAGEMENT TOOLS** and click on **Categories management** in the tree menu.

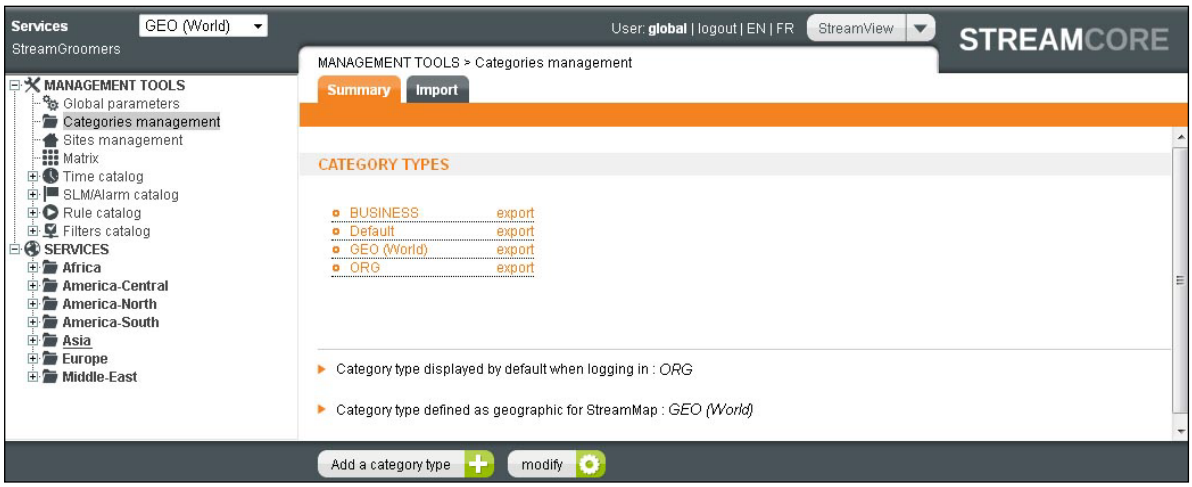


Figure 38 – Categories types' management screen

Note: A "default" category type is created for any new database.

To change the category type to be displayed in the tree menu by default when logging in, or the category type to be used in StreamMap:

1. From the **Categories management** screen, click on the **Modify** button
2. Choose the category type and click on the **Submit** button

39 CATEGORY TYPE PARAMETERS

The parameters for a category type are:

Parameter	Description / Values
Name	Category type name. It must be unique.
List of categories	Categories related to the category type. The list can be displayed directly in the tree by selecting the category type in the upper frame, or by clicking on the category type in the **categories management** screen.

40 ADD A CATEGORY TYPE

To add a new category type:

1. From the **Categories management** screen, click on the "Add a category type" button.
2. Select one of the following options:

- Empty category type: to create a type without any categories
- Predefined category type: to create a type (ORG, GEO, ACCESS…) with predefined categories

3. Click on the **Submit** button to apply the changes

41 MODIFY A CATEGORY TYPE NAME

To modify the name of a category type:

1. From the **Categories management** screen, click on the category type
2. Click on the **Modify** button, enter the new name and click on the **Submit** button

42 DELETE A CATEGORY TYPE

To delete a category type:

1. From the **Categories management** screen, click on the category type
2. Click on the **Delete** button

Note: In order to delete a category type, there must not be any site assigned to any category defined for this type.

43 CATEGORIES EXPORT/IMPORT

A category type and its categories can be exported, and imported in another SGM database.

To export categories:

1. From the **Categories management** screen, click on export next to the category type
2. Save the file

To import categories:

1. From the **Categories management** screen, click on the *Import* tab

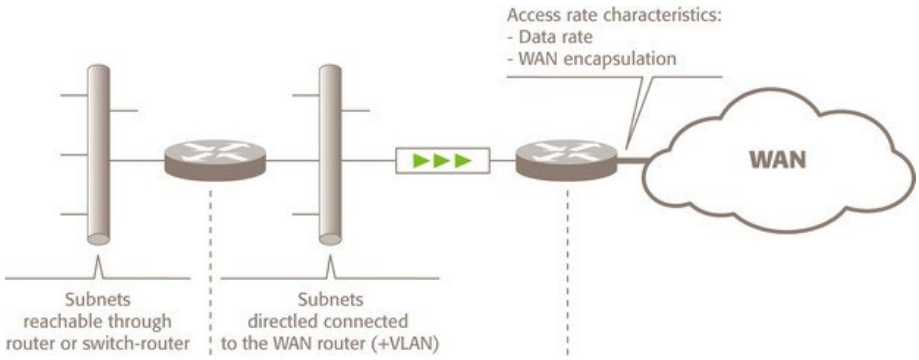
2. Enter the name of the new category type
3. Import a file previously exported and containing categories

6.3 SITES PROVISIONING

6.3.1 Introduction

The main parameters required per site are network parameters:

- access link characteristics
- subnets (directly connected to the WAN router or not)



Other parameters are available for visibility services (location in StreamMap, NetFlow, business hours reporting, VoIP/video measurements…).

6.3.2 Parameters

The **main** parameters of a site can be displayed by clicking on the *Parameters>Configuration* tab:

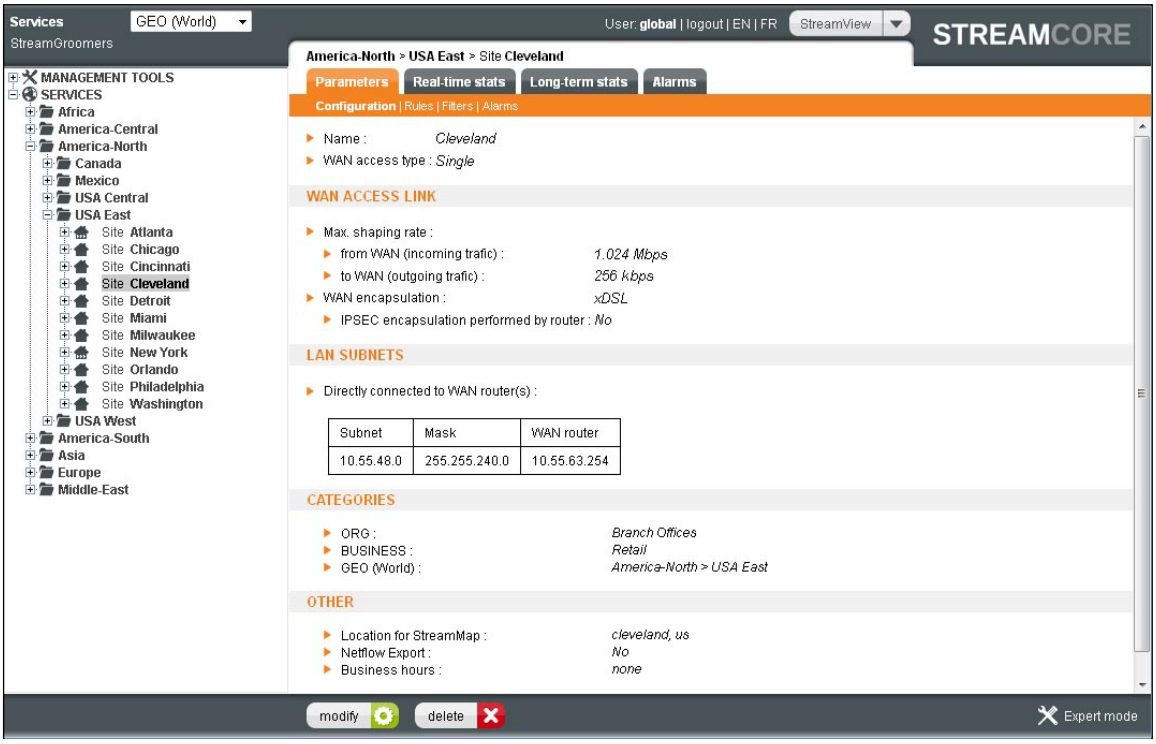


Figure 39 – Site selection in the tree menu

Parameter	Description / Values	
	Site with a StreamGroomer	Site without a StreamGroomer
Access link parameters		
WAN access type	The possible values are: - Single - Redundant Active/Passive - Redundant Active/Active (see chapter 7.3 on access link rules to learn more about these options)	
Backup link management	If the Access Type parameter is set to "Redundant Active/Passive" or "Redundant Active/Active", then this parameter is displayed and activates: - automated detection of an access link availability by an active probe or SNMP - automated QoS backup policy and new traffic classification in case an access link fails	*Not applicable*
Management of the 2 access links	If the Access Type parameter is set to "Redundant Active/Active", then this parameter is displayed and can be set to: - Aggregate: a single access link rule is used in the rules tree (for instance when per packet or per session load balancing is enabled on WAN routers) - Independent: 2 independent access links are used in the rules tree (for instance when per subnet or community load balancing is enabled on WAN routers)	*Not applicable*
Access link characteristics: max shaping throughput + WAN encapsulation	The max shaping throughput is used: - For visibility purpose: to compute the access link usage throughput - For performance control purpose: to schedule traffic and prevent inbound/outbound congestion on the access link The WAN encapsulation is used to take into account the frame format when scheduling traffic. (see chapter 7.3 on access link rules to learn more about these options)	
Subnet parameters		
Subnet + Mask + VLAN + WAN router	When defining subnets associated with the site, it is key to distinguish subnets: - directly connected to WAN router (s): these subnets will be used by the SG to identify local traffic, and when provisioning grooming rules. These subnets will also be used on remote StreamGroomers to identify this site traffic. - through other LAN router or switch-router: these subnets will only be used on remote StreamGroomers to identify this site traffic.	When no StreamGroomers are deployed on the site, it is not mandatory to distinguish subnets connected directly or not to the WAN router, and to define VLAN. All subnets are only used on remote StreamGroomers to identify this site traffic.
Categories		
List of categories	One category can be selected for each category type	
Other parameters		
Location	Geographic address used to locate the site automatically in StreamMap	
NetFlow export	This parameter activates the NetFlow export for the site:	This parameters activates the NetFlow export for the site:

	- Total: all traffic classified in the access link rule - Per application: all traffic classified in terminal rules with the NetFlow export parameter set to yes - Audio / Video: all traffic classified in audio/video rules - Shaping other sites: all traffic classified in "Shaping other sites" rule	- Total: all traffic classified in the shaping rules - Per application: all traffic classified in terminal rules with the NetFlow export parameter set to yes
Business hours	Select a business hours profile (defined in Management tools). This information is only used by StreamReport when generating reports with business hours option. (see chapter 14.5 to learn more about Reporting business hours configuration)	
VoIP/Video measurements	This parameter activates: - the VoIP/Video measurements for rules with VoIP/Video measurements set to RTP+MOS, RTP or signaling - VoIP/Video sub-tabs in real-time or long-term statistics tab	Not applicable
Web caching	This parameter activates Web caching module	Not applicable

The **expert** parameters of a site are:

Expert parameter	Description / Values	
	Site with a StreamGroomer	**Site without a StreamGroomer**
Data Center	This parameter must be set to "Yes" for sites acting as a Data Center. The properties of Data Centers are: - Data centers are always displayed in StreamMap even if sites display is filtered with categories. - Statistics per category is available in the "Long-term stats" tab of the site. - The "Active Control" parameter only impacts the local access link scheduling (not grooming or shaping rules scheduling, which is controlled by branch offices "Active Control" parameter). - The "Automated filter direction inversion" parameter is set to "Yes" if a Shaping other sites rule is created.	Not applicable
Active Control	This parameter activates: - Data Center site: scheduling of access link rules only. - Other site: scheduling of all network rules in the site tree, and scheduling of grooming rules on Data Center sites.	This parameter activates the scheduling of shaping rules on Data Center sites
LAN inventory tools	This parameter activates the "Active discovery" and "Host analysis" sub-tabs of the "LAN inventory" tab on the site.	Not applicable
Comments	This parameter is used to add any kind of comments per site.	

6.3.3 Add/Modify/Delete Operations

44 ADD A SITE

To add a site:

1. Right-click on SERVICES. Select "Add… → Site"
2. Enter the information related to the site
3. Click on the **Submit** button

Note: In order to add a site directly into a category, right-click on the category and perform the same operations.

45 MODIFY A SITE

To modify a site:

1. In the tree menu, click on the site and select the *Parameters - Configuration* tab
2. Click on the **Modify** button, enter the new parameters, and click on the **Submit** button.

46 DELETE A SITE

To delete a site:

1. In the tree menu, click on the site and select the **Parameters** tab
2. Click on the **Delete** button

Note: To delete a site associated with a StreamGroomer, the StreamGroomer must be deleted first.

6.3.4 Summary and Management

47 INTRODUCTION

In order to get a summary of sites configuration or make mass configuration changes, open the **MANAGEMENT TOOLS** in the tree menu, click on **Sites management** in the tree menu. The following parameters can be displayed or updated:

Parameters	Summary tool	Mass configuration change tools	
		Set parameters tool	Import tool
Network Parameters			
WAN access type	-	-	Yes
Backup link management	-	-	Yes
Access link characteristics: max shaping throughput + WAN encapsulation	Yes	-	Yes
Subnet + Mask + VLAN + WAN router	Yes	-	Yes
Main Parameters			
Categories	Yes	-	Yes
Location	Yes	-	Yes
Subnet analysis	Yes	-	-
NetFlow export	Yes	Yes	Yes
Business hours	Yes	Yes	Yes
VoIP/Video measurements	Yes	Yes	Yes

Web caching	Yes	Yes	Yes
Expert Parameters			
Active LAN inventory tools	Yes	Yes	Yes
Data Center	Yes	Yes	Yes
Active Control	Yes	Yes	Yes
Comments	Yes	-	Yes

48 SITES SUMMARY

In order to display a summary of the configured sites and their properties:

1. From the **Sites management** screen, click on the *Summary* tab
2. (Optional) Select a subset of sites by choosing categories, and select the information to be displayed
3. Click on the **Submit** button

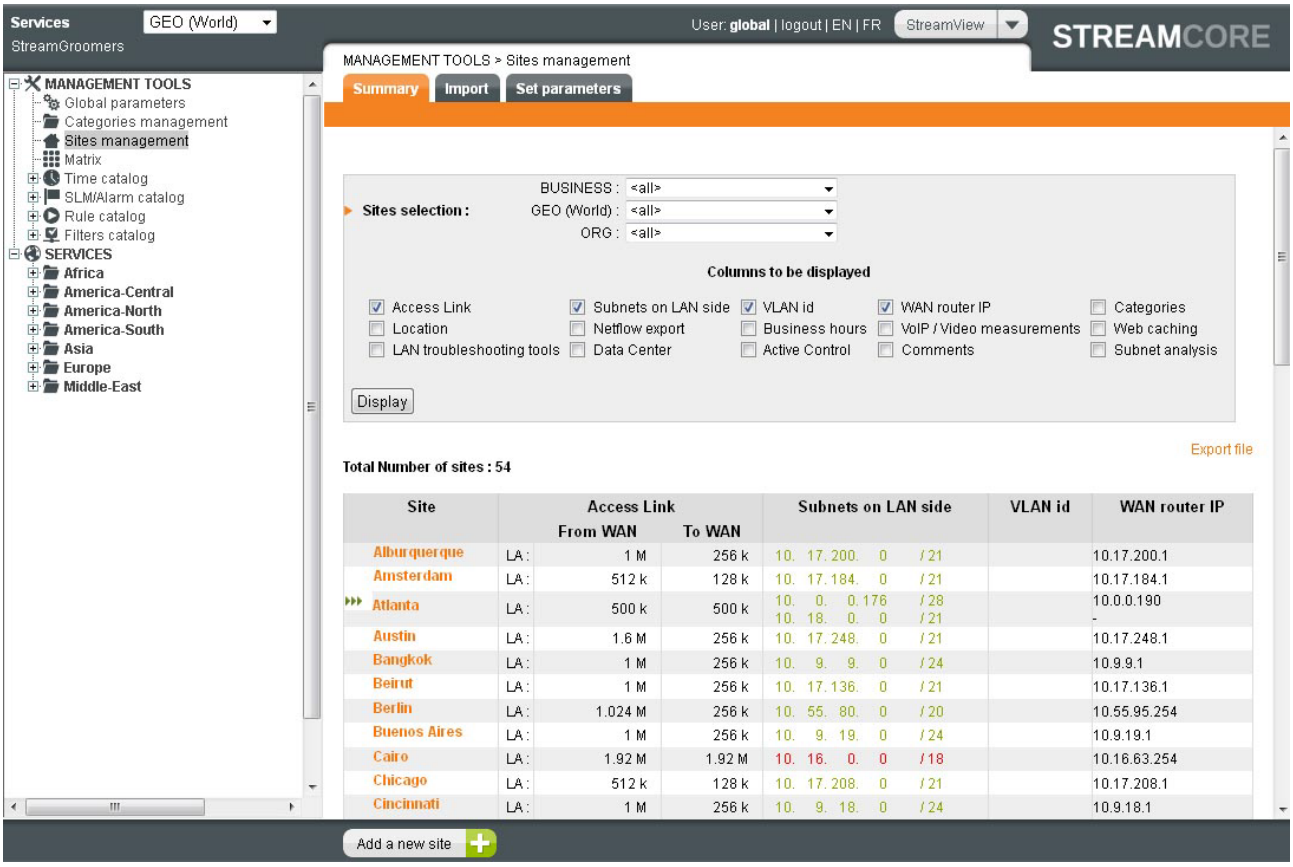


Figure 40 – Site summary

Note: The "Subnet Analysis" option will automatically check if there are overlapping subnets between the sites. Sites with subnets included in or overlapping with subnets defined for other sites will be displayed in red.

49 SET PARAMETERS

Mass configuration changes can be performed on a set of sites for the following parameters:

1. **Site main parameters:**

- NetFlow export

- Business hours
- VoIP/video measurements
- Webcache parameters

2. **Site expert parameters:**

- Data Center
- Active Control from data centers
- LAN inventory tools

The steps to follow are:

1. From the **Sites management** screen, click on the *Set parameters* tab
2. Select sites or a category
3. Define the parameters to be sent
4. Click on the **Apply** button

50 SITES EXPORT/IMPORT

Instead of managing sites one by one directly in the Graphical User Interface, it is possible to perform several operations at once by using the import/export feature. The following operations are available:

- Site creation
- Site characteristic modification

Note: To obtain a correct page layout when the file is opened using Microsoft Excel, you may need to launch the application and then open the file using the **File** > **Open** (Ctrl + O) command. Columns are separated by commas in the CSV format.

CSV FILE STRUCTURE

The CSV file is structured in 4 blocks of lines for each site:

- Configuration: Single line containing all parameters (except access links, subnets, categories)
- Access links: Single or two lines containing per access link parameters
- Subnets: One line per subnet parameters
- Categories: One line per category

	SiteName	AccessType	BackupMana	accessLink	rateDownloa	rateUpload	frameForma	encryptedW	encryptionA	subnetIP	maskIP	vlanId	directlyConn	WANIpRoute	category	Map
# Agence1 configurat	Enter the site name in the line below															
	Agence1	S	no													brest: fi
# Agence1: access lin	Enter the access link parameters in the line below (data rate must be defined in Kbit/s) (possible values for frameFormat are : xDSL - LL - ATM - Ethernet - Transparent)															
				AL1	1000	1000	xDSL									
				AL2	10000	10000	xDSL									
# Agence1: subnets	Add a line per subnet and enter the subnet parameters (set the directlyConnected field to Yes if the subnet is directly attached to the WAN router)															
										10.0.96.0	255.255.255.0		yes	10.0.96.39		
										10.0.98.0	255.255.255.0		yes	10.0.98.39		
# Agence1: category	Add a line per category and enter the category to which the site belongs (the category must have been defined in StreamView previously)															
															Internet Access	
															France	
#																

	Line Block	Column Name	Specific Values
Site name	Configuration	SiteName	-
Network Parameters			
WAN access type	Configuration	AccessType	S (Single) AA (redundant Active-Active) AP (redundant Active-Passive)

Backup link management	Configuration	BackupManagement	Yes, No
Access link name	Access links	accessLink	AL1, AL2
Access link data throughput	Access links	rateDownload, rateUpload	Numeric value in Kbps
Access link frame format	Access links	frameFormat	xDSL, LL, ATM, Ethernet, Transparent
Access link with IPSec encapsulation	Access links	encryptedWAN, encryptionAlgorithm	Yes, No AES, DES/3DES
Subnet + Mask	Subnets	SubnetIP, MaskIP	xx.xx.xx.xx
VLAN	Subnets	vlanId	Numeric value
Directly connected subnet or not	Subnets	directlyConnected	Yes, No
WAN router IP address	Subnets	WANIpRouter	xx.xx.xx.xx
Main Parameters			
List of categories	Categories	Category	-
Location	Configuration	Map	-
NetFlow export	Configuration	NetFlowExport	Yes, No, Per application, Audio-video, Other sites
Business hours	Configuration	Biz_hour	-
VoIP/Video measurements	Configuration	VoIP/Video	Yes, No
Web caching	Configuration	Webcaching	Yes, No
Expert Parameters			
Data Center	Configuration	DataCenter	Yes, No
Active Control	Configuration	ActivControl	Yes, No
LAN inventory tools	Configuration	lanTool	Yes, No
Comments	Configuration	comment	-

51 EXPORT SITES CONFIGURATION

To export sites configuration:

1. From the **Sites management** screen, click on the *Summary* tab
2. (Optional) Select a subset of sites by choosing categories, and select the information to be displayed
3. Click on the **Submit** button
4. Click on the **Export file** button. Save the file locally.

52 IMPORT SITES CONFIGURATION

To add or update sites defined in a CSV file:

1. From the **Sites management** screen, click on the *Import* tab
2. Click on **Browse** to select the CSV file to be imported and click on the **Import file** button.
3. Wait until the file is completely parsed.

At the end of the parsing process, a message will be displayed describing the final results — either that the operation has been successful or that an error has occurred (bad category name…).

Note: All site parameters can be modified by CSV-file import / export, **except the site name**. Indeed, the site name is used as the identifier during the parsing process to check if the site already exists in the database:

If it exists, then the parsing process compares existing parameters with imported file parameters: if differences are detected (subnet change, new data throughput …), the modifications are applied.

If it does not exist, the parsing process creates a new site.

Note: 5.3 and 6.0 releases CSV file formats are not compatible. For instance, a 5.3 CSV file cannot be imported on a 6.0 release SGM.

6.4 SITE / CATEGORY SEARCH

To have a direct access to a site (or a category), the search engine can be used:

1. Click on **SERVICES** in the tree menu and select the *Home* tab.
2. Enter the site or category name and click on **Go** to drill down to the site.

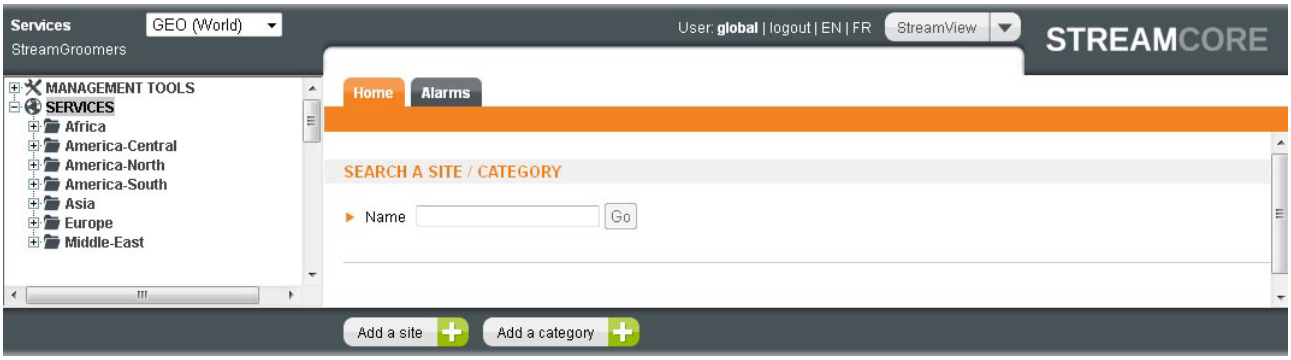


Figure 41 – Site or category search engine

6.5 NETFLOW COLLECTION

6.5.1 Introduction

The SGM and SCO both have the ability to collect Netflow v5 and v9 tickets on StreamGroomers as well as third party devices. Netflow tickets contain data on IP network traffic as it enters or exits an interface, usually a router or switch. Analyzing these tickets can help you to understand network traffic source and destination flows, understand the root of network congestion, and discover the cause of bottlenecks.

When a data center equipped with a SG manages remote sites not equipped with StreamGroomers, the network administrator has a limited visibility on all the network traffic on the remote sites. For example, he cannot monitor the traffic that takes place between the remote sites.

One solution consists in using the routers of the remote sites as companions of the SG of the data center by activating their Netflow export capabilities. Once the SGM or SCO receives Netflow tickets from the remote devices attached to the remote sites, the network administrator is able to monitor and troubleshoot problems by consulting the long-term statistics of every remote site.

StreamView allows the network administrator to associate a network device to a managed site with an object called **external probe**. The network device must be able to send Netflow tickets to the SGM or the SCO. The traffic details reported by the external probe will be associated with the site on which the external probe is created.

Note: Not all devices support v5 and v9 Netflow. Check with your device supplier or manual for further information.

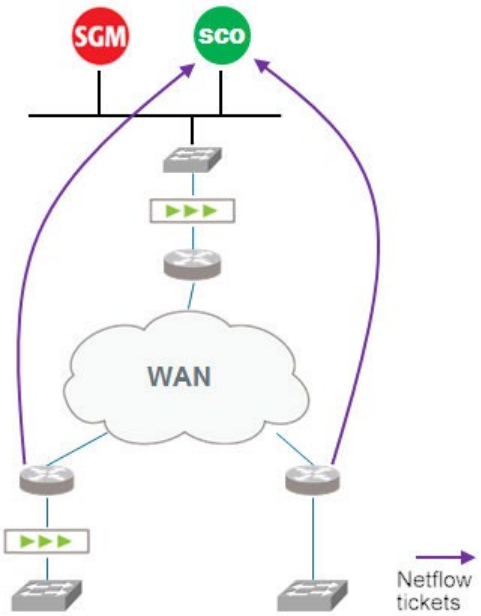


Figure 42 – Netflow ticketing

To implement netflow ticket collection, the following actions are required:

- Configure the network device to send Netflow tickets. Consult your software vendor manual or an experienced network engineer. Then provide the IP address of the SCO or SGM and the UDP port of the netflow collector service (SCO or SGM).
- On the SGM, associate the network device to an ***external probe*** object using the StreamView application.

Note: An external probe can be any network device except StreamGroomers. SG performance is not impacted when exploiting the Netflow feature.

6.5.2 Parameters

In StreamView, a network device is identified by a name and its IP address (for example a router IP address). In addition, a list of WAN network interfaces identifiers can be specified. This list allows identifying the direction of every packet (for example, for a router, from LAN to WAN or from WAN to LAN).

Parameter	Description / Values
Active probe	
Probe name	Enter an external probe name for example CiscoDTCNT_NYC1
IP Address	IP address of the network device (external probe)
WAN Interfaces Index	SNMP interface indexes (ifIndex) associated to the WAN interfaces of the network device (separated by comma). Enter an integer greater than 0.
UDP Port	Port of the Netflow collector of the SGM or SCO. Enter a value in the range 9991 and 9999. The value is optional. If the port is not specified, the product chooses a default port.

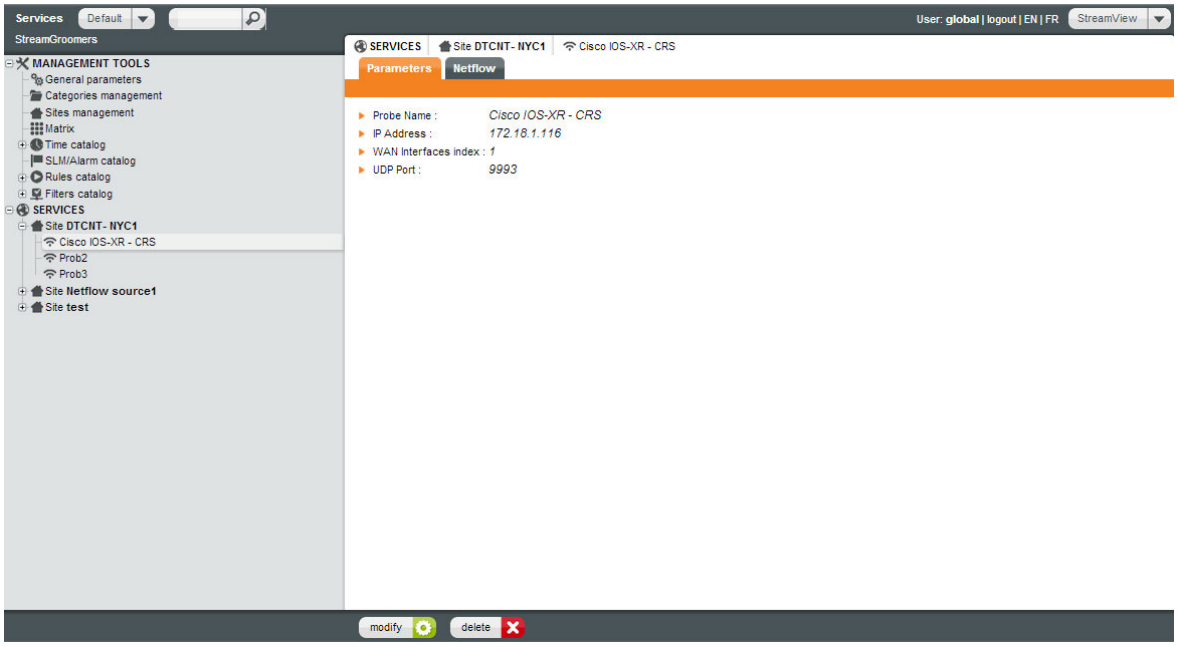


Figure 43 – External Probe Parameters

6.5.3 Add/Modify/Delete Operations

An external probe is declared in the "Services" section for a given site. Several external probes can be added to a site.

53 ADD AN EXTERNAL PROBE

1. Select the *Site* then right-click and select *External Probe*.
2. Enter probe parameters
3. Click **Submit**

54 MODIFY AN EXTERNAL PROBE

1. Select the *Site* then right-click and select *External Probe*.
2. Click **Modify**
3. Enter modifications

55 DELETE AN EXTERNAL PROBE

1. Select the *Site* then right-click and select *External Probe*
2. Click **Delete**
3. Confirm deletion click **OK**

Or

1. Select the *Site* then select *External Probe*
2. Click the red **delete button** at the bottom of the display pane
3. Confirm deletion click **OK**

For information regarding the Netflow, tab and sub-tabs refer to Netflow Visibility Services on p149

7 UMT – Per Site "Rules Tree"

7.1 INTRODUCTION

Streamcore makes service management easy and flexible by providing all information available through a Unified Mapping Tree™:

- Whether this information is located on the SGM (statistics or configuration database) or on a StreamGroomer (real-time statistics),
- Whether this information is related to a site equipped with a StreamGroomer appliance or without.

All the operations on the Unified Mapping Tree are performed after having selected the "Services" tree menu:

The structure of the Unified Mapping Tree can be divided into 3 kinds of objects:

- Category (group of sites)
- Site
- Per site rules tree (network, application, VoIP/Video rules)

This chapter describes:

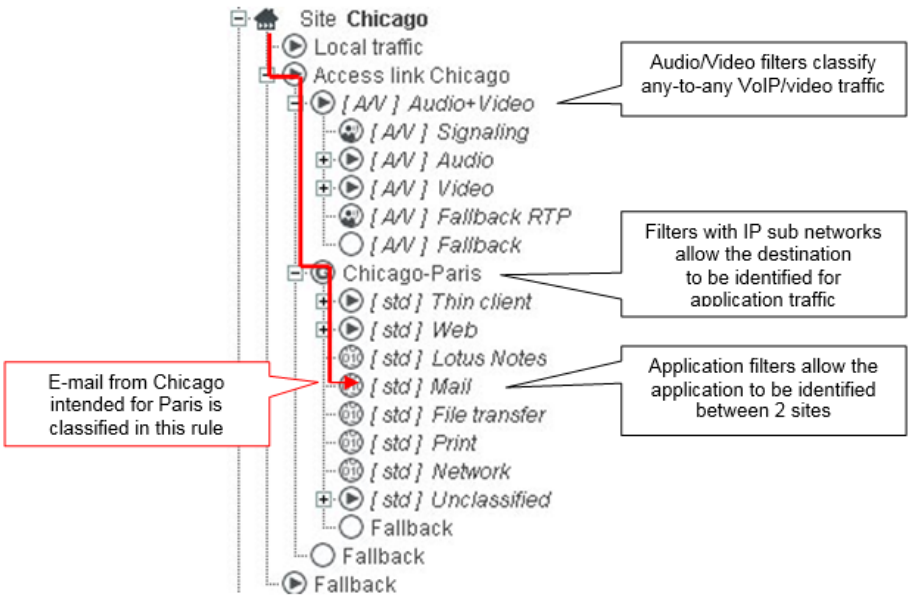
- How the rules tree is structured (chapter 7.2)
- Access link rules (chapter 7.3)
- Shaping/Grooming rules (chapter 7.4)
- Intermediate, data and audio/video rules (chapter 7.5)
- Group of rules (chapter 7.6)

7.2 RULES TREE OVERVIEW

7.2.1 Principle

56 TOP DOWN CLASSIFICATION

In order to identify the different types of traffic, a tree of rules is defined and **filters** are associated with each rule, so as to ensure the classification of the traffic through the tree hierarchy. Traffic passes through the branches **from top to bottom**, and is classified according to a rule as soon as it meets the criteria imposed by the filters associated with the rule. It passes through the tree hierarchy until it reaches a terminal rule (leaf rule). **Therefore, the positional order of the rules is very important.**



The definition of a coherent classification is important for Monitoring & Reporting and also for active performance control and optimization.

When navigating through the tree for a site, the user is virtually positioned within the site. This concept is fundamental to understand the concepts of local and remote locations as used on the screens. All references to "local" designate the site within which the navigation is taking place.

57 TYPES OF RULE

The tree hierarchy for a site can contain:

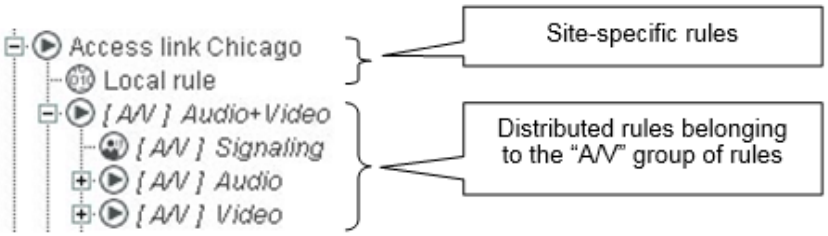
- Site-specific rules

  Site-specific rules are valid only for the concerned site. Such rules can be for instance an access link rule, shaping/grooming rules to match traffic exchanged between 2 sites, or an application rule defined locally to match a specific traffic.

- Rules distributed from a reference group of rules

  A distributed rule must necessarily be part of a distributed instance of a Group of rules. It appears in italics in the rules tree hierarchy for the site, and starts with the name of the reference Group of rules in square brackets. Groups of rules are usually defined to match application or audio/video traffic, and distributed across a set of sites to ensure a homogeneous classification.

The addition, modification, or deletion of a distributed rule must necessarily take place in the reference Group of rules defined in the **MANAGEMENT TOOLS > Rules catalog**, and is applied automatically to all of the distributed instances. See chapter 7.6 to learn more.



Different types of rules can be defined in the tree, with different properties such as automated filters or the capability to be included or not in a group of rules.

		DESCRIPTION	FILTERS	GROUP OF RULES
	Local Traffic	Rule used to classify all traffic going through the StreamGroomer and which is not exchanged over the WAN.	Automated (inherited from subnets defined on the site)	No
	Access link	Rule associated with all the traffic exchanged over the WAN. There can be one or 2 access link rules on a site. Specific performance measurements can be enabled, as well as backup management policies.	All IP (for a single access link) Other filters can be defined	No
	Shaping	Rule associated with the traffic exchanged between two sites, one of them being equipped with a StreamGroomer. Network performance measurements can be enabled.	Automated (inherited from subnets defined on the remote site)	No
	Grooming	Rule associated with the traffic exchanged between two sites equipped with a StreamGroomer. Advanced network performance measurements can be enabled. Advanced end-to-end optimization features can be enabled (compression, WAN load balancing…)	Automated (inherited from subnets defined on the remote site)	No
	Intermediate	Rule used to add a new level of classification into the tree to classify audio/video or application traffic. Such a rule can be used to perform statistics aggregation or to add a level of scheduling for QoS purpose. Such a rule can be included in a group of rules.	Custom filters (or automated filters inherited from sub-rules)	Yes
	Terminal data	Leaf rule used to classify application traffic. Application performance measurements are automatically computed, and specific performance control options are available. Such a rule can be included in a group of rules.	Custom filters	Yes

	Terminal audio/video	Leaf rule used to classify audio/video traffic. Audio/video performance measurements are automatically computed, and specific performance control options are available. Such a rule can be included in a group of rules.	Custom filters	Yes
	Fallback	Last rule in a tree for all traffic that has not been classified in upper rules. Such a rule can be included in a group of rules.	None	Yes

58 CLASSIFICATION CRITERIA

One or several filters can be defined per rule. In some cases, they are automatically defined (on a shaping or grooming rule for instance) or they can be inherited from sub-rules in case of an intermediate rule. For other types of rules, the custom classification criteria that can be provisioned when adding a filter are:

Level 2 (Ethernet header)	VLAN, MAC address
Level 3 (IP header)	IP address or subnet (remote and / or local) Protocol, ToS / DCSP field
Level 4 and above	UDP / TCP port or range of ports TCP Call direction
Level 5 and above	Layer 7 pattern marching URL for HTTP traffic, Common name for HTTPS traffic Codec or audio / video for RTP traffic

7.2.2 Rules Tree for a Site with a StreamGroomer

All of the traffic exchanged between the site and the WAN can be managed, because it passes through the StreamGroomer:

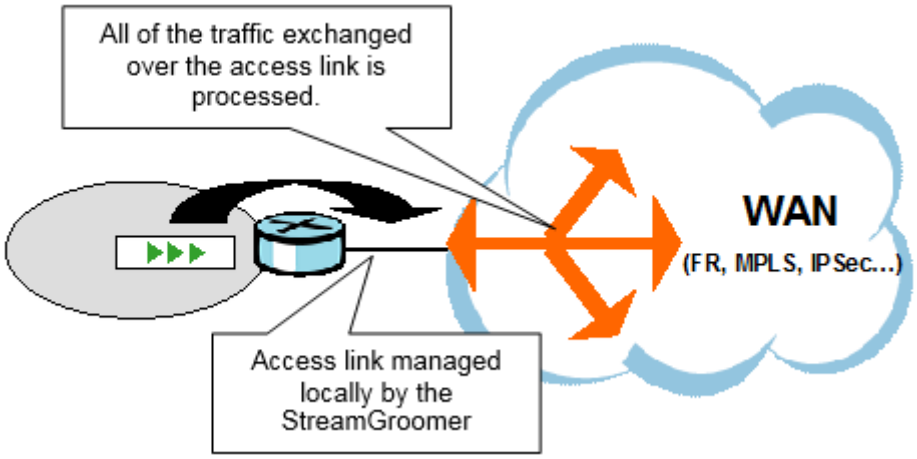
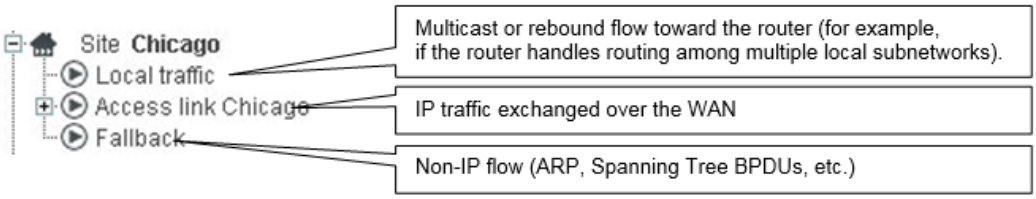


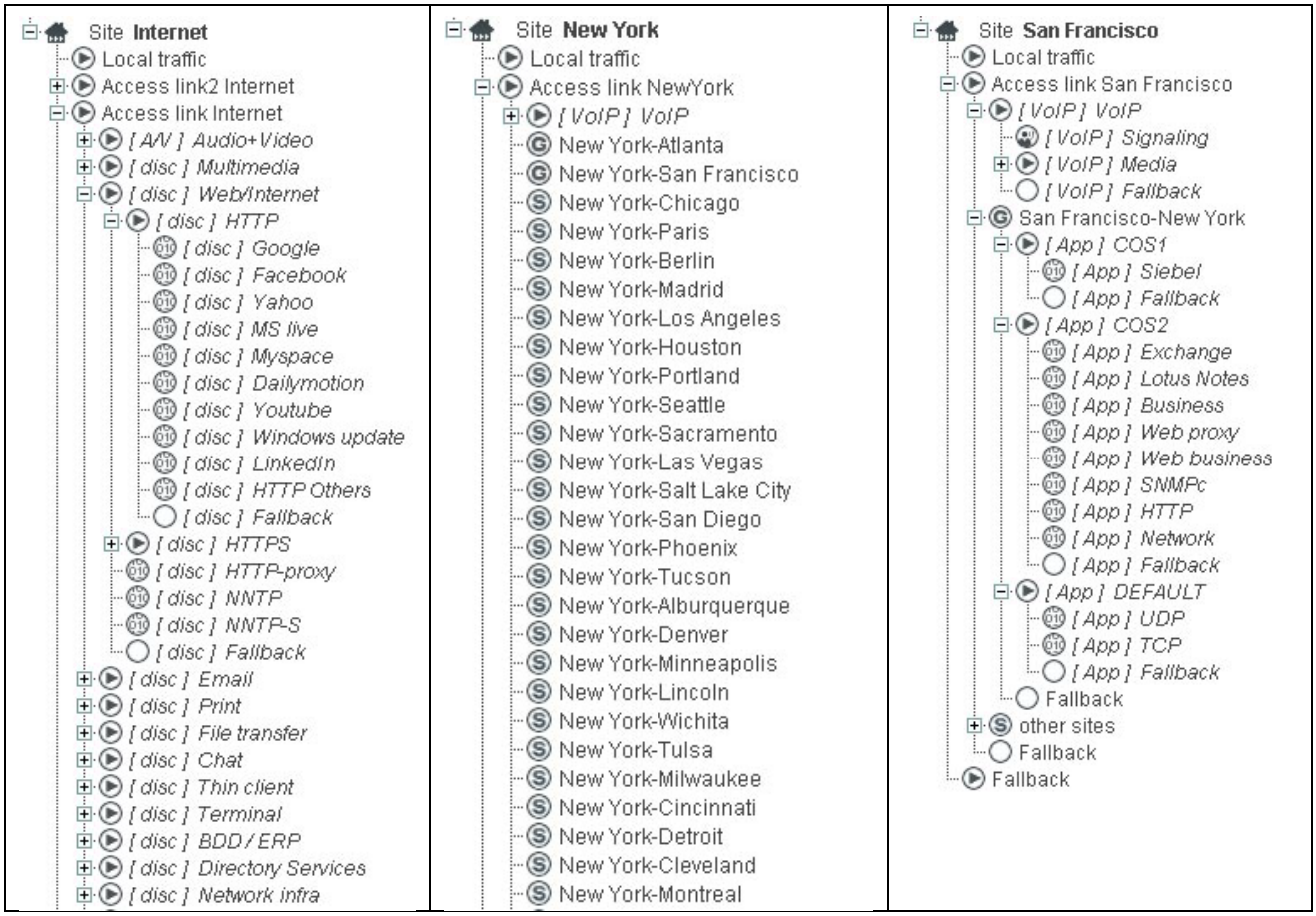
Figure 44 – Management of all traffic for a site with StreamGroomer.

The first level of the tree menu for a site with StreamGroomer is shown below.



Below the access link, the rules defined in the tree depend on the type of site. For an Internet access, application and audio/video rules will be defined directly, whereas for a data center or a branch office, shaping or grooming rules will also be provisioned to identify application traffic exchanged per remote site. The table below shows typical rules tree depending on the type of site:

Internet access	Data Center	Branch Office
All audio/video and application rules are defined directly below the access link rule. Multi-level classification can be defined to different types of traffic. Advanced classification can be defined for : • HTTP traffic (based on URLs) • HTTPS traffic (based on certificate info) The "traffic discovery" predefined group of rules can be used for instance.	Traffic must be must be classified per remote site: • Any-to-any VoIP/Video traffic must be classified in VoIP/Video rules configured directly below the access link rule. • Branch application traffic must be classified in application rules created below site-to-site rules (shaping, grooming) between a Data Center and a branch office.	Any-to-any traffic must be distinguished from the traffic exchanged with the Data Centers: • Any-to-any VoIP/Video traffic must be classified in VoIP/Video rules configured directly below the access link rule. • Data Center application traffic must be classified in application rules created below site-to-site rules (shaping, grooming). • Any-to-any application traffic is managed in the "Shaping other sites" sub-tree



7.2.3 Rules Tree for a Site without a StreamGroomer

The access link of a site without a StreamGroomer can be managed with Shaping rules from one or more StreamGroomers located at other sites. In this case, only the traffic exchanged with these sites will be displayed and managed.

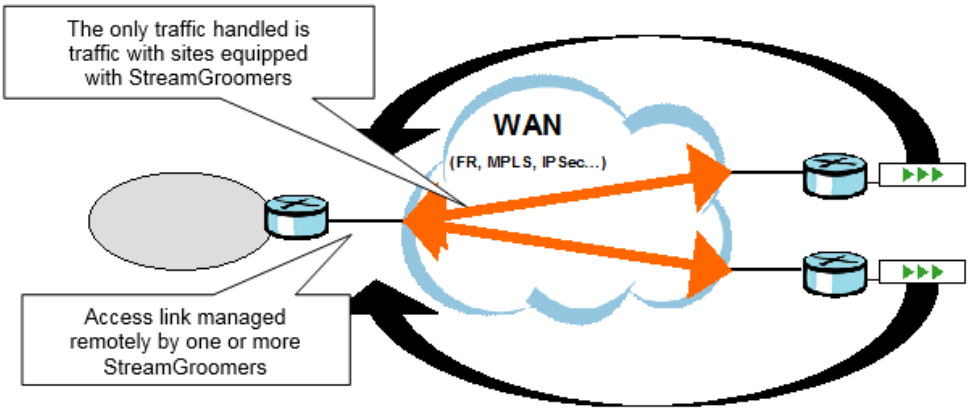
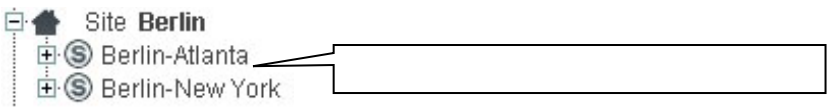
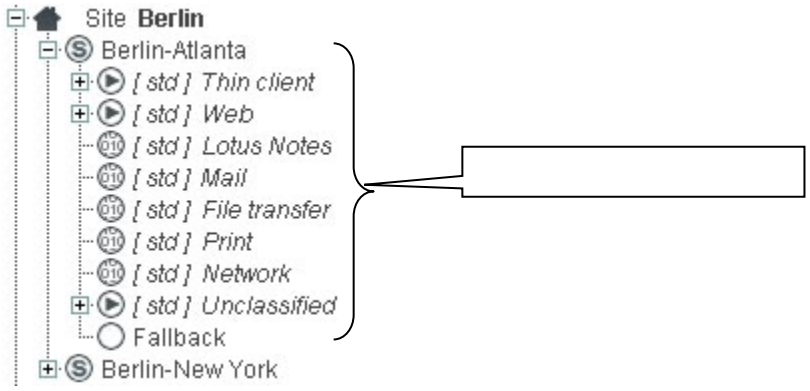


Figure 45 – Management of traffic over the access link of a site without StreamGroomer.

The first level of the tree menu for a site with StreamGroomer is shown below.



For a site without a StreamGroomer, only application traffic exchanged with the Data Centers must be considered (VoIP/Video traffic management is performed only for sites with StreamGroomers). Under each site-to-site shaping rule will be defined a tree of application data rules.



7.2.4 Rules Tree Summary

59 RULE PARAMETERS SUMMARY

To display a summary of the rules parameters (QoS action and parameters, visibility parameters…) within a rules tree, click on **SERVICES > … > Site xx**, and on the *Parameters – Rules* tab:

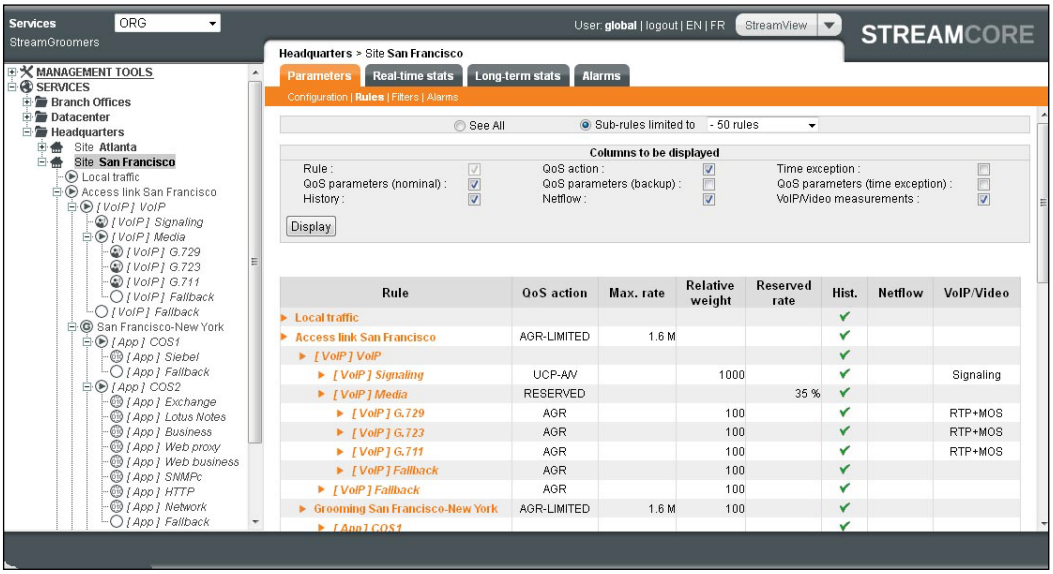


Figure 46 – Rule parameters summary on a site

60 FILTERS SUMMARY

To display a summary of the filters within a rules tree, click on **SERVICES > … > Site xx**, and on the *Parameters – Filters* tab:

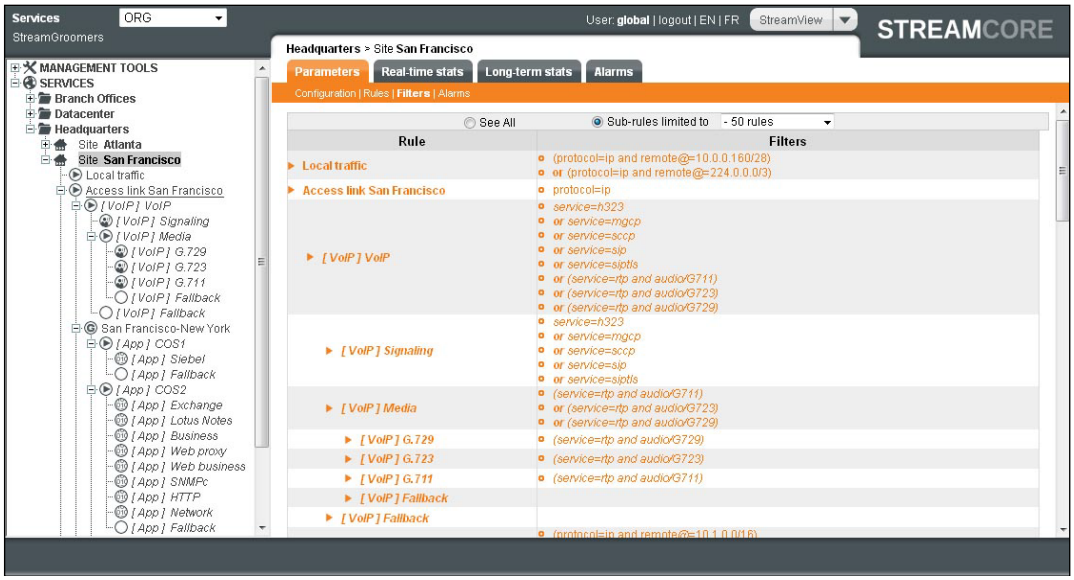


Figure 47 – Rule filters summary on a site

7.3 ACCESS LINK RULES

7.3.1 Introduction

Access link rules are present on sites with a StreamGroomer, and used to manage a local access link.

		DESCRIPTION	FILTERS
	Access link	Rule associated with all the traffic exchanged over the WAN. There can be one or 2 access link rules on a site. Specific performance measurements can be enabled, as well as backup management policies.	**All IP** (for a single access link) Other filters can be defined

Most properties of access link rules are inherited from network parameters defined on the site (see chapter 6.3.2). The recommended configuration on a site depending on the WAN access type is:

Site parameters WAN access topology	Access type	Backup Management	Management of the 2 access links
Single access link	Single	*Not applicable*	*Not applicable*
Two access links in active/passive configuration	Redundant active/passive	Yes	*Not applicable*
Two access links with per packet or per session (CEF) load balancing on the routers	Redundant active/active	Yes	Aggregated
Two access links with - per subnet or application load balancing on the routers or - Streamcore WAN load balancing	Redundant active/active	Yes	Independent

7.3.2 Parameters

The **main** parameters of an access link can be displayed by clicking on the *Parameters-Configuration* tab:

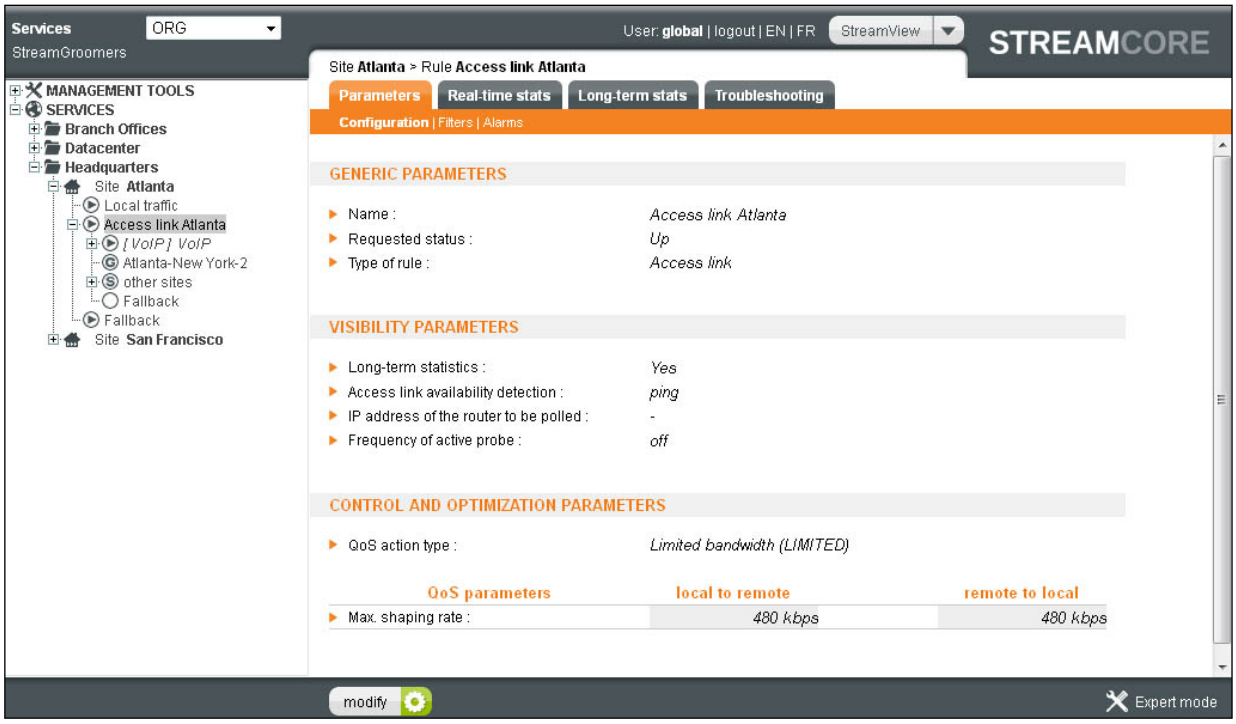


Figure 48 – Access link rule – Parameters

Parameter	Description / Values	
Generic parameters		
Name	(automatically inherited from the site name)	
Requested status	Up	
Type of rule	Access link	
Visibility parameters		
Long-term statistics	(default=Yes) To store or not long-term statistics for the rule	
Access link availability detection (see chapter 7.3.5)	Ping	SNMP
IP address of the router to be polled	IP address of provider egde router	IP address of WAN access router. Additional SNMP ifName and SNMP community parameters are required.
Frequency of the active probe	1, 2, 5, 10 seconds	10 seconds, 30 seconds, 1 min., 2 min.
Control and optimization parameters		
QoS action type	Limited bandwidth (LIMITED) (cannot be changed)	
Max. shaping throughput	(automatically inherited from the site network parameters, see chapter 7.3.4.1)	

The **expert** parameters of an access link are:

Expert parameter	Description / Values
Control and optimization parameters	
Throughput correction	% of the max shaping throughput (used mainly to shape inbound traffic)
WAN encapsulation	(automatically inherited from the site network parameters, see chapter 7.3.4.1)

IPSEC encapsulation performed by the router	

Note: Except access link availability monitoring or throughput correction parameters, it is not recommended to change any other parameters since all of them are inherited from the site parameters.

7.3.3 Filters

The filters associated with an access link can be displayed by clicking on the ***Parameters-Filters*** tab. By default an "All IP" filter is created to match all the IP traffic except the traffic classified in the "Local traffic" rule.

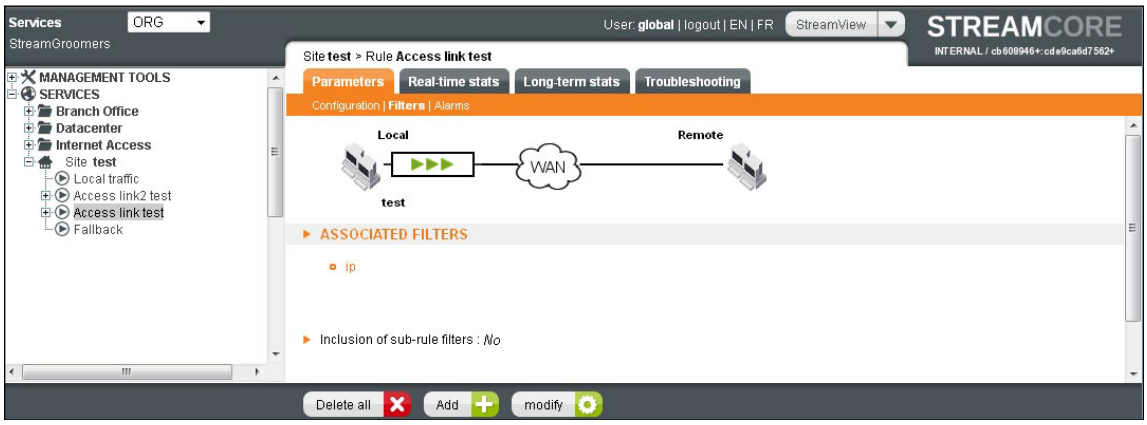


Figure 49 – Access link rule - Filters

Note: The only reason for updating access link filters is when 2 access links rules have been created and advanced classification per access link must be provisioned.

7.3.4 Add/Modify/Delete Operations

61 ADD AN ACCESS LINK

Access links rules are automatically created when adding a StreamGroomer to a site.

A single access link is usually created. The only case when two access links are created is when the access type on a site is set to "redundant active/active" and the access link management is set to "Independent".

The "Max. shaping throughput" and "WAN encapsulation" parameters on access link rules are automatically inherited from the site network parameters as follows:

Site parameters				Access link rule
Access type	*Access link Management*	*Access 1 data throughput + WAN encaps.*	*Access 2 data throughput + WAN encaps.*	*"Max. shaping throughput" and "WAN encapsulation" parameters*
Single	-	D kbps	-	D kbps
Redundant active/passive	-	D1 kbps	D2 kbps	D1 kbps (D2 kbps in backup mode)
Redundant active/active	Aggregated	D1 kbps	D2 kbps	D1 + D2 kbps (D1 or D2 in backup mode)
	Independent	D1 kbps	D2 kbps	rule1 shaping throughput = D1 kbps rule2 shaping throughput = D2 kbps

Note: In order to better manage congestion when applying QoS, -10% or -20% correction is automatically applied to the throughput shaping to incoming traffic (from WAN).

62 MODIFY AN ACCESS LINK RULE

To update access link parameters, click on **SERVICES> … >Site xx>Access Link xx** and then on the "Modify" button. Enter the parameters and click on the "Apply" button.

63 DELETE AN ACCESS LINK

Access links cannot be deleted.

7.3.5 Backup Link Management

An access link's availability can be monitored by the StreamGroomer for several purposes:

- Performance monitoring and SLA (see chapter 9.2.1.2)
- Backup link management (for StreamGroomers in Monitoring&Control mode)

In order to monitor an access link's availability for backup link management, 2 types of measurements can be used:

- Ping: an active probe can be launched by the StreamGroomer to measure the availability of the network link between the access router and the first service provider node (provider egde router in an MPLS environment for instance). Additional performance measurements are also available such as latency and packet loss (see chapter 9.2.1.2)
- SNMP Polling: the StreamGroomer can poll by SNMP the MIB II ifName parameter related to the router access link.

Note: The ping and SNMP polling traffic are launched from the StreamGroomer Administration Ethernet port. A default route must therefore have been configured for the ADMIN port (see chapter 4.2.4).

On a site with 2 access link topology, if the StreamGroomer detects that one of the access links is down, it will perform the following actions:

- Update the QoS shaping throughput according to the data throughput of the remaining access link
- (Option) Apply a backup QoS policy (see chapter 11.3.3.1)
- If 2 independent access link rules have been defined, reclassify the traffic in the remaining access link

Case 1: second WAN access link down	Case 2: main WAN access link down
	

Note: This reclassification of traffic in case of access link unavailability also applies if the StreamGroomer is in Monitoring mode.

7.4 SHAPING/GROOMING RULES

7.4.1 Introduction

Application traffic exchanged between 2 sites can be managed through two types of network rules:

		DESCRIPTION	FILTERS
	Shaping	Rule associated with the traffic exchanged between two sites, one of them being equipped with a StreamGroomer. Network performance measurements can be enabled (see chapter 9.2.1.2).	Automated (inherited from subnets defined on the remote site)
	Grooming	Rule associated with the traffic exchanged between two sites equipped with a StreamGroomer. An LMP (Link Management Protocol) is established between two StreamGroomers that are exchanging traffic under Grooming. When synchronized, this protocol has the following added-value: 1/ Network performance measurements (see chapter 9.2.1.2). 2/ Management of a window to control the total volume of data passing over the link. This flow control allows the StreamGroomers to adapt to changes of the data throughput (see chapter 11.2.4.2). 3/ Advanced end-to-end optimization features can be enabled (see chapter 12.1): Compression WAN load balancing	Automated (inherited from subnets defined on the remote site)

7.4.2 Parameters

64 SHAPING RULE PARAMETERS

The **main** parameters of a shaping rule can be displayed by clicking on the *Parameters-Configuration* tab:

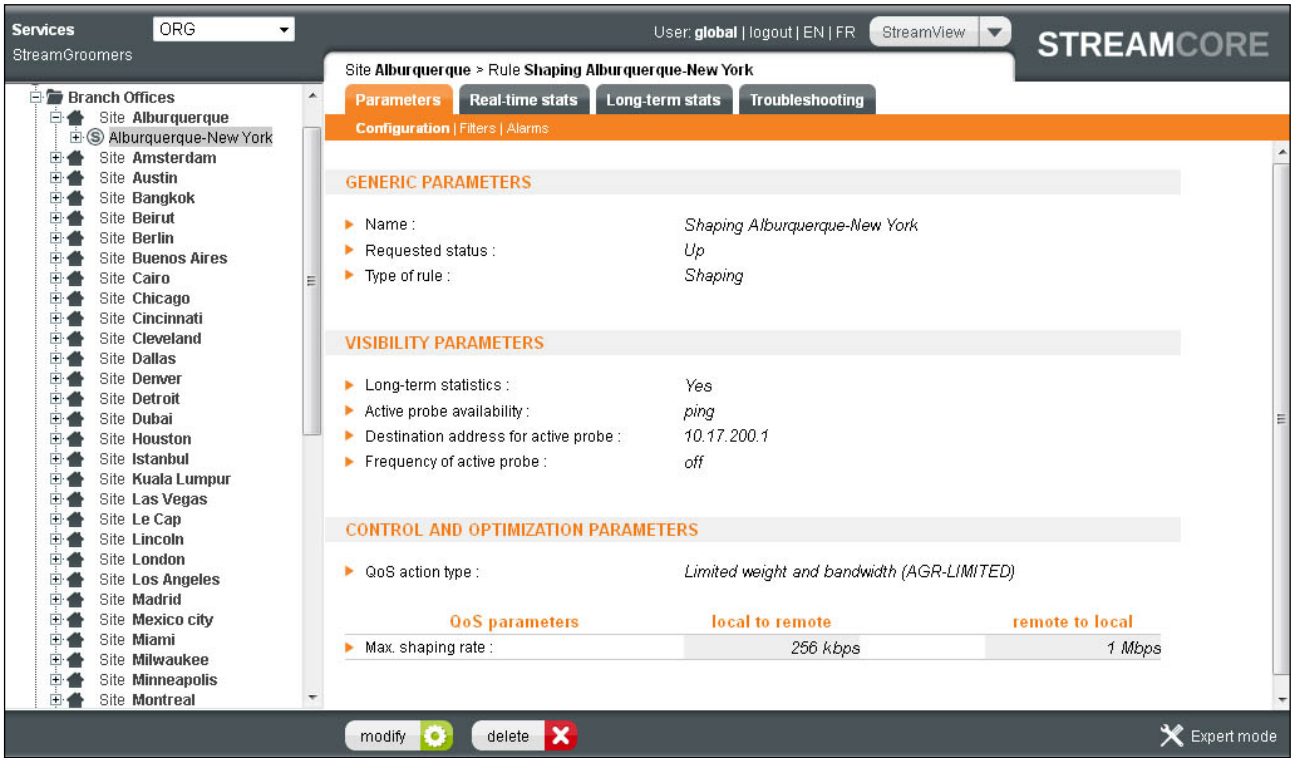


Figure 50 – Shaping rule - Parameters

Parameter	Description / Values
Generic parameters	
Name	(automatically inherited from the 2 sites name)
Requested status	Up
Type of rule	Shaping
Visibility parameters	
Long-term statistics	(default=Yes) To store or not long-term statistics for the rule
Active probe availability	Ping
Destination address for active probe	IP address of the remote WAN access router
Frequency of active probe	1, 2, 5, 10 seconds
Control and optimization parameters	
QoS action type	Limited weight and bandwidth (AGR-LIMITED) (cannot be changed)
Relative weight	(default value=100) This parameter is used to allocate bandwidth to the shaping rule if it competes for bandwidth on the local access link (displayed on a site with SG)
Max. shaping throughput	(automatically inherited from the 2 sites network parameters)

The **expert** parameters of a shaping rule are:

Expert parameter	Description / Values
Control and optimization parameters	
Throughput correction	% of the max shaping throughput
WAN encapsulation	(automatically inherited from the site network parameters)
IPSEC encapsulation	

65 GROOMING RULE PARAMETERS

The **main** parameters of a grooming rule can be displayed by clicking on the *Parameters-Configuration* tab:

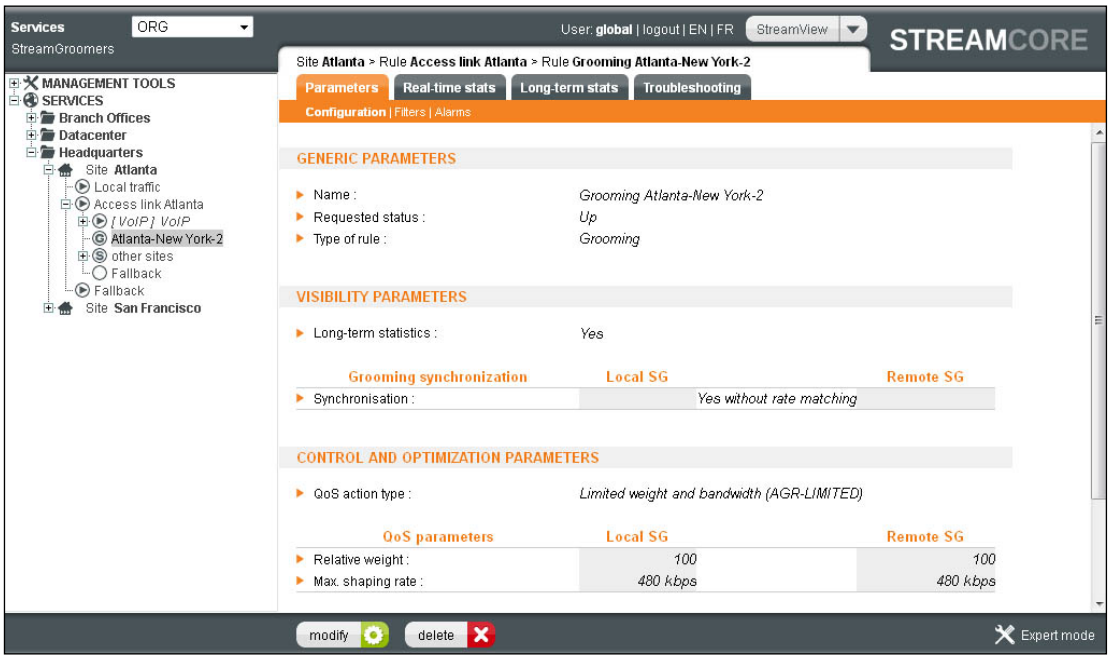


Figure 51 – Grooming rule - Parameters

Parameter	Description / Values
Generic parameters	
Name	(automatically inherited from the 2 sites name)
Requested status	Up
Type of rule	Grooming
Visibility parameters	
Long-term statistics	(default=Yes) Optional storage of long-term statistics for the rule
Grooming synchronization parameters	
Synchronization	(default=yes) Activates or deactivates the grooming protocol (network performance measurements, optimization features). The possible value are: No Yes without throughput matching Yes with throughput matching (value available only in tunnel mode)
Control and optimization parameters	
QoS action type	Limited weight and bandwidth (AGR-LIMITED) (cannot be changed)
Relative weight	(default =100) This parameter is used to allocate bandwidth to the grooming rule if it competes for bandwidth on the local access link
Max. shaping throughput	(automatically inherited from the 2 sites network parameters)
Grooming optimization parameters	
Tunneling	(default=wizard creation value) Sets up a tunnel between the 2 StreamGroomers
Compression	(default=wizard creation value)

The following table summarizes the various Grooming characteristics according to the StreamGroomer operating mode and the Synchronization parameter.

StreamGroomer Mode Parameter	**Grooming Synchronization Parameter**	***Measurement of network indicators***	***Traffic shaping***	***Tunneling***	***Throughput matching***
Monitoring&Control	With throughput matching	X	X	X	X
	Without throughput matching	X	X	X*	–
	No	–	X (shaping backup)	–	–
Monitoring	With throughput matching	X	–	–	–
	Without throughput matching	X	–	–	–
	No	–	–	–	–
Bypass	–	–	–	–	–

*Function of the *Tunnel* parameter

Selection: Rate Compression Load Frames **Performance** All

Performance	10 s 16:51:30-16:51:40	1 min 16:50:00-16:51:00	10 min 16:40:00-16:50:00
Grooming status	*Synchronized (no auto-adaptation) (2011/09/14 11:08:18) : (7 h 43 min)*		
Grooming Round-trip time min. (ms)	1	0	0
Grooming Round-trip time avg. (ms)	1	1	0
Grooming Round-trip time max. (ms)	2	2	3
Grooming jitter avg. (ms)	2	1	1
Grooming jitter max. (ms)	3	3	3
Grooming Availability ratio (%)	100	100	100

The Grooming synchronization indicator is located on the *Real-time stats* page of the Grooming rule (under the "*performance*" heading).

Why is the Grooming not synchronized?

Grooming may be desynchronized for any of several reasons:

- The Synchronization parameter is set to "No"
- One of the StreamGroomers has been shifted to Bypass mode
- Grooming configuration problem (incorrect IP address or route)
- A StreamGroomer has been wrongly connected

The **expert** parameters of a grooming rule are:

Expert parameter	Description / Values
Visibility parameters	
Grooming synchronization parameters	
IP address	(default=wizard creation value) LAN/WAN IP address used by the StreamGroomer to communicate with the remote StreamGroomer (for active network performance measurements, throughput matching protocol and tunnel mode)
Port	(default=49 152) UDP port used by the StreamGroomer to communicate with the remote StreamGroomer (for active network performance measurements or for the tunnel mode)
Other end IP addresses / ports	(default=Yes) When establishing a grooming through a NAT, set this value to "Manual" in order to be able to enter remote public IP addresses on each grooming rule.
Keep Alive timer / Retries	(default=1s/5) Synchronization keep alive and retry parameters.
Control and optimization parameters	
WAN encapsulation	(automatically inherited from the site network parameters)
IPSEC encapsulation performed by the router	
Grooming optimization parameters	
Min. roundtrip delay	(default=100 ms) Parameter used by the throughput matching algorithm to limit the total amount of data exchanged within the grooming rule.
Packets aggregating timer	(default=0 ms) Max waiting timer to allow packet aggregation in ms. Increasing the timer will add a delay but will improve the compression ratio.
Shaping backup	(default =Yes) Set this parameter to "Yes" in order to enable QoS actions when the grooming is not synchronized.
Load Balancing & Backup	

Associate grooming rule	(default=Disabled) When 2 grooming rules are defined between 2 sites, then load balancing can be enabled between the 2 rules, either per session or per application.
Load Balancing Mode	
DiffServ	
Tunnel ToS marking	(default=Transparent) To set the DSCP/ToS field of the the grooming tunnel packets. The value can be fixed or can be transparent.
Tunnel control packets ToS marking	(default=No) To set the DSCP/ToS field of the the grooming control protocol packets

7.4.3 Filters

The filters associated with a shaping/grooming rule can be displayed by clicking on the ***Parameters-Filters*** tab. All the filters are automatically inherited from the remote site parameters. It is not possible to disable automatic filters on shaping rules.

There is usually no need to disable automatic filters on grooming rules except in very specific cases.

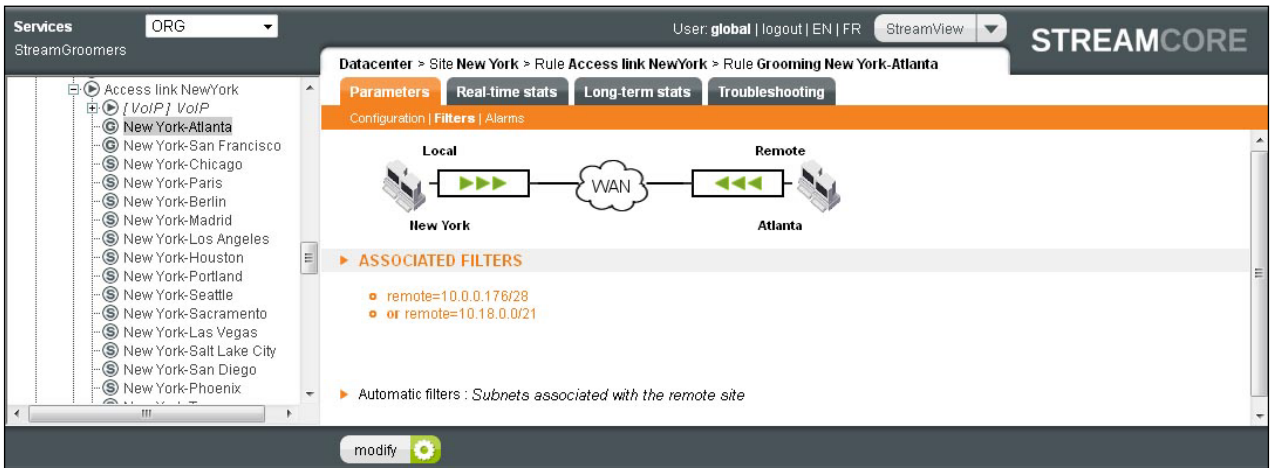


Figure 52 – Shaping/Grooming rule – Filters

7.4.4 Add/Modify/Delete/Move Operations - Tree Menu

66 ADD A SHAPING RULE

To create a Shaping rule directly from the tree menu:

1. Right-click on **"SERVICES > … > Site xx > Access link xx > Other"** and select **"Insert before… → Shaping"**.
2. The creation wizard is automatically launched. Select the remote site and the different parameters.
3. Click on the **Finish** button.

Figure 53 – Add a shaping rule wizard

Parameter	Description / Values
Shaping rule towards	Select a site in the list
Groups of rules to be applied (optional)	Select one or more application groups of rules to classify the traffic below the shaping rule
Group of alarms to be applied (optional)	Select one or more network group of alarms to detect abnormal service levels
Frequency of active probe	(default=Off) Activate a ping to measure availability and network performance

Note: When only some specific remote sites are managed by shaping/grooming rules, a generic "Shaping other sites" rule can be created in order to manage traffic exchanged with all other sites. In order to do so, select the remote site "Other sites".

67 ADD A GROOMING RULE

To create a Grooming rule directly from the tree menu:

1. Right-click on **SERVICES > … > Site xx > Access link xx > Other** and select **Insert before… → Grooming**.
2. The creation wizard is automatically launched. Select the remote site and the different parameters.
3. Click on the **Finish** button.

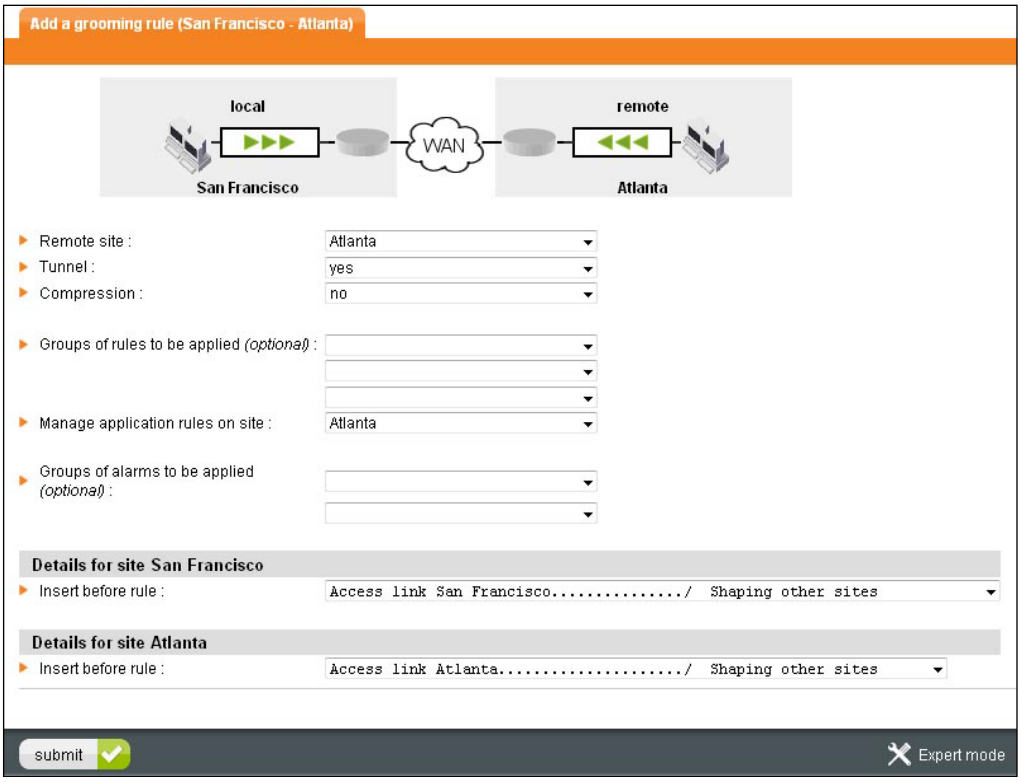


Figure 54 – Add a grooming rule wizard

Parameter	Description / Values
Remote site	Select a site in the list
Tunnel	Enable or no tunneling by default
Compression	Enable or no compression by default
Groups of rules to be applied (optional)	Select one or more application groups of rules to classify the traffic below the grooming rule
Manage application rules on site	Select on which site the application rules will be displayed (usually the branch office and not the data center)
Group of alarms to be applied (optional)	Select one or more network group of alarms to detect abnormal service levels
Frequency of active probe	(default=Off) Activate a ping to measure availability and network performance

68 MODIFY A SHAPING/GROOMING RULE

To modify the configuration parameters of a Shaping or a Grooming rule:

1. Click on **SERVICES > ... > site xx > Shaping xx or Grooming xx** in the tree menu for the site.
2. Select the *Parameters – Configuration* sub-tab.
3. Click on the **Modify** button, enter the modifications, and then click on the **Submit** button.

69 DELETE A SHAPING/GROOMING RULE

To delete a Shaping or a Grooming rule from the tree menu, click on it and then on the "*Delete*" button.

70 MOVE

To move a Shaping or Grooming rule, right-click on it and then select **Move**. The function is available only on a site with a StreamGroomer: in the right screen displaying the infrastructure rules hierarchy, choose the new place and then click on the **Submit** button.

7.4.5 Add/Delete Operations - Matrix Management Tool

71 SUMMARY

In order to display a summary of the site-to-site traffic management:

1. Open the **MANAGEMENT TOOLS**, select **Matrix** in the tree menu and click on the ***Network rules*** tab
2. Select a subset of sites to be displayed by choosing categories (option)
3. Click on the **Submit** button

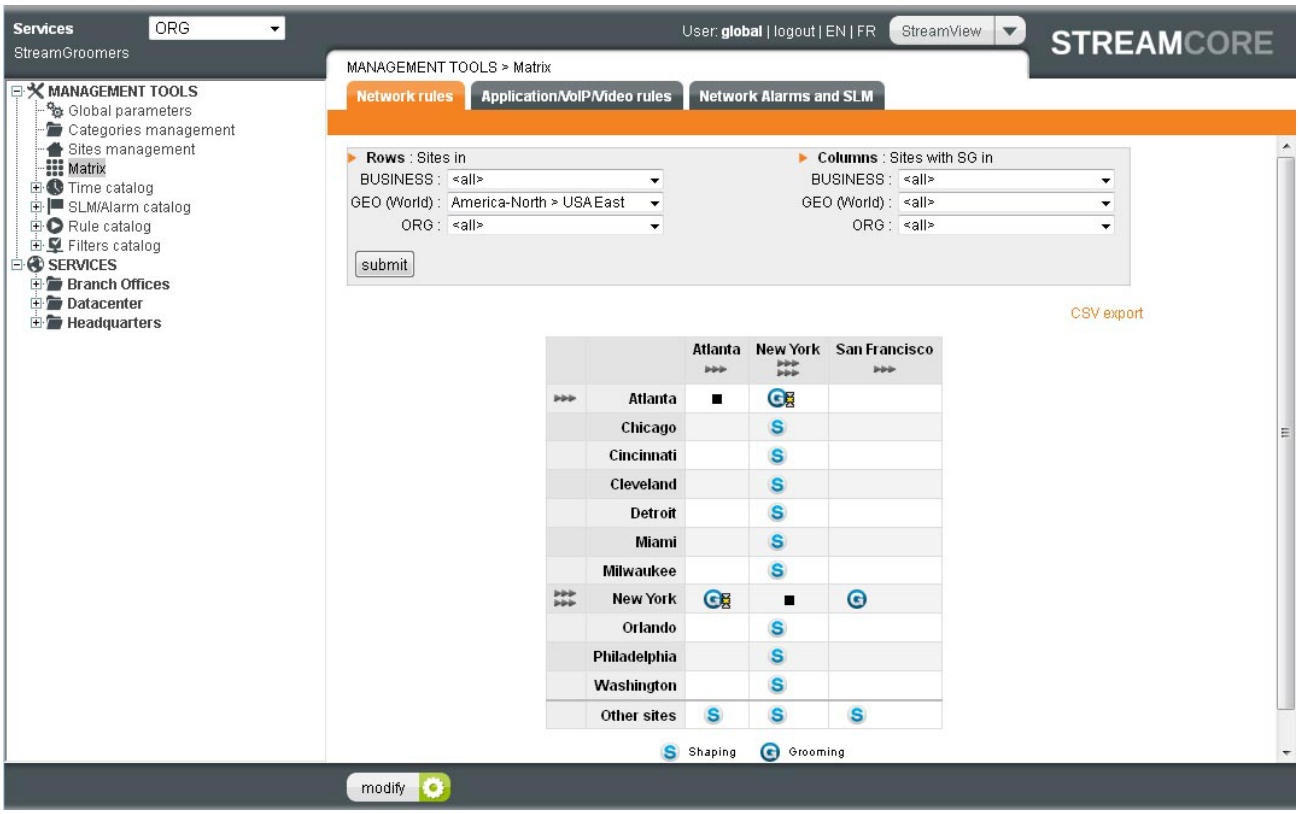


Figure 55 – Visualization of the site-to-site traffic management matrix

Note: Only sites with StreamGroomers can be displayed in columns

72 ADD A SINGLE RULE

In order to create a shaping / grooming rule from the matrix:

1. Display the network rules matrix as explained previously.
2. Click on the **Modify** button.
3. Click on the intersection between the sites for which the traffic has to be managed.
4. The shaping rule or grooming rule creation wizard described in chapter 7.4.4.1 and 7.4.4.2 is automatically launched. The only additional parameter is the location in the tree where the rule will be created.
5. Click on the **Finish** button.

73 ADD MULTIPLE RULES

Many shaping or grooming rules can be created in one shot by using the network rules matrix:

1. Display the matrix as explained previously.
2. Click on the **Modify** button.
3. Click on the **Create all** button in order to fill a column with Shaping/Grooming rules.
4. An auto configuration of shaping / grooming creation wizard is automatically launched:

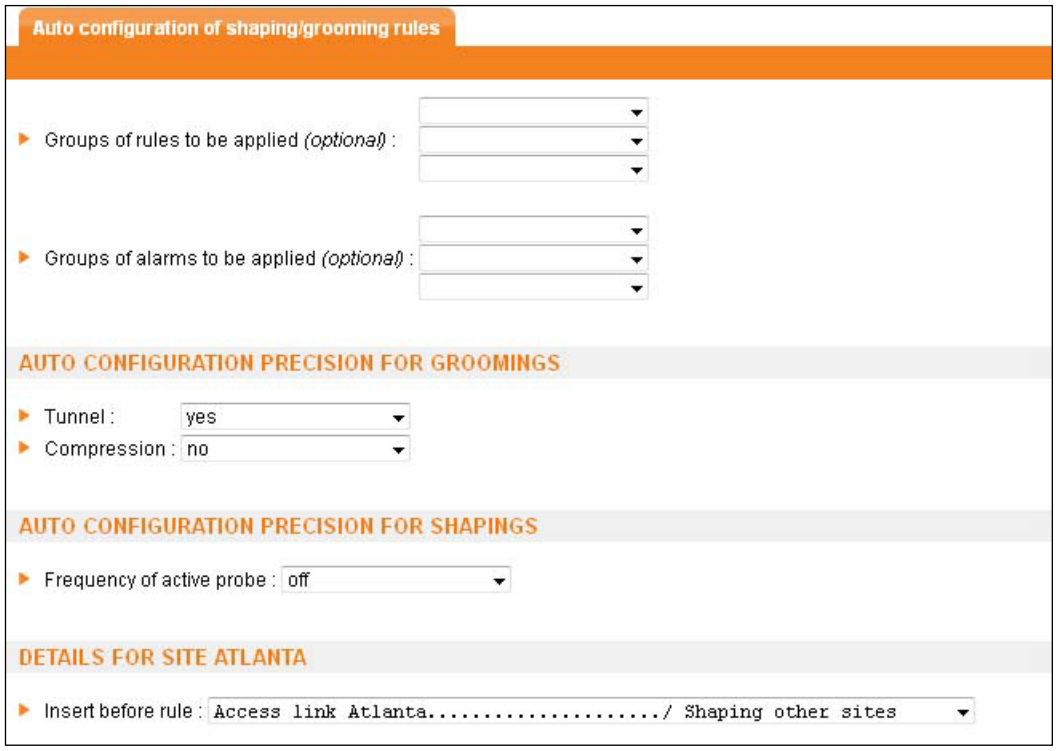


Figure 56 – Auto configuration of shaping / grooming rules wizard

Parameter	Description / Values
Groups of rules to be applied (optional)	Select one or more application groups of rules to classify the traffic below the grooming rule
Groups of alarms to be applied (optional)	Select one or more network group of alarms to detect abnormal service levels
Auto-configuration for grooming	
Tunnel	Enable or disable tunneling by default
Compression	Enable or disable compression by default
Auto-configuration for shaping	
Frequency of active probe	(default=Off) Activate a ping to measure availability and network performance
Details	
Insert before rule	Select a rule

1. Click on the **Submit** button
2. Wait until the end of the operation (it can take some time if numerous lines have been displayed).

When only some specific remote sites are managed by shaping/grooming rules, a generic "Shaping other sites" rule can be created in order to manage traffic exchanged with all other sites. From the network rules matrix:

1. Display the matrix as explained previously
2. Click on the **Modify** button
3. Click on the intersection between the "Other sites" line and the site for which the traffic has to be managed, or click on the *"Create all"* to create rules for all sites selected in the columns.

74 DELETE A SINGLE RULE

In order to delete a shaping / grooming rule from the network rules matrix:

1. Display the matrix as explained previously.
2. Click on the **Modify** button.
3. Click on the delete sign next to the shaping / grooming rule, and submit the confirmation message.

75 DELETE MULTIPLE RULES

Many shaping or grooming rules can be deleted in one shot by using the network rules matrix:

1. Display the matrix as explained previously.
2. Click on the **Modify** button.
3. Click on the **Delete all** button in order to fill a column with Shaping/Grooming rules.
4. Wait until the end of the operation (it can take some time if numerous lines have been displayed).

7.5 INTERMEDIATE, TERMINAL DATA OR AUDIO/VIDEO RULES

7.5.1 Introduction

Application and VoIP/video traffic is classified into "Intermediate", "Terminal data" and "Terminal audio/video" rules. Unlike access link or shaping/grooming rules, the filters are not automated and must be defined. Moreover, these types of rules can belong to groups of rules distributed over a set of sites.

The type of rule can be changed at any time to transform an "Intermediate rule" into a "Terminal data" or "Terminal audio/video" rule, or vice-versa.

		DESCRIPTION	FILTERS
	Intermediate	Rule used to add a new level of classification into the tree to classify audio/video or application traffic. Such a rule can be used to perform statistics aggregation or to add a level of scheduling for QoS purpose. Such a rule can be included in a group of rules.	Custom filters (or automated filters inherited from sub-rules)
	Terminal data	Leaf rule used to classify application traffic. Application performance measurements are automatically computed, and specific performance control options are available. Such a rule can be included in a group of rules.	Custom filters
	Terminal audio/video	Leaf rule used to classify audio/video traffic. Audio/video performance measurements are automatically computed, and specific performance control options are available. Such a rule can be included in a group of rules.	Custom filters

Note: At any time, it is possible to change the type of rule and transform an "Intermediate rule" into a "Terminal data" or "Terminal audio/video" rule, or vice-versa.

7.5.2 Parameters

The **main** parameters of an "Intermediate", "Terminal data" or "Terminal audio/video" rules can be displayed by clicking on the *Parameters-Configuration* tab:

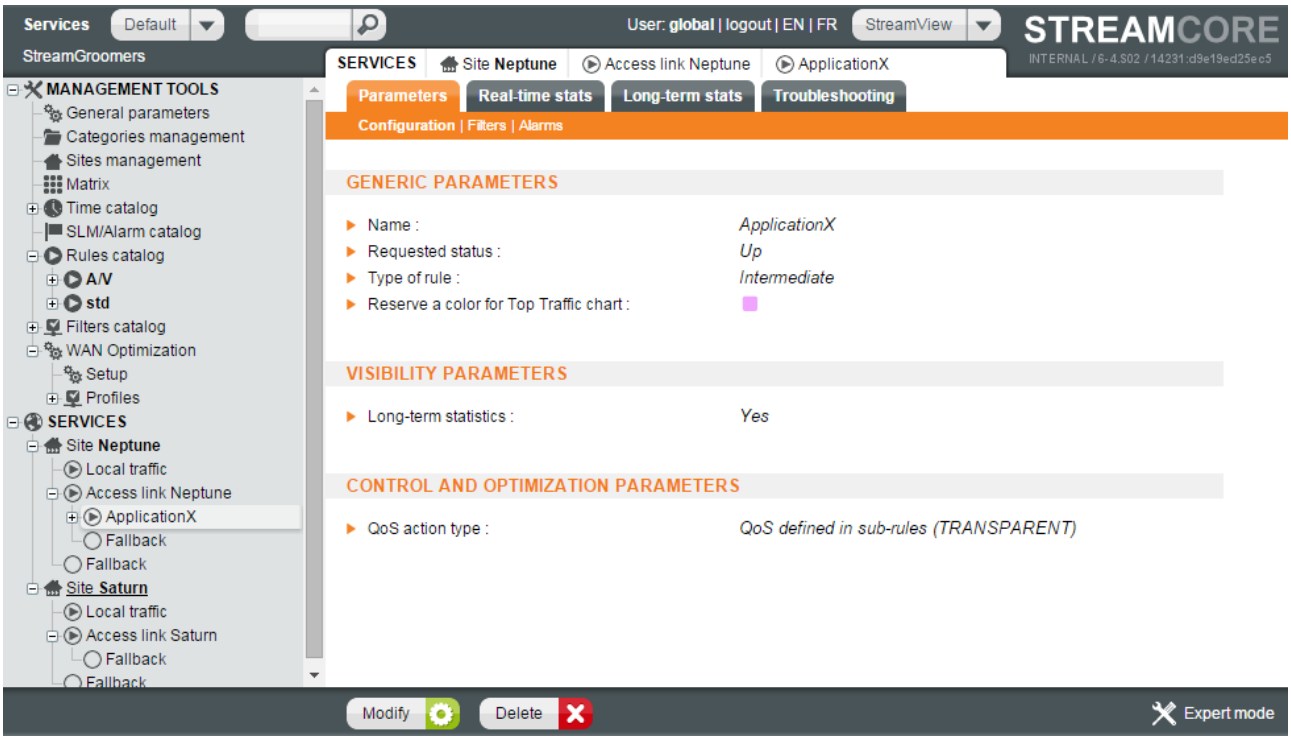


Figure 57 – Intermediate rule parameters

Parameter	Description / Values
Generic Parameters	
Name	Name of the rule
Requested status	Up (default), Down
Type of rule	Intermediate rule, Terminal data, Terminal audio/video
Reserve a color for Top Traffic chart	This option is set to "No" automatic by default. However it is possible assign a color to a rule by selecting one of the 25 reserved colors from the combo box display. This option is only available for Intermediate and Terminal rules. Custom colors can only be viewed in Long-term stats -Top Traffic charts. It is also possible to reserve a color for a rule coming from a group of rules (Rule Catalog) as well. See Figure 58 – Reserving a color for a specific rule from the Rules catalog and Figure 59 – Rules displayed with reserved color
Visibility Parameters	
Long-term statistics	(default=Yes) Optional storage of long-term statistics for the rule
NetFlow export per application	(default=Disabled) Enable / disable NetFlow export if the NetFlow parameter on the site is set to "per application"
VoIP/video measurements	Select the type of performance measurements for VoIP/video traffic (see chapter 9.2.1.4)

(terminal audio/video rules)	
Control and Optimization parameters	
QoS action type	(See chapter 11.3.2 and 11.4.2 to learn more)
QoS time exception	
Set of parameters	

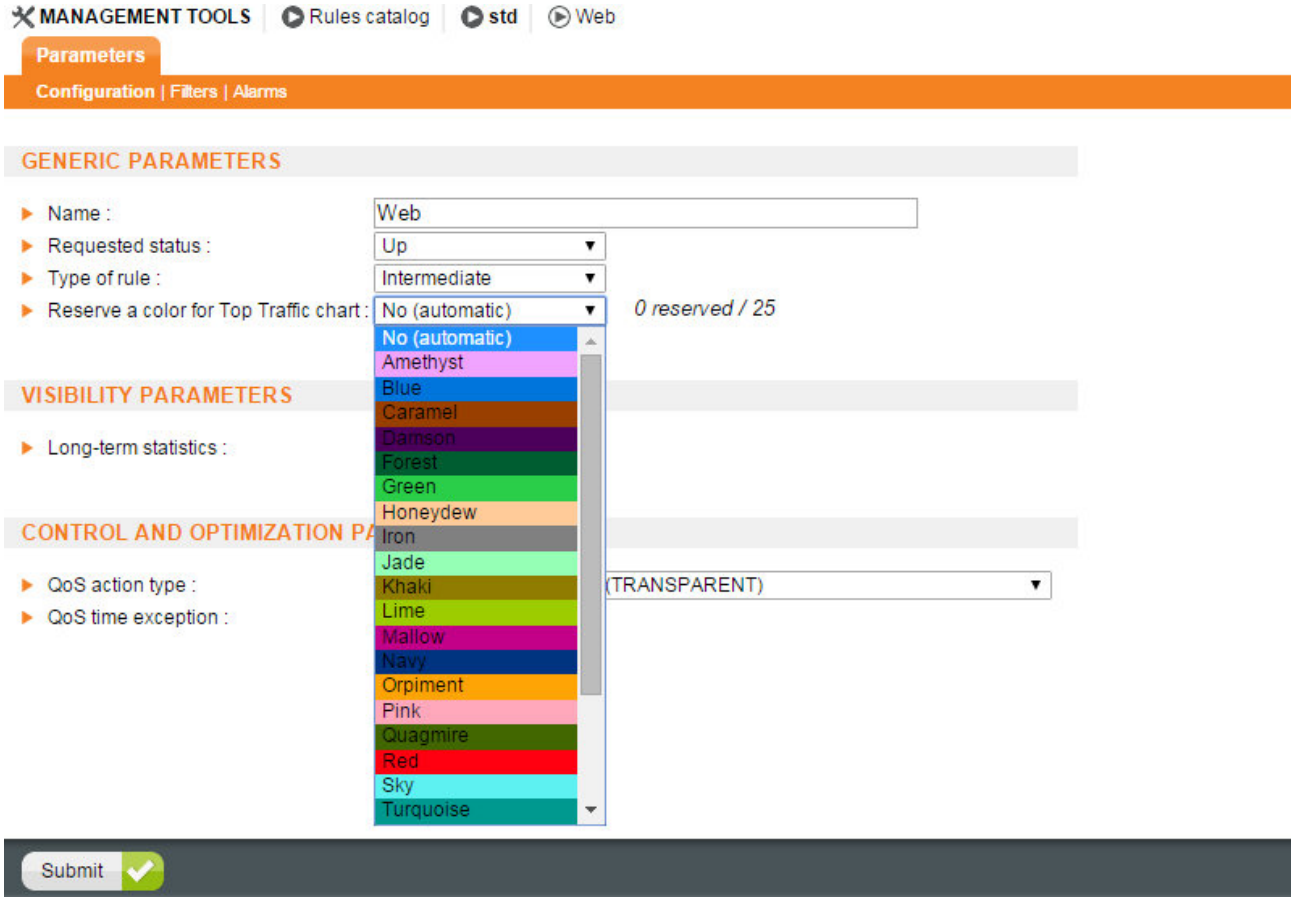


Figure 58 – Reserving a color for a specific rule from the Rules catalog

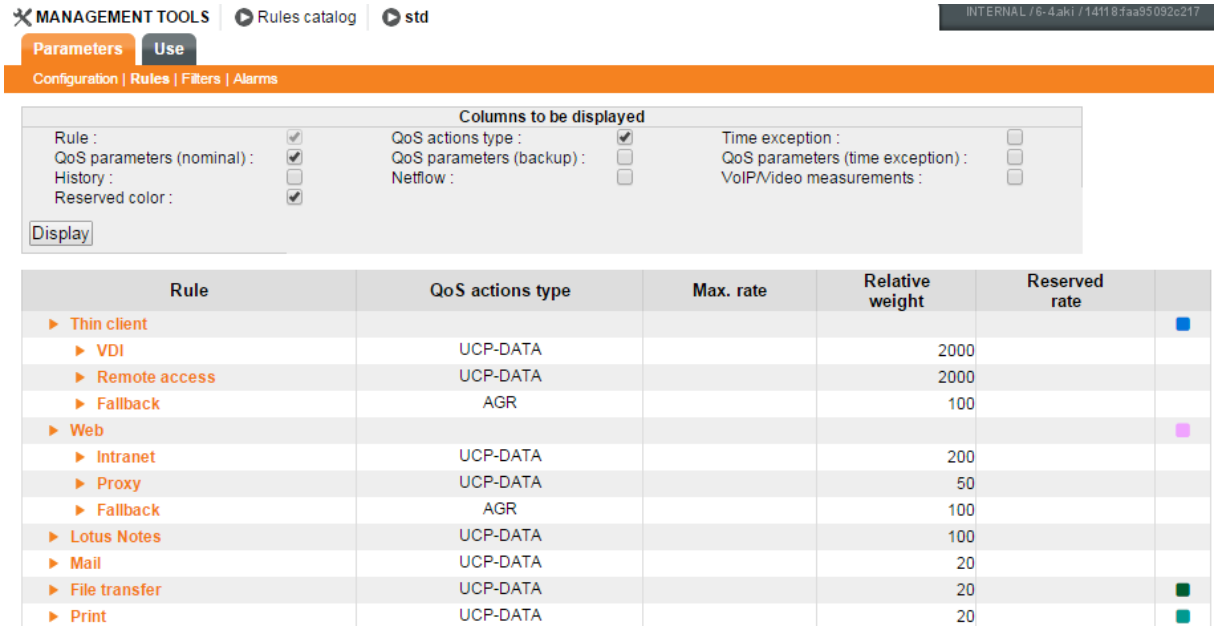


Figure 59 – Rules displayed with reserved color

Additional **expert** parameters are available for "Terminal data rules" or "Terminal audio/video rules":

Expert parameter	Description / Values
Control and optimization parameters	
DiffServ	
DSCP marking to LAN	(See chapter 11.5.2.1 to learn more)
DSCP marking to WAN	
Queues	
Size (bytes)	(See chapter 11.5.2.2 to learn more)
Queue drop policy	
Other	
Compression	(if grooming rule sub-tree) Enable / disable compression for traffic classified in the rule.
Comment	Any text

7.5.3 Filters

76 FILTERS SUMMARY

The filters associated with an "Intermediate", "Terminal data" or "Terminal audio/video" rule can be displayed by clicking on the *Parameters-Filters* tab. More details can be displayed for a specific filter by clicking on it.

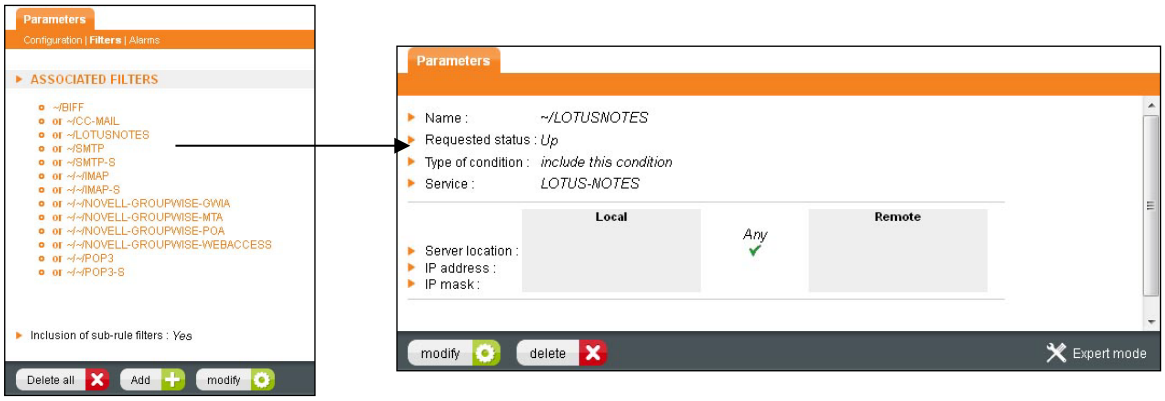


Figure 60 – Filters summary and parameters display

77 FILTER PARAMETERS

The **main** parameters of a filter are:

Parameter	Description / Values
Name	Name of the filter (automatically filled if left blank)
Requested status	Up (default), Down
Type of condition	Include (default), Exclude
Filters catalog	Displayed only when creating or modifying a filter. When selecting a filter in the list, it automatically pre-fill all the parameters. See next chapter to learn more.
Service	Select a value among the list of predefined protocols and applications:
Server location	For all services running over UDP/TCP, this parameter defines on which side the server port is located. The possible values are: - "Any": the classification does not take into account the UDP/TCP call direction - "Local" or "Remote": the classification takes into account the UDP/TCP call direction
Host	Check this box to enforce the IP mask to /32
IP address	Enter a local and/or remote xx.xx.xx.xx value
IP mask	Enter a local and/or remote xx.xx.xx.xx value
Server port	When "TCP", "UDP" or "UDP+TCP" service is selected, a single value or a range value (for instance 80 or 80-82) can be defined (multiple entries separated by a comma can also be defined)

The **expert** parameters of a filter are:

Expert parameter	Description / Values
DNS name	When the "Host" checkbox is set, the DNS name can be entered instead of an IP address, and the SGM will automatically retrieve the IP address from the DNS server
MAC address	Enter a MAC address
DiffServ	Select the DiffServ field format (COS/TOS or DSCP) and enter the value
VLAN	Enter a VLAN ID

When a **L7-specific criteria service** is selected, additional parameters are available:

L7-specific criteria service	*Parameter*	Description / Values
HTTP HTTP-PROXY	*Hostname*	Hostname of the Web traffic to be classified
	URL	URL of the Web traffic to be classified
HTTPS	*Common name*	SSL certificate common name of the encrypted traffic
	Organization name	SSL certificate organization name of the encrypted traffic
	Organization unit name	SSL certificate organization unit name of the encrypted traffic
	Locality name	SSL certificate locality name of the encrypted traffic
RTP+RTCP	*Payload*	List of predefined RTP payload type: audio+video (default), audio, video, audio/G.711, audio/MS…
	Codec	If "custom" payload is selected, the payload type value can be entered (the inbound RTP flow will be inspected)

For HTTP, HTTP-PROXY and HTTPS services:

- A wild card (*) can be used in any name
- Other ports than traditional ports (80 for HTTP, 8080 for HTTP-PROXY, 443 for HTTPS) can be defined on a StreamGroomer to track L7-criteria. See expert parameters in chapter 4.2.4.

78 FILTERS CATALOG

Filters can be created directly on rules, but also in the Filters catalog available in Management tools. There are 2 ways to create filter template:

1. **Manual creation:** right-click on **MANAGEMENT TOOLS > Filters catalog**, and select "Add Filter Template".
2. **Automated creation through the troubleshooting tools:** by checking the "Filter creation" when displaying connections in Troubleshooting tools, "Create" button are available next to each session displayed. By clicking on **Create**, it will pre-fill a filter template within the Filters catalog.

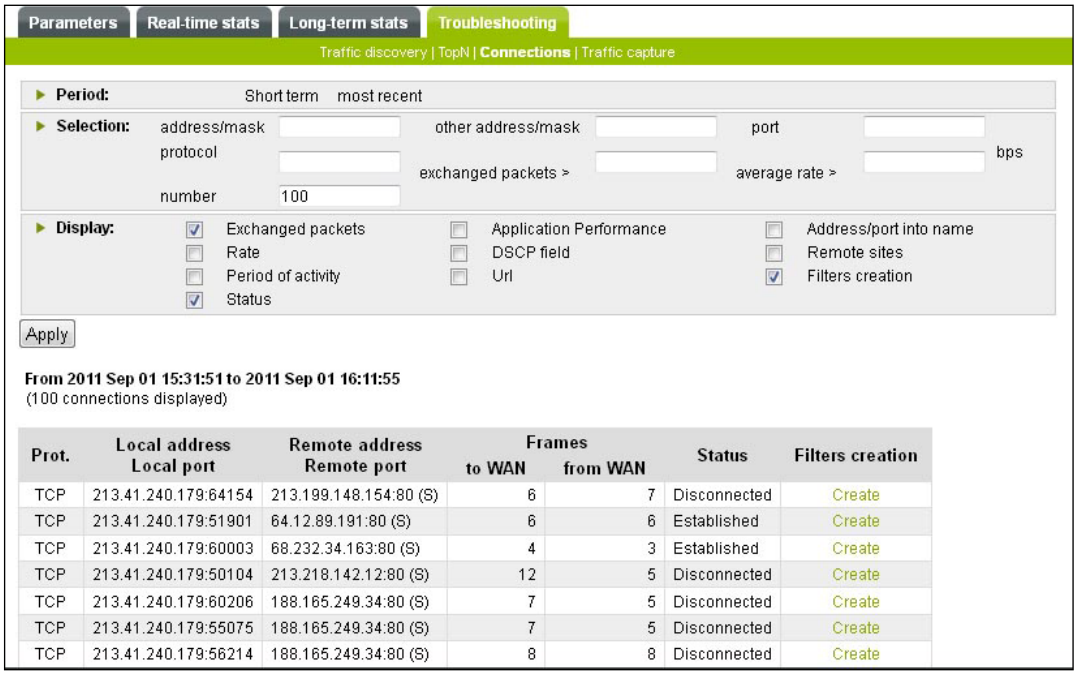


Figure 61 – Automated filter creation through troubleshooting tools

To use a filter in the catalog in the Create/Modify screen of a filter, select a value in the "Filters catalog" list.

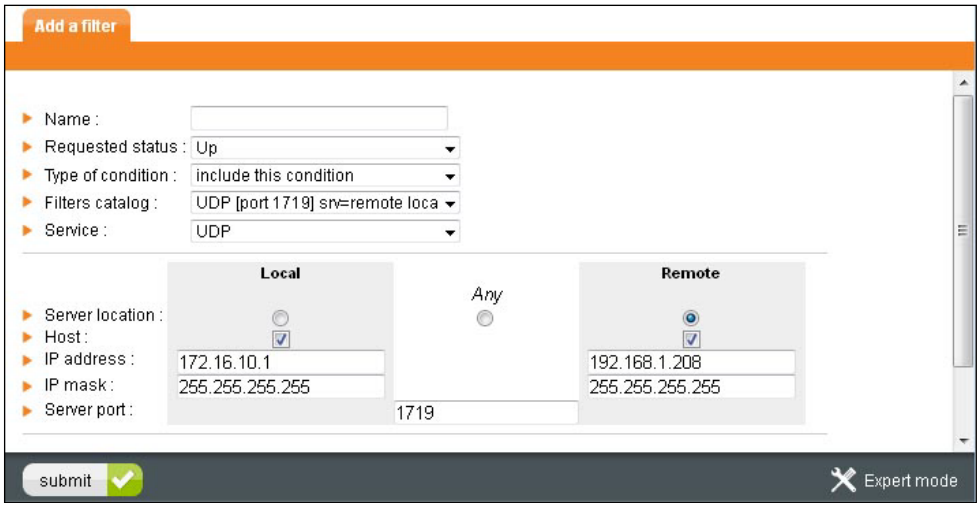


Figure 62 – Filter template selection

Note: When creating a filter for an HTTP, HTTPS or RTP+RTCP session, then the L7 classification criteria will also be pre-filled in the filter template.

7.5.4 Add/Modify/Delete/Move Operations

79 ADD

To add a specific rule (directly in a site rules tree) or a distributed rule (within a reference Group of rules):

1. Right-click on the rule before which the new rule should be inserted and select **"Insert before… → Intermediate rule** or **Terminal data rule** or **Terminal audio/video rule"**.
2. Fill in the various fields
3. Click on the **Submit** button.
4. The filter creation assistant is displayed automatically.
5. Click on the **Submit** button. The creation of the rule with a first filter is completed.

80 MODIFY

To modify a rule, first click on the rule and then select the *Parameters – Configuration* sub-tab. Click on the **Modify** button, enter the modifications, and then click on the **Submit** button.

To modify the filters of a rule, first click on the rule and then select the *Parameters – Filters* sub-tab. The following modifications are available:

- **Updating a filter:** Click on the filter in the right-hand operating window; click on the **Modify** button, enter the modifications, and then click on the **Submit** button.
- **Adding a filter:** Click on Filters associated: + new in the right-hand operating window; enter the filter parameters, and then click on the **Submit** button.
- **Deleting a filter:** Click on the filter and then on the "*Delete*" button.

Note: The "Inclusion of sub-rule filters" parameter of an Intermediate rule can be set to "yes" so that the sub-rule filters are automatically transferred.

Caution: Sub-rules cannot be included if exclusion filters have been defined.

81 DELETE

To delete a rule, click on it and then on the **Delete** button. Validate the confirmation message.

82 MOVE UP/DOWN

To move a rule up or down from one level in the rules tree, right-click on it and then select **Move up** or **Move down**.

83 MOVE

To move a rule, right-click on it and then select **Move**. In the right screen displaying the application rule hierarchy, choose the new place and then click on the **Submit** button.

Note: This functionality is not available within a reference Group of rules.

84 COPY/PASTE

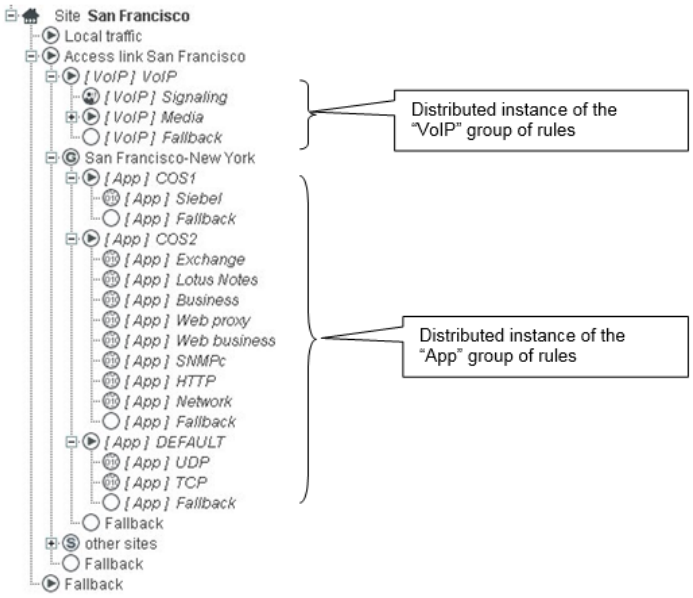
To copy a rule, right-click on it and then select **Copy**. To insert it elsewhere in the tree menu, right-click on the rule that will appear below it, and then select **Paste before**.

7.6 GROUPS OF RULES

7.6.1 Introduction

Groups of rules are used to ensure a homogenous application and/or VoIP/video traffic classification (as well as performance control/optimization) across a set of sites.

A distributed rule must be part of a distributed instance of a Group of rules. It appears in italics in the rules tree hierarchy for the site, and starts with the name of the reference Group of rules in square brackets. Groups of rules are usually defined to match application or audio/video traffic, and distributed across a set of sites to ensure a homogeneous classification.



Adding, modifying, or deleting of a distributed rule must take place in the reference Group of rules, and is applied automatically to all of the distributed instances.

7.6.2 Reference Group of Rules Management

85 PARAMETERS

In order to manage a group or rules, open the **MANAGEMENT TOOLS** and click on **Rules catalog** in the tree menu, click on the group and select the *Parameters-Configuration* tab.

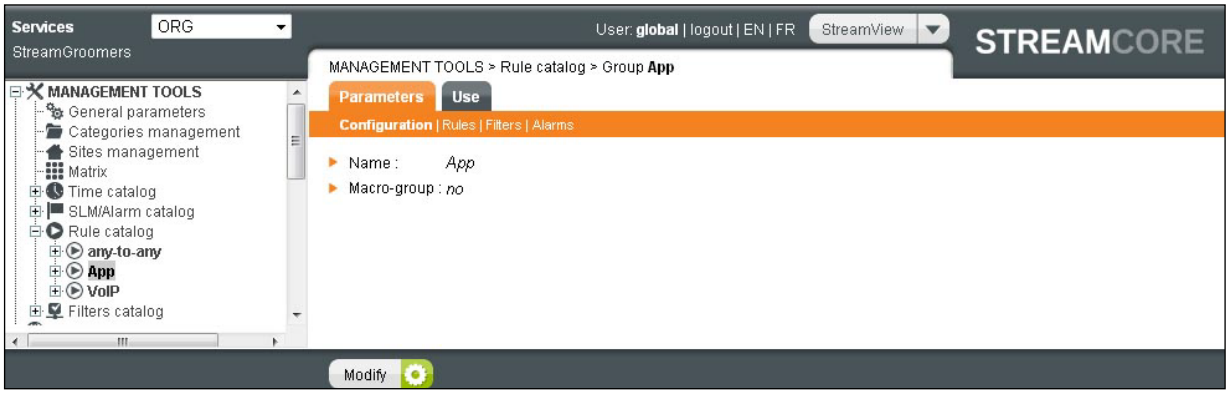


Figure 63 – Group of rules parameters

Parameter	Description / Values
Name	Group name
Macro-group	The default parameter is set to "No". When set to "Yes", groups of rules can be added within the macro-group of rules.

86 RULES AND FILTERS SUMMARY

A summary of rules and filters within the group can be displayed by selecting the *Parameters-Rules* or *Parameters-Filters* tab (exactly as the rules and filters summary on a site).

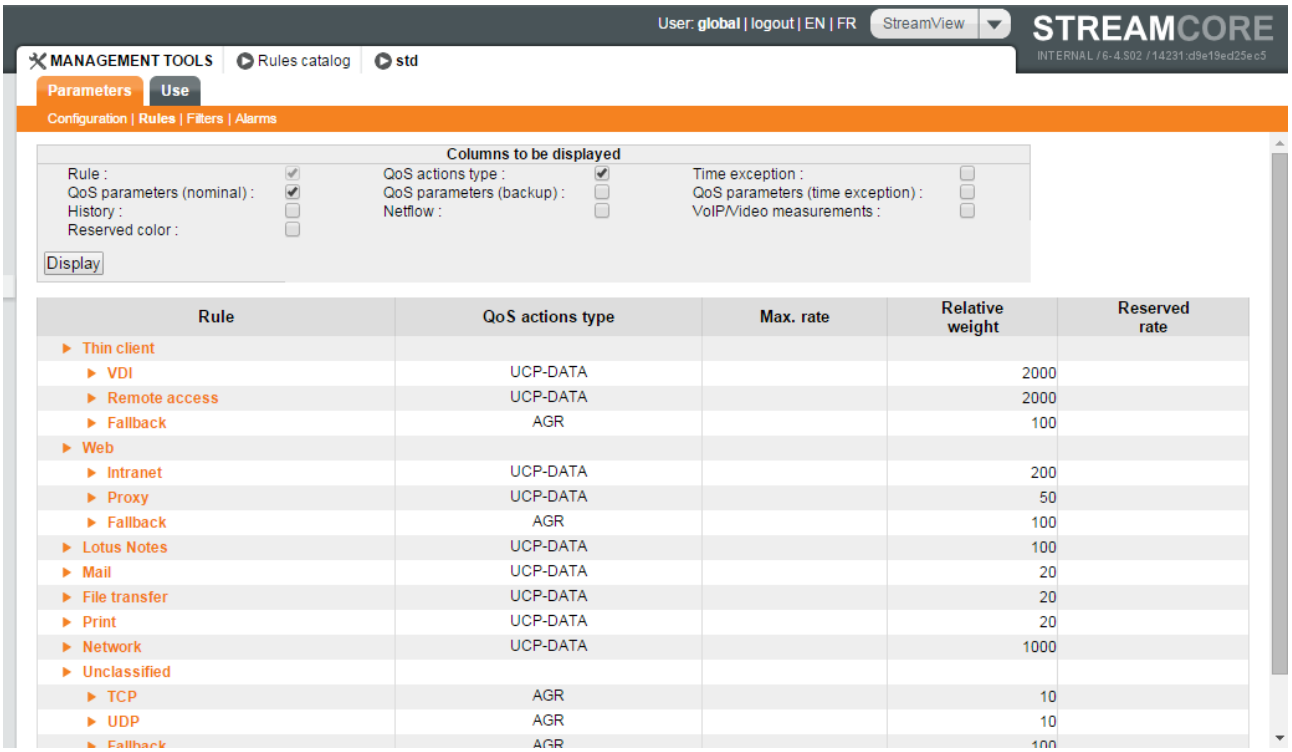


Figure 64 – Group of rules summary

87 DISTRIBUTION SUMMARY

All of the distributed instances of a reference Group of rules can be displayed by clicking on **SERVICES > Rules catalog > Group xx**, and then selecting the *Use* tab.

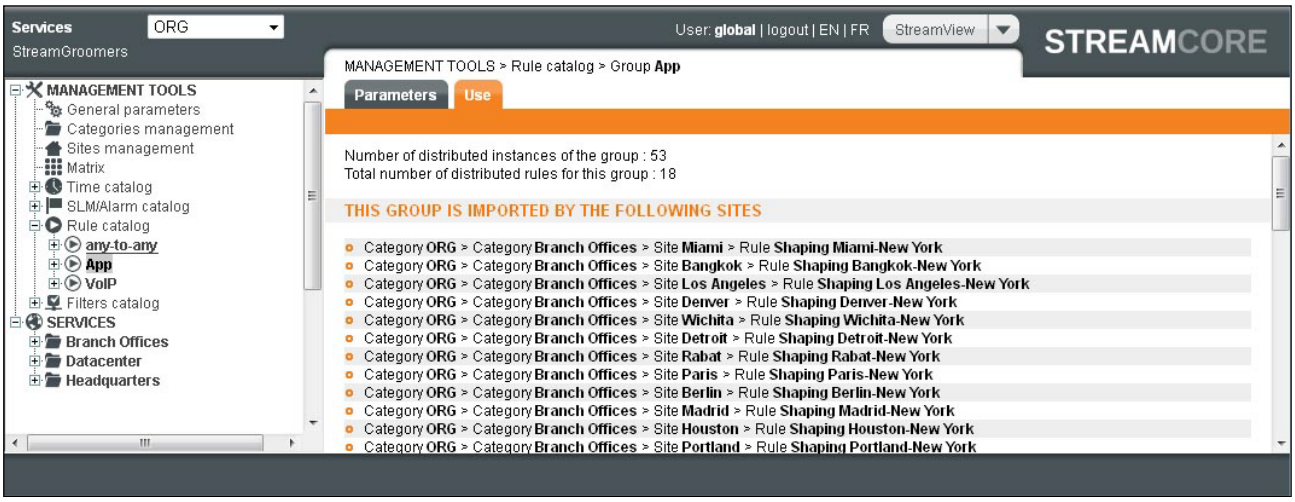


Figure 65 – Group of rules distribution summary

88 CREATE A REFERENCE GROUP OF RULES

To create an empty reference Group of rules:

1. Open the **MANAGEMENT TOOLS**, right-click on Rules catalog, and then select "Add… → Group" or "Add… → Macro-group".
2. Enter the group name, select the type among the following values:

Group of rules type	Description
Empty (default)	Empty group of rules
Predefined standard applications	Group to classify standard enterprise applications
Predefined standard VoIP	Group to classify standard VoIP traffic
Predefined standard audio+video	Group to classify any form of audio or video traffic (VoIP, videoconferencing, UC…)
Full traffic discovery (>400 applications)	Group to be used for an audit with a comprehensive list of auto-discovered applications classified into categories

3. Click on the **Submit** button.

89 MODIFY

To change the name of a group or rules, first click on the group and then select the *Parameters – Configuration* sub-tab. Click the **Modify** button, enter the modifications, and then click the **Submit** button. To update the Rules tree, "Intermediate", "Terminal data" and "Terminal audio/video" rules and filters are managed in a group of rules exactly as in the Rules tree of a site. Rules can be added, modified, deleted etc.

90 DELETE

To delete a group or rules, click on it and then on the **Delete** button then **Submit**.

Note: A reference group of rules can be deleted only if they are not distributed on any site.

91 IMPORT / EXPORT OF A REFERENCE GROUP OF RULES

To export a group of rules (except macro-group), click on **MANAGEMENT TOOLS > Rules Catalog**, select the *Summary* tab and click on the group of rules to be exported: a file xx.cli containing all information will be downloaded.

Figure 66 – Export a group of rules

To import a group of rules, select the *Import* tab, define the name of the new group, and import the file.

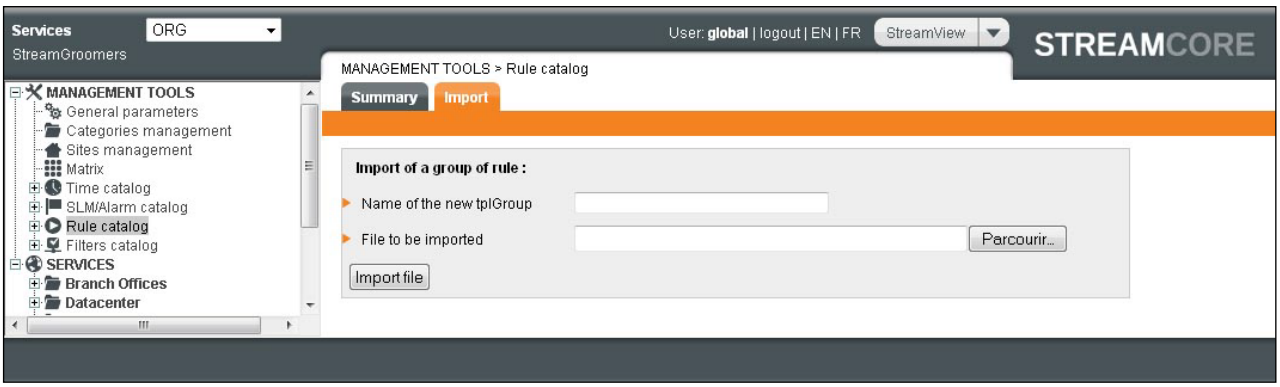


Figure 67 – Import a group of rules

7.6.3 Add/Delete Operations – Tree Menu

92 ADD

A group of rules can be inserted directly on an existing site:

1. Right-click on the rule that will be placed under the Group of rules, and select "**Insert before... > Group of rules**".
2. Select the reference group of rules, then click on the **Submit** button.

When Shaping or Grooming rules are created, the wizard offers the possibility to distribute one or more reference groups of rules.

93 DELETE

To delete a distributed instance of a group of rules, right-click on **the first rule** in the instance, and then select **Delete**.

7.6.4 Add/Delete Operations – Matrix Management Tool

94 MATRIX SUMMARY

In order to display a matrix summary of the group of rules used per site:

1. Open the **MANAGEMENT TOOLS**, select **Matrix** in the tree menu and click on the *Application/VoIP/Video rules* tab
2. Select a subset of sites to be displayed by choosing categories (optional)
3. Click on the **Submit** button.

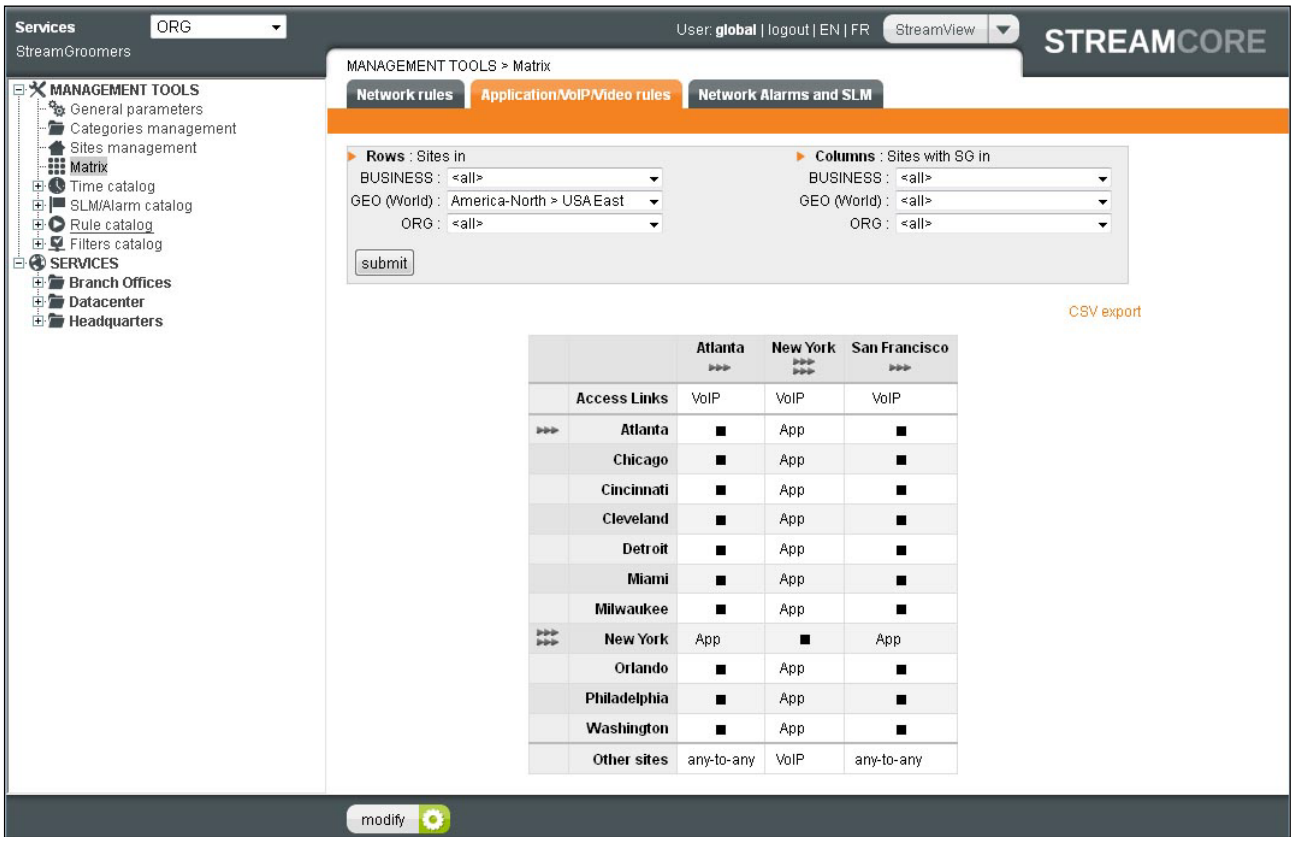


Figure 68 – Group of rules matrix summary

95 ADD

In order to create many group of rules through the matrix:

1. Display the app/VoIP/Video rules matrix as explained previously
2. Click on the **Modify** button
3. Click on the intersection between the sites for which the traffic has to be managed, or use the **Create all** buttons to apply several changes in a single click.

96 DELETE

In order to create many group of rules through the matrix:

1. Display the app/VoIP/Video rules matrix as explained previously
2. Click on the **Modify** button

3. Click on the intersection between the sites for which the traffic has to be managed, or use **Delete all** buttons to apply several changes in a single click.

8 UMT – WAN Optimization

8.1 INTRODUCTION

Steamcores WAN Optimization solution offers a multi-featured tool set that helps distributed Enterprises improve efficiency of their application servers. WAN Optimization enables the use of WAN effectively therefore reducing traffic and potential latency.

Enterprise applications for cross-collaborative projects are becoming a commonplace. Teams often span multiple geographies, requiring network speed, reliability and efficiency essential. Poor application response times can lead to unhappy users as well as inefficient use to time and money. WAN optimization can help by providing smart use of protocols, caching, and compression. These three methods are the main tools used by Streamcore to provide a WAN Optimization solution.

WAN Optimization mode enables you to speed-up data exchange across multiple sites. Its principle function is to reduce the number of bottlenecks between the WAN and LAN by using an effective replication system based on data packet IDs. As a result bandwidth and network performance between the WAN and LAN is optimized.

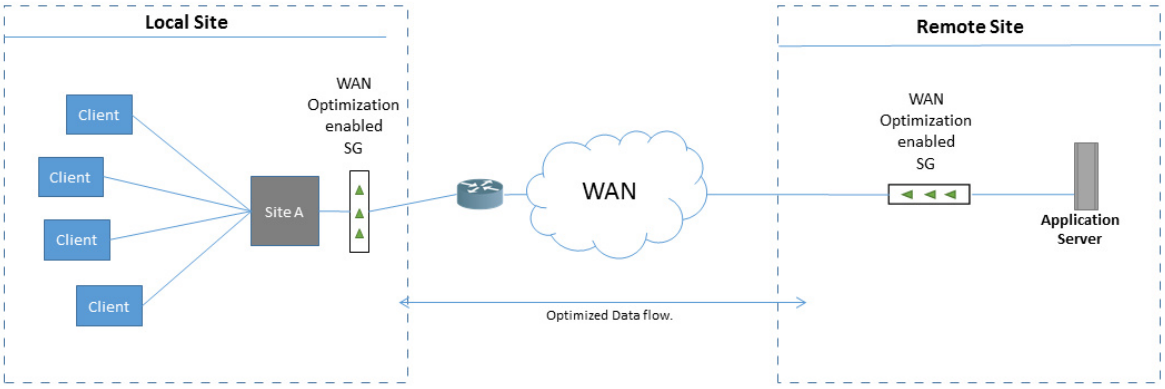


Figure 69 – Example of WAN Optimization Remote to Local Site deployment

Note: An application in this context is an IP address or subnet.

8.1.1 Protocol Optimization

The aptly named "chatty" protocols like CIFS and MAPI operate fine in LAN environments where network speeds are high (typically around 50-100 gigabits per second) and distances are relatively short. In this environment, the back-and-forth communication exchanges that require acknowledgements (hence the name chatty) do not lead to latency. In this context, large file downloads, as well as application usage are negligible.

In contrast, from a WAN perspective, these protocols are not efficient. This is principally due to WAN speeds being slower than LANs speeds. In addition, conversation acknowledgments have longer distances to travel. Ultimately, the same back-and-forth "chatty" communication described above becomes a performance limitation. High levels of latency occur and QoS becomes a major issue, especially for users who access enterprise applications remotely. A file that might take seconds to access or download from a LAN can take several minutes in a WAN context. This may seem trivial, however for a distributed enterprise with a large global workforce, fast and easy access to data is vital. Using WAN optimization mitigates latency problems with many of the common protocols.

Note: Only TCP traffic can be optimized

8.1.2 Cache Optimization

Streamcores cache optimization does not use the traditional "whole" object cache system, which is widely used on Web browsers. Data is optimize by delivering chucks data to be memorized (cached) on a site. Imagine a user that is working on a large shared document and needs to access and edit the document over a WAN. The document is accessed from a remote server and is initially cached locally. Changes made to the document are

saved but the entire document is not resent over the WAN. A reference to the old data is created and sent across the WAN along with the new data. This saves a large amount of network resources because only a reference to the old data is sent across the WAN.

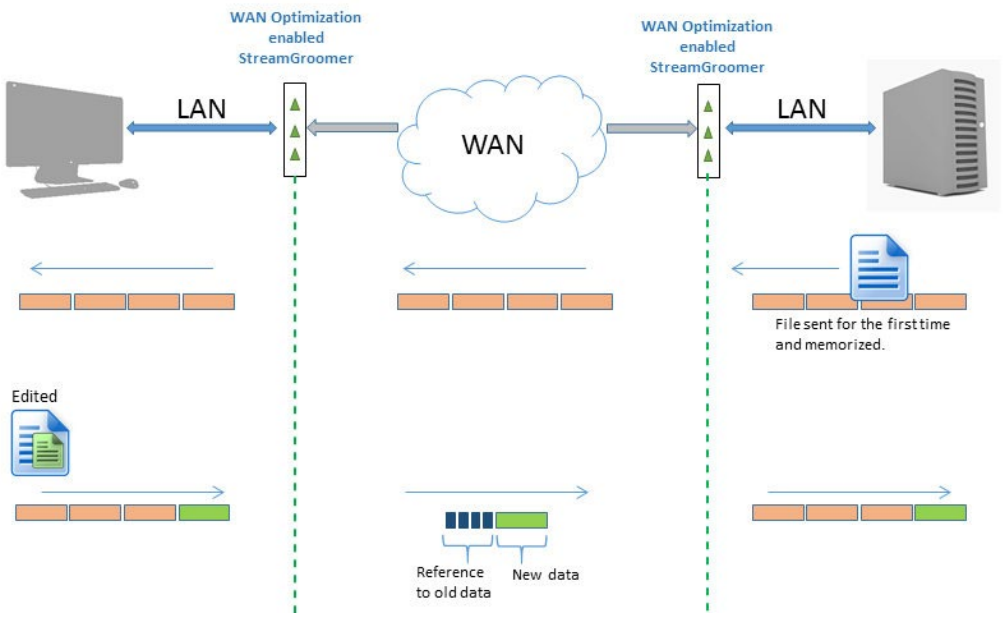


Figure 70 – Cache Optimization

8.1.3 Compression

Streamcore uses the standard lossless compression protocol. It is recommended to use this option in conjunction with the two previously mentioned optimizations.

8.2 GETTING STARTED STEP-BY-STEP GUIDE TO WAN OPTIMIZATION

This section focus on getting you up and running with WAN Optimization. It outlines what you need to get started as-well-as points out some best practices for getting the most out of the available tools.

Note: You should have some previous knowledge of TCP/IP protocol stack, network ports, SSL Certificates and general network architecture in order to understand the guide.

97 STEP 1 – WAN OPTIMIZED STREAMGROOMERS

Streamcore has a range of StreamGroomers that are WAN Optimization compatible, notably the *e*-series boxes:

- *SG360e*
- *SG860e*
- *SG1660e*
- *SG3260e*

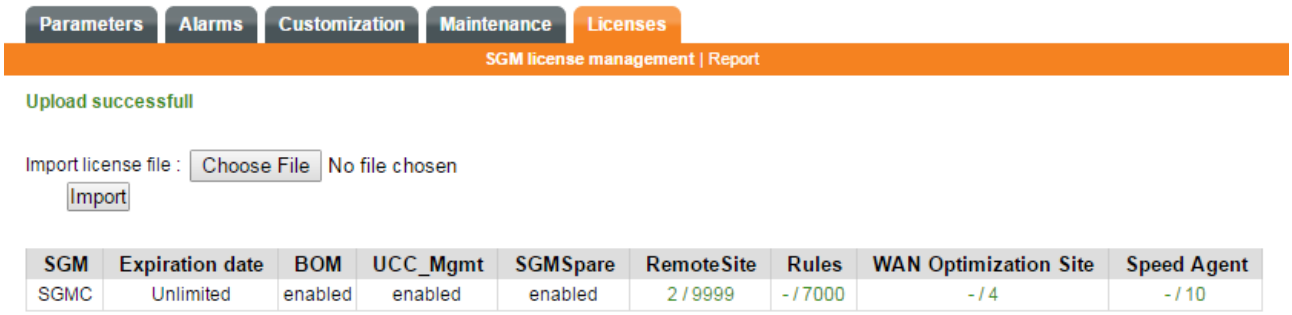
If you do not have any of the above indicated SGs installed, contact Streamcore support to advise you on your options.

Note: For WAN Optimization features, ensure that you have Software Suite v6.3 or later installed.

98 STEP 2 – LICENCES

To implement a WAN Optimization solution, make sure that you have the appropriate licenses installed. Depending on your organizations architecture, you may require several types of license. There are two types of licenses available.

- WAN Optimization Site license – this is a mandatory license that is applied to each WAN optimized site you configure.
- *SpeedAgent* Client license – this license is generally used for offsite users who want to benefit from WAN Optimization. The *SpeedAgent* is installed on a user's mobile device (typically a notebook PC).



SGM	Expiration date	BOM	UCC_Mgmt	SGMSpare	RemoteSite	Rules	WAN Optimization Site	Speed Agent
SGMC	Unlimited	enabled	enabled	enabled	2 / 9999	- / 7000	- / 4	- / 10

Figure 71 – WAN Optimization and Speed Agent licenses activated

You can check if you have the correct licenses from SGMConf by selecting **System > Licenses**.

Use the "Choose File" button to successfully import a license file. In the example displayed above, the user has the ability to deploy 4 sites with WAN Optimization and use 10 SpeedAgents.

Note: If you do not have a WAN Optimization or SpeedAgent license file please contact streamcoresupport@automic.com

99 STEP 3 – WAN OPTIMIZATION BY EXAMPLE

Typically WAN Optimization is deployed when a set of users regularly access application servers based on a remote site. These users need to work seamlessly without latency or delays, which can impede their work.

We are going to implement an example WAN Optimization configuration between a fictional **Branch Office** and **DataCenter** site.

Our example will take on the following characteristics:

1. The Branch Office represents the client site where most users are based.
2. The DataCenter represents the server site where Application servers are accessed by the client.
3. Users who are based in the BranchOffice (local) need fast and easy access to applications stored in the DataCenter (remote).
4. Data flows through the WAN via two routers.
5. A ***SG860e*** is installed in the Branch Office site.
6. A ***SG3260e*** is installed in the DataCenter site.

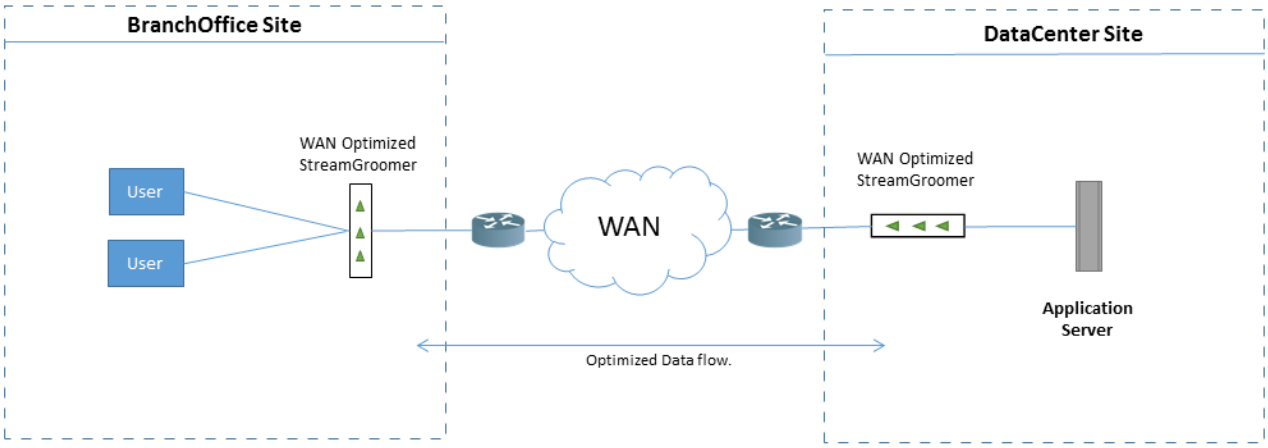


Figure 72 – Basic example of WAN Optimization between Local and Remote Site

100 STEP 4 – PLANNING CHECKLIST

Before setting up you should consider the following:

- The Branch Office site StreamGroomer LAN/WAN address.
- The LAN/WAN address of the Data Center/Application Server StreamGroomer.
- You have a copy of OPE 6.3 or above (required for WAN optimization)
- The LAN gateway switch-router or LAN router addresses (if required)
- The Application Server(s) and/or subnet address that you want to be optimized. For each application server you must enter the port number if they do not use the standard TCP ports. This is defined in the SGs IP router section in StreamView. We recommend that you enter host IP addresses.
- For every application that requires encryption you should prepare SSL Certificates.
- Your organizations firewall should be configured to enable the following TCP ports:
  - 32896 – To send user data for session
  - 32897 – For link management for WAN optimizations
  - 32443 – To secure data for session
- HTTP via Proxy – permissions and ip address information if required.
- VLANs – permissions and ip address information if required.

101 STEP 5 – PROVISIONING SITES AND SGS

In our example, we have provisioned two sites using the StreamView application:

1. **Neptune = Branch Office**
2. **Saturn = DataCenter**

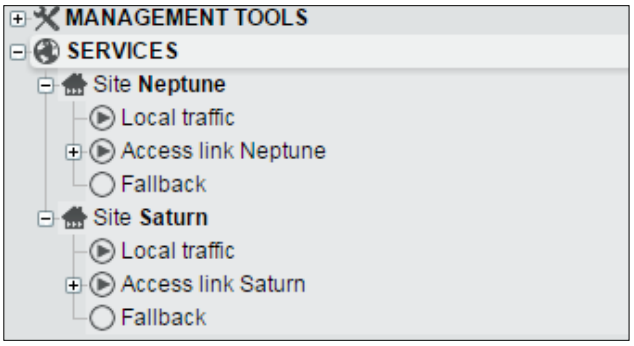


Figure 73 - Two sites provisioned Neptune and Saturn

See Sites Provisioning for further information regarding how to create your sites.

We have also provisioned two StreamGroomers (SGs) using the StreamView application:

1. *SG860e* = **Neptune**
2. *SG3260e* = **Saturn**

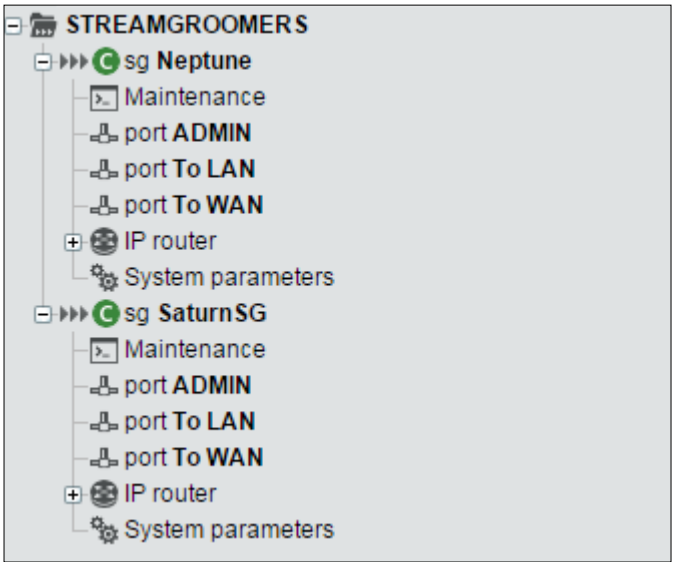


Figure 74 - Two SGs provisioned Neptune and Saturn

Note: In this example we have used the same site and SG names for simplification.

The SGs LAN/WAN address for both the **Neptune** and **Saturn** is entered at SG provisioning stage; as well as the default LAN gateway switch-router or LAN router address for **Neptune** and **Saturn**.

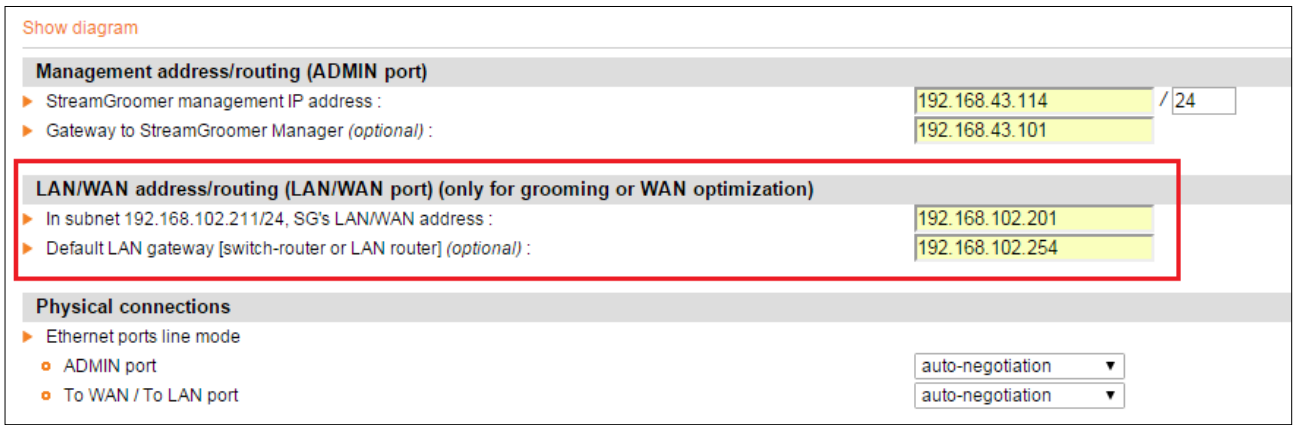


Figure 75 – LAN/WAN Address/Routing information required for WAN Optimization

Our SGs have been set to the operational mode — **Monitoring + Tagging + Control**. It is essential that you change the SG mode to ensure that WAN Optimization functions.

Important: Before you change your SG operational mode, ensure that you have at least Software Suite v6.3 installed on each SG. This step is mandatory in order for WAN Optimization to work. To check your software version click **STREAMGROMMERS>xx Release Management > Read status**.

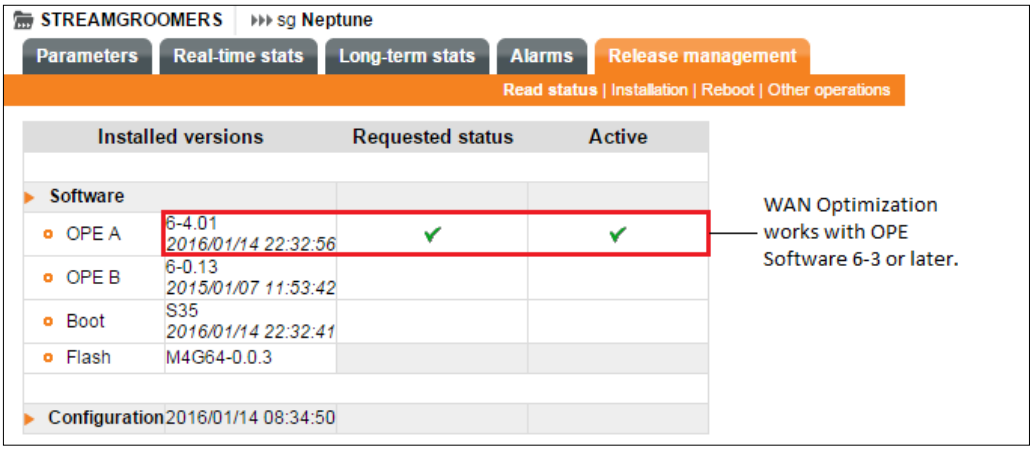


Figure 76 - Check the SG read status to ensure that you have the correct OPE Software installed

To change the SG Operational Mode click **STREAMGROMMERS>xx**, then **Modify** from in the **Parameters tab** and select **Monitoring + Tagging + Control** from the combo box.

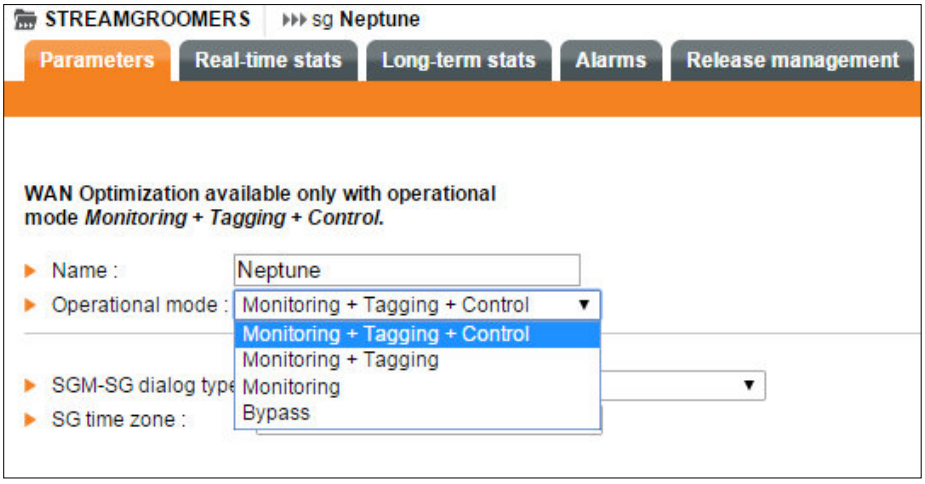


Figure 77 – Select-Monitoring + Tagging + Control for WAN Optimization

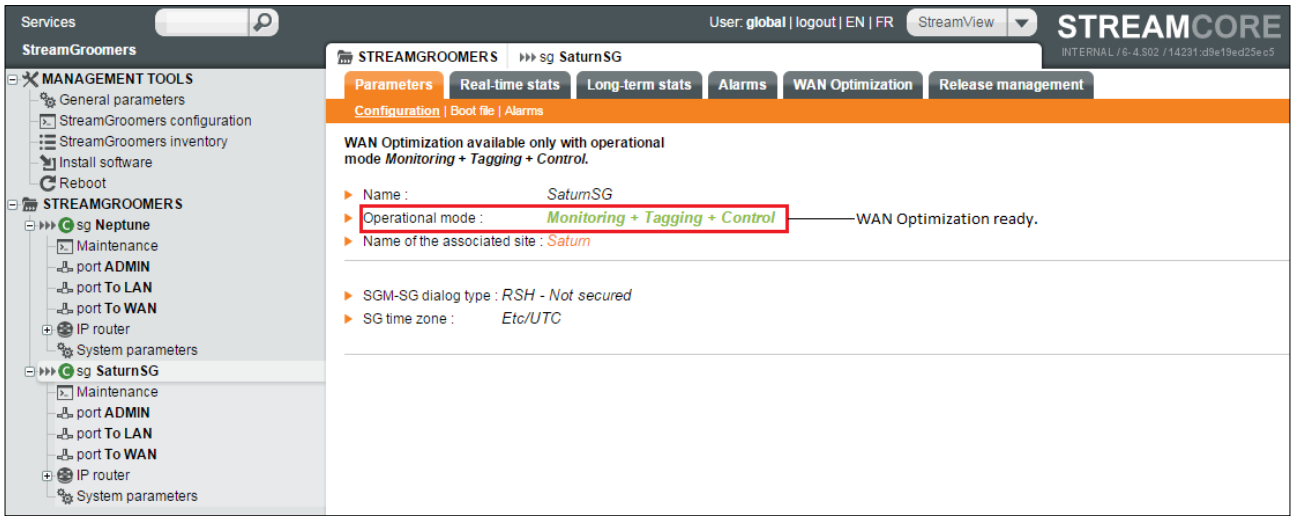


Figure 78 – Our two SGs configured and ready for WAN Optimization

See StreamGroomer Provisioning for an in-depth explanation of each SG setup stage.

Note: The WAN Optimization tab shown in Figure 78 is optional and can be activated during SG provisioning. It is advised that you use this tab for statistical analysis and information only.

102 STEP 6 – OPTIMIZED PEERING

Our two sites **Neptune** and **Saturn** are now ready to be peered using the WAN Optimization Matrix tool.

Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization** then **Matrix** from the displayed list.

By default no Matrix is displayed on the page, use the two main combo boxes to select your options and then click the **Submit** button.

See The Peering Matrix Tool for further details concerning the labels and their functions.

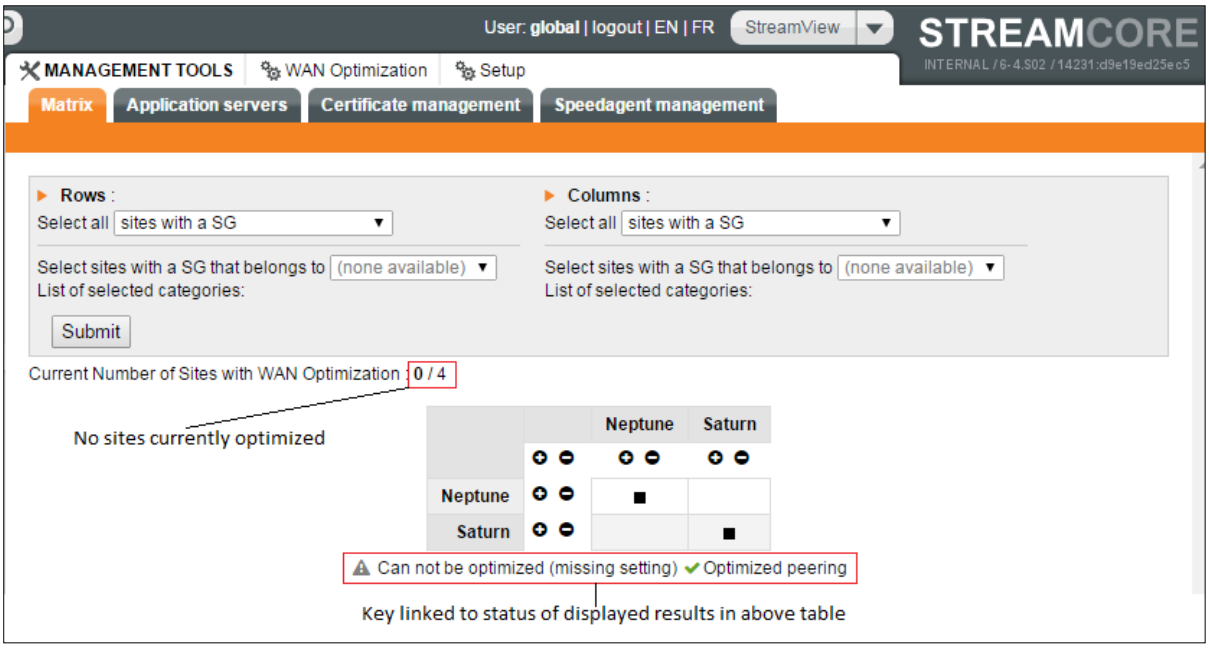


Figure 79 - Matrix displays all sites with SGs but nothing is optimized

After we have selected **Neptune** and **Saturn** to be optimized, we must click the **Submit** button to finalize the process. Notice in Figure 80 that the label "Current Number of Sites with WAN Optimization" still displays "0/4", denoting that no site optimization has taken place.

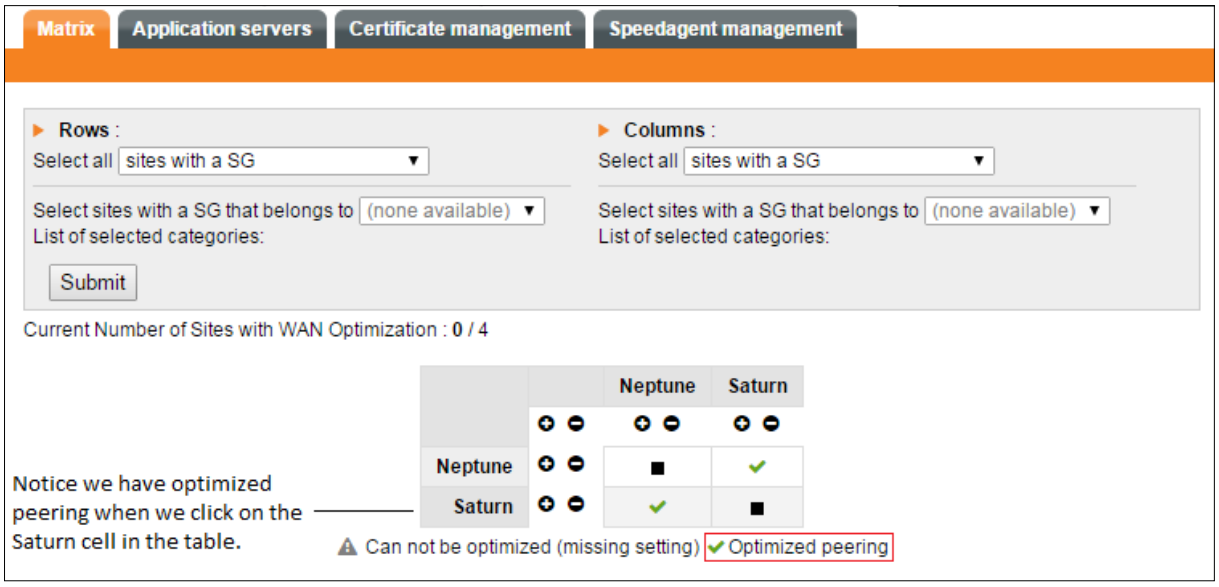


Figure 80 - Displays Matrix when sites can be optimized but no licenses are consumed

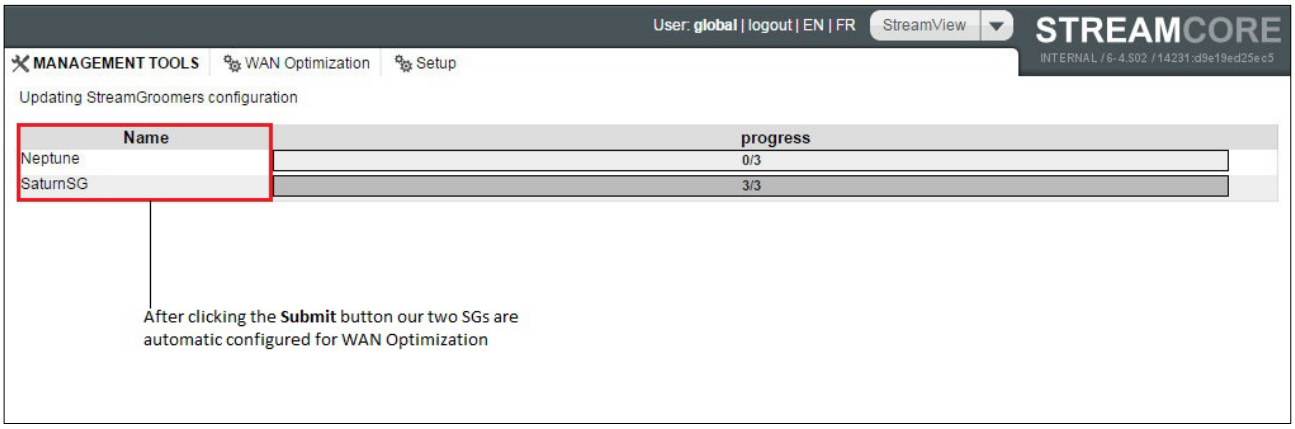


Figure 81 - SGs are automatically configured when the Submit button is clicked

After the WAN Optimization "Submit" button has been clicked and the sites have been configured, the WAN Optimization Matrix is redisplayed. The resulting display now reflects our newly configured sites, notice in Figure 82 that the label "Current Number of Sites with WAN Optimization" has been updated to display "2/4", denoting that our licenses have now been used.

Note: WAN Optimization and Speed Agent licenses are based on a licensing lease system. If you remove a license from a site or mobile device the license is returned to the license pool.

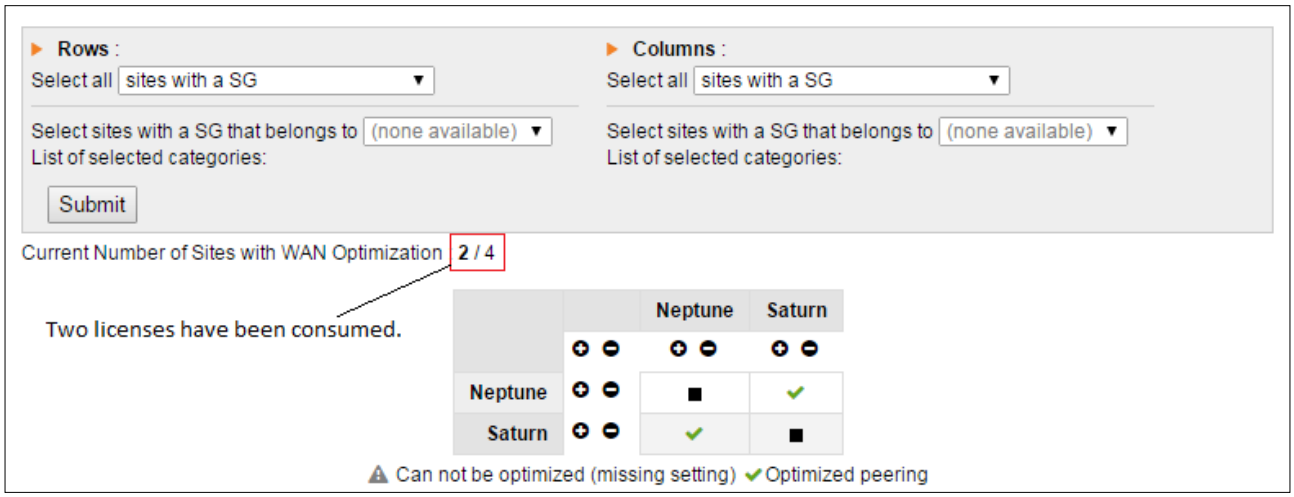


Figure 82 - Optimization configured and two licenses have been consumed

103 STEP 7 – WAN OPTIMIZED APPLICATION SERVER

As we have discovered in the previous step, WAN Optimization between our two sites has been configured. We can now add our Application Server using the Application Server tool.

The first thing that we notice on the Application Server page is that the WAN Optimization configuration has automatically taken into consideration the subnet address of the **Saturn** (Datacenter) site.

Note: This automatic process is configured when you provision your site as a Datacenter at site provisioning stage.

This means that we could in theory activate the entire **Saturn** site (subnet) to active Application Servers using the subnet address. This will work fine you are using a standard default profile and standard SSL certification for all SGs.

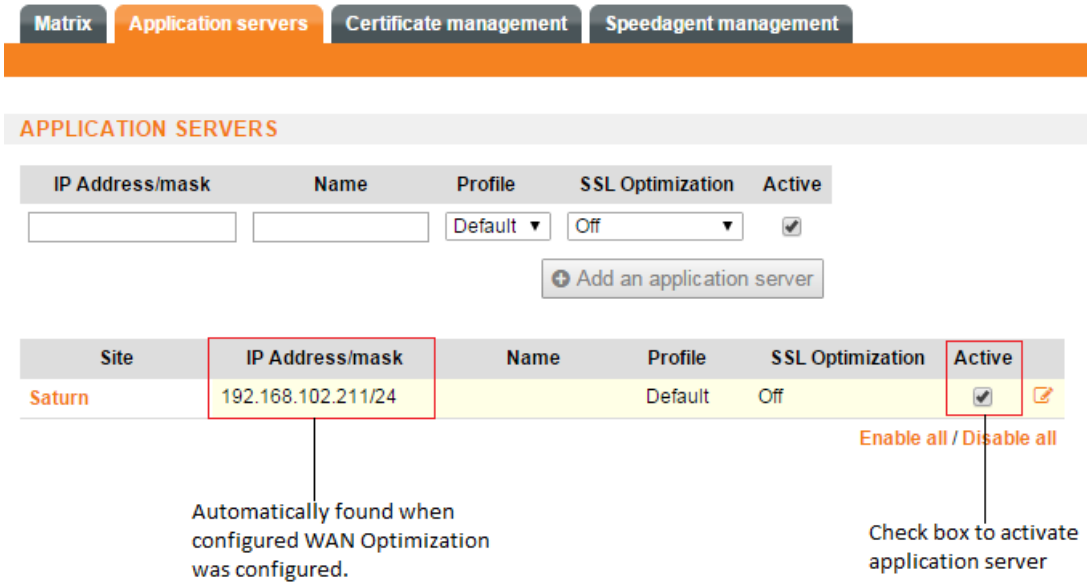


Figure 83 - Subnet address of Saturn Site can be added so all WAN Opt SG are active on subnet

We can be more specific and add the LAN/WAN IP address of our WAN Optimized SG called **Saturn.** This is more useful to us because know that this SG handles specific traffic from our Application Server. This is the traffic we want to optimize.

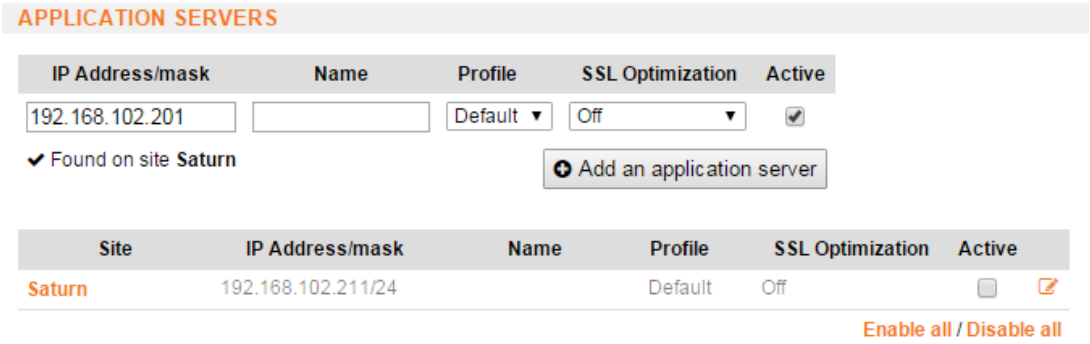


Figure 84 - LAN/WAN address of a WAN Optimization SG

Note: Although the sites have been configured for optimization, traffic between sites will not be optimized until an application server has been enabled.

See Profiles to customize profiles.

See Certificate Management.

104 TESTING OUR WAN OPTIMIZED SITES

To summarize:

- Make sure that you plan before you set up your WAN Optimization.
- Provision your sites and SGs using the appropriate up to date Software Suite.
- Ensure that your provision SGs are in Monitoring + Tagging + Control operational mode
- Select the correct sites with WAN optimized SG using the Matrix tool.
- Add your Application Servers with the Application Server tool
- Add your custom profiles if required
- Manage your certificates if required
- Add your SpeedAgents if required

The following figures demonstrate the effectiveness of WAN Optimization. Here are the results of two passes of data between **Neptune** (Branch Office) and **Saturn** (DataCenter).

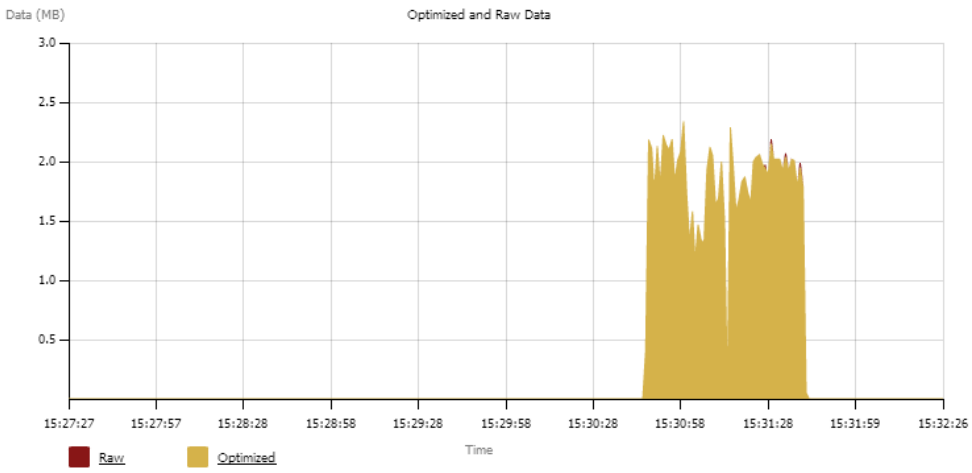


Figure 85 – Data sent to Neptune for the first time to be cached

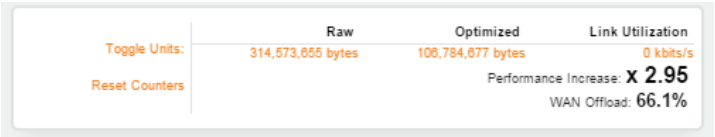


Figure 86 – Stats displaying first send data that is cached

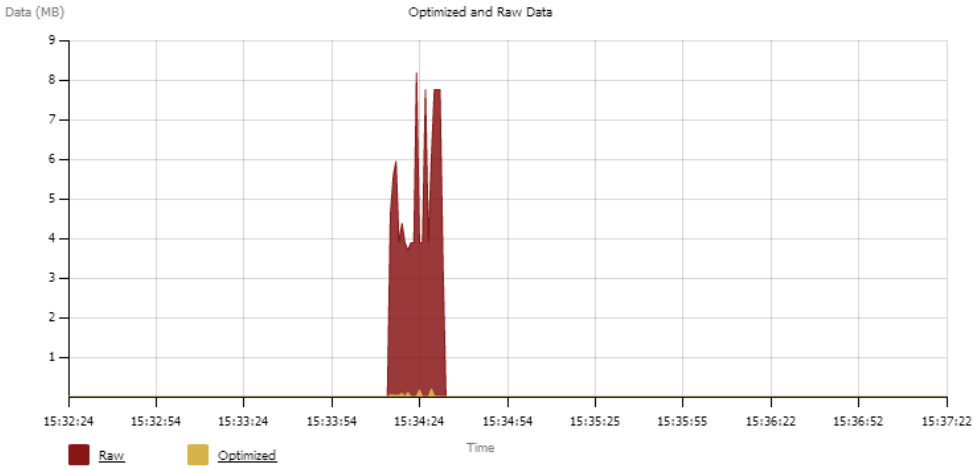


Figure 87 – Data in red is what the Neptune site would have seen if no WAN optimization had taken place

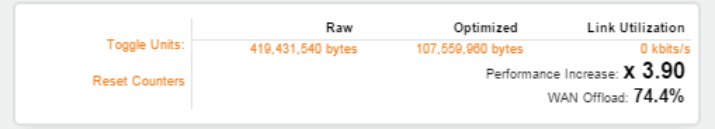


Figure 88 – Stats displaying performance increase and WAN offload increase

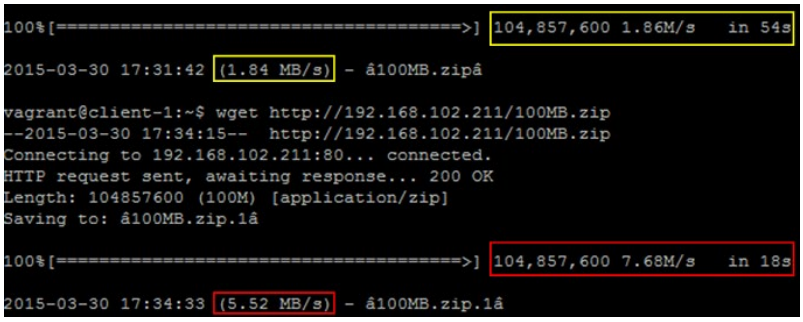


Figure 89 – WAN Optimization demonstrated

For a detailed explanation regarding the live traffic graphs refer to Live Traffic on p194

8.3 GENERAL WAN OPTIMIZATION SETUP

In this section we will detail every task in detail to setup WAN optimization.

The **main** setup parameters can be displayed by clicking Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup**. The page displays four tabs:

- **Peering Matrix –** This matrix allows you to view all SGs that can be WAN Optimized and enables you to activate them for optimization.
- **Application Servers –** This tab allows you to add application servers that you want enabled. Enabling you to specify the server IP Address, Optimization profile.

- **Certificate Management –** This tab enables you to manage SSL Server Certificates.
- **SpeedAgent Management –** The SpeedAgent management tool enables you to manage sites with Speed Agents.

In relation to WAN Optimization there are some common scenarios where user actions might cause certain effects on traffic and user experience. See WAN Optimization – User actions, effects on the traffic and user experience in the Appendix.

8.4 THE PEERING MATRIX TOOL

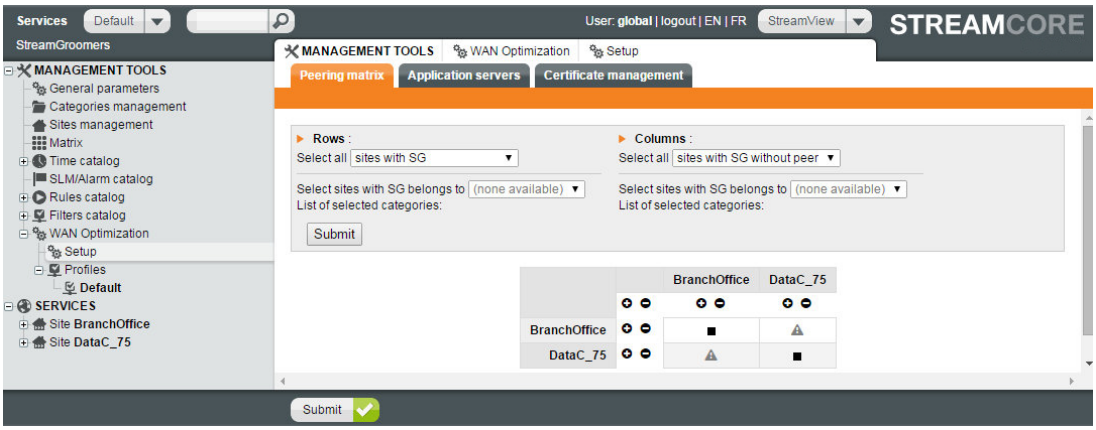


Figure 90 – Peering Matrix

The Peering Matrix tool is design to help:

- Maximize efficiency by providing quick results of sites that can be configured for WAN optimization.
- Display sites without peering enabling you to take necessary action to peer them with other sites.
- Display sites that are not SG enabled. Enables you to identify sites that cannot be WAN Optimized.

By default no Matrix is displayed on the page, however by using the two main combo boxes and clicking the submit button results are shown. Both the row and columns combo boxes contain the following options:

- Sites with SG – sites that are ready to be configured
- Sites with SG without peer
- Datacenter – makes it easy to configure datacenter to site directly to see that act as a datacenter so you can provide direct

Important: Pooling must to setup between WAN Optimized sites to have statistics.

8.5 CONFIGURING ALL SITES WITH SGS

To configure site with SGs:

1. Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup** and select **Peering Matrix**.
2. Select **Sites with SGs** from the **Rows** combo box. Select sites from a category if required by using the additional combo box.
3. Select **Sites with SGs** from the **Column** combo box. Select sites from a category if required by using the additional combo box.
4. Click the **Submit** button to results.

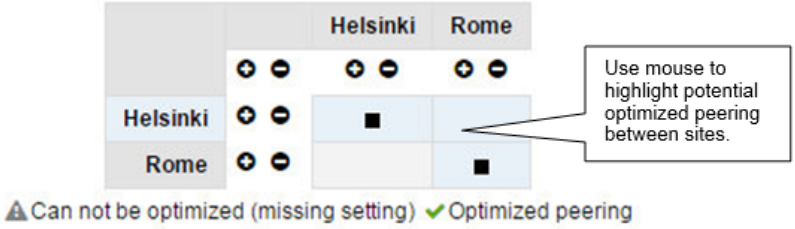


Figure 91 – Creating WAN Optimization between the Rome and Helsinki sites

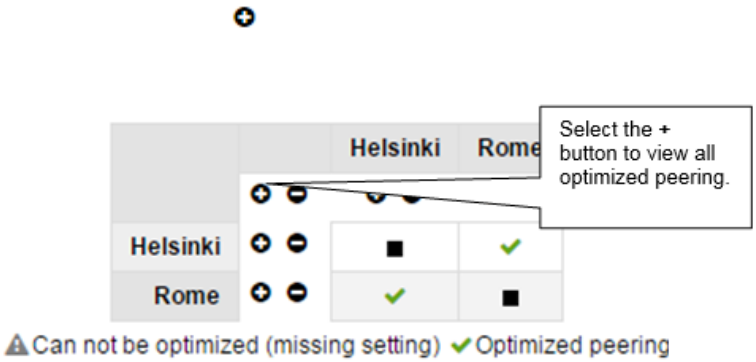


Figure 92 – Display all optimized peering

7. Click the **Submit** button located at the bottom of the page to finalize the WAN Optimization.

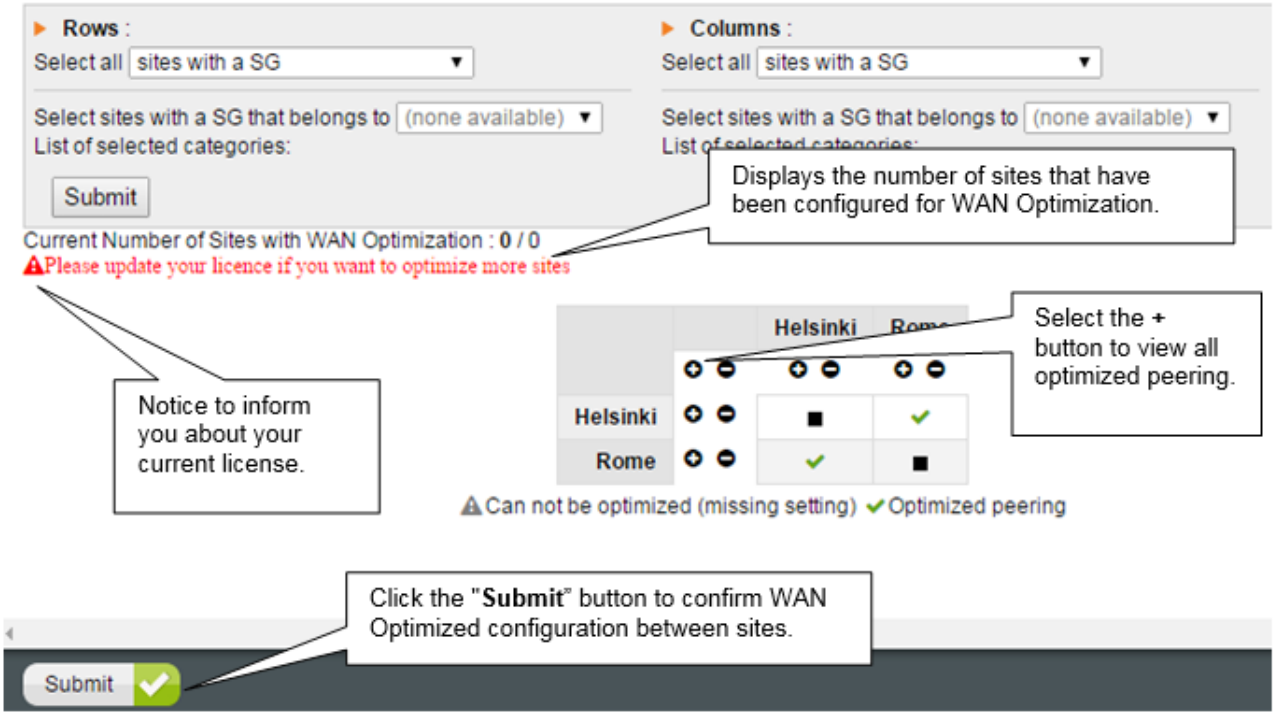


Figure 93 – Sites with SGs and optimized peering

To select all **Sites with SGs** and all sites with **Datacenters** use the same method as describe above by replacing either the row or column combo box with the Datacenter option.

105 MODIFY WAN OPTIMIZED SITES

To modify WAN Optimized sites:

1. Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup** and select **Peering Matrix**.
2. Sites that have been previously optimized will automatically appear on the peering matrix page.

4. Click the **Submit** button and the bottom of the page to confirm your modifications.

106 DELETE WAN OPTIMIZED SITES

To delete WAN Optimized sites:

1. Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup** and select **Peering Matrix**.
2. Sites that have been previously optimized will automatically appear on the peering matrix page.

4. Click the **Submit** button and the bottom of the page to confirm deletion.

8.6 APPLICATION SERVERS TOOL

8.6.1 Add/Modify/Delete Operations – Application Servers Tool

107 ADD AN APPLICATION SERVER

To add an Application server:

1. Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup** and select **Application Servers**.

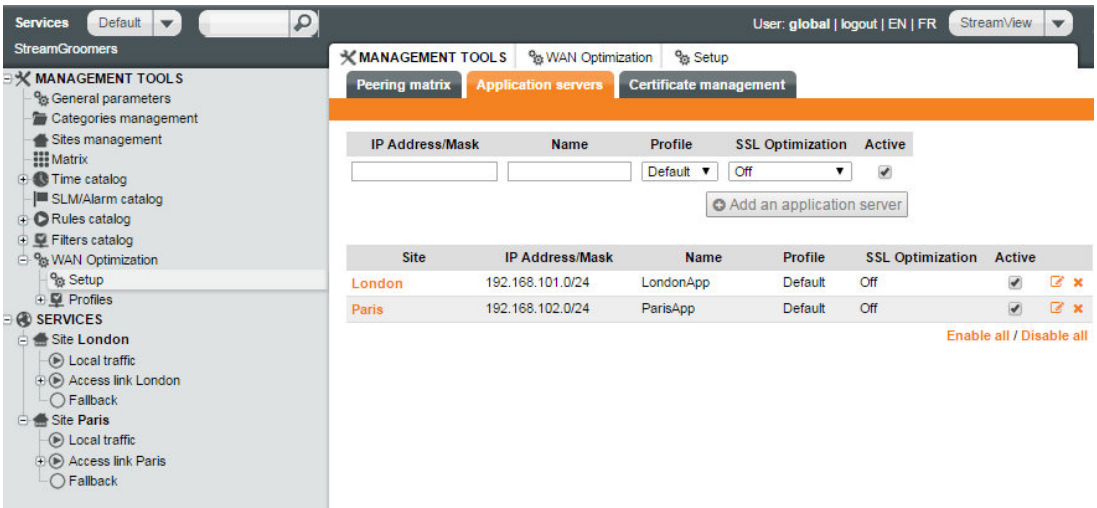


Figure 94 – Adding an Application Server

2. Enter the Application Server IP Address and Mask for example 192.162.xx.xx./24. If a valid application server is found a message will appear "Found on site xxxx". Other messages include "Address not found" and "Duplicate Address/Mask".

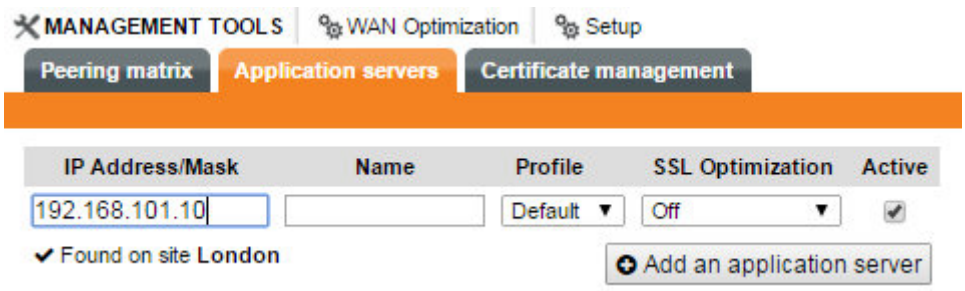


Figure 95 – Application Server Found

3. Enter the application server name for your reference.
4. If you have created a specific profile for an application server, it will appear in the **profile** combo box. The default setting is set to **Default**. Refer to creating profiles for further information.
5. If you are using SSL Certificates they will appear in the **SSL Optimization** combo box providing that you have added them using "Certificate Management". The default setting is **Off**. Refer to Certificate Management for further information.
6. By default, the **Active** checkbox is checked.
7. Select the "Add an application server" button. It will then displayed in the application server table on the page.

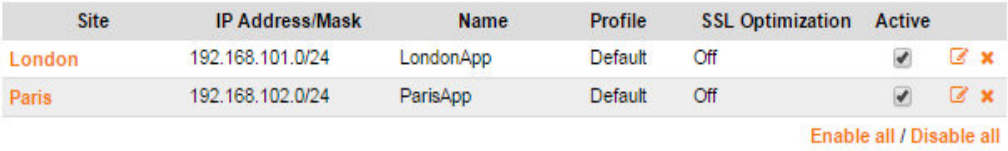


Figure 96 – Application Server Table

108 MODIFY AN APPLICATION SERVER

To modify an Application server:

Figure 97 – Editing an Application Server

2. When the edit mode is enabled, it is possible to modify the **Name**, **Profile**, and **SSL Optimization** sections only. To change the IP address and mask you must add a new application server.
3. After modifications have been made click the **Apply** button to save.

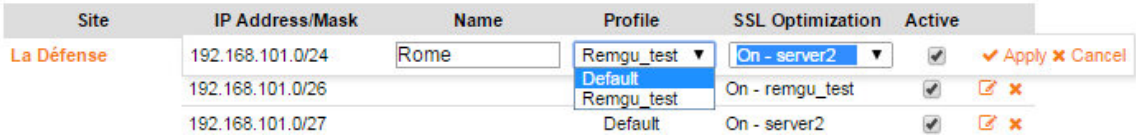


Figure 98 – Modify an Application Server Site

109 DELETE AN APPLICATION SERVER

To delete an application server:

2. Click the **Apply** button to remove the application server or click **Discard Changes** to return the application server to its previous state.

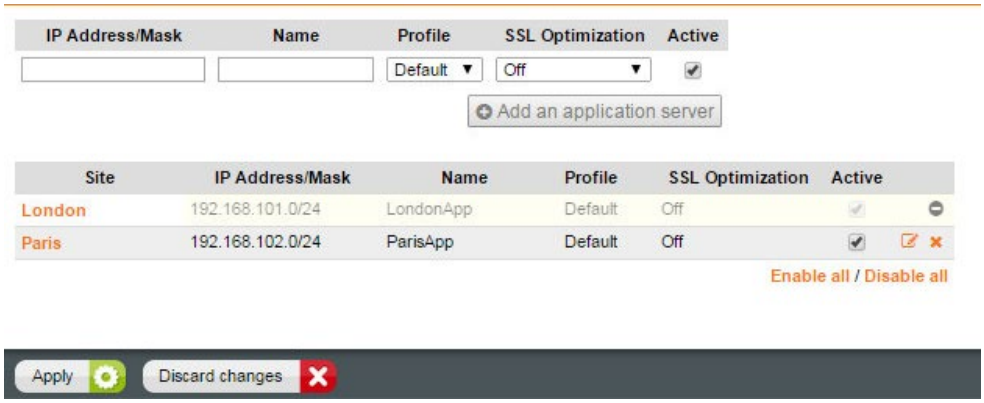


Figure 99 – Application server ready for removal

110 ENABLING AND DISABLING APPLICATION SERVERS

There are several ways to enable or disable application servers. The simplest method is to select either the "Enable all" or "Disable all" button displayed below the application server table. However, this is not always practical when you need to enable or disable specific servers, the **Active** checkbox(s) can be used to enable or disable specific application servers.

Figure 100 – Enables or Disables all Application Servers

111 VIEWING WAN OPTIMIZATIONS ON A SPECIFIC SITE

By clicking on a site name from the application table you will be directed to **SERVICES > … > Site xx >** to the **Parameters** tab and WAN Optimization sub-tab.

This displays a site configured application servers and enables you to have a clear view of all of the sites all optimizations.

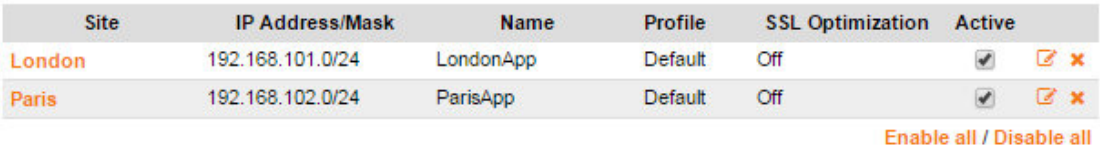


Figure 101 – Site WAN Optimizations

8.7 CERTIFICATE MANAGEMENT

8.7.1 Add/Modify/Delete Operations – Certificate Management

112 ADD A SSL CERTIFICATE

To add a SSL Certificate:

1. Click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization > Setup** and select **Certificate Management**.
2. The first time you use the certificate management tool you will be required to create a **SGM Certificate** vault password. Set your password, confirm the password and then click the **Submit** button.

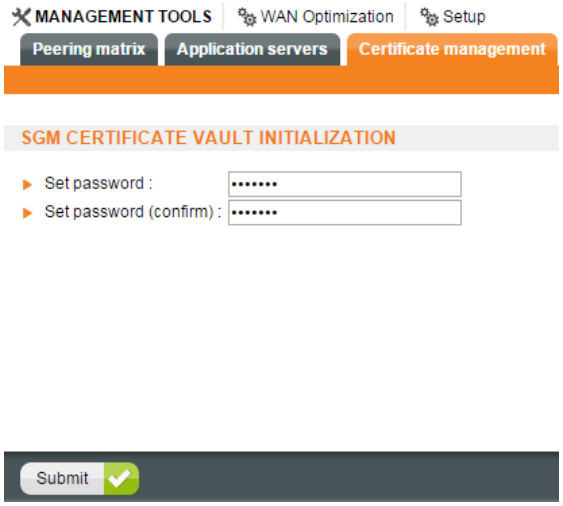


Figure 102 – Set certificate vault password

3. When you have unlocked the vault, you will be able to import specific certificates and keys. Select the **Import SSL Server Certificate** button.

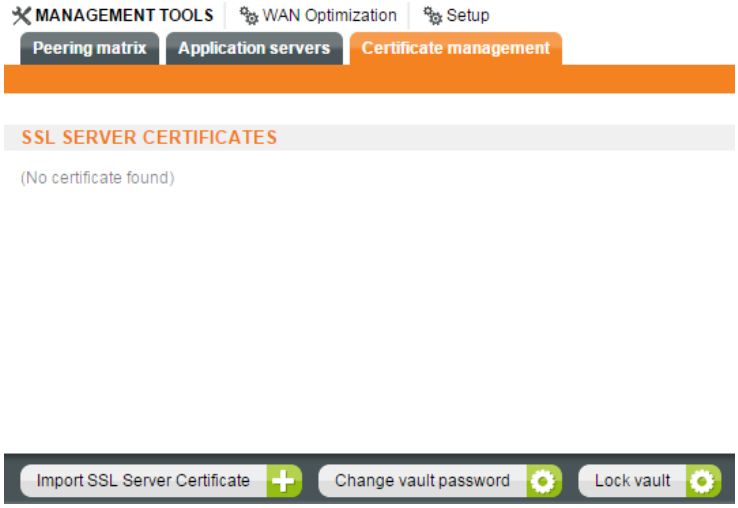


Figure 103 – Import a SSL Certificate

4. The import ssl server certificate enables you to specify certificate parameters.

Parameter	Description / Values
Import SSL Server Certificate	
Alias	Enter a display name that you can identify when adding the certificate in the **SSL Optimization** combo box in the **Application Server** tab when you.
Certificate files	Two options are available select an option using the radio button:

	Two files: certificate and private key (PEM). One file should contain a server certificate, added by using the "Public certificate" selection button. The other file should be a private key, added by using the "Private key" selection button. **One file:** contains the certificate and private key (PFX/PKCS#12).
Public certificates	Use the button to add your server certificate (.crt).
Private key	This button is only active when two file PEM the "Two files" Use the button to add your key (.pem).
Password	Enter the private key password.

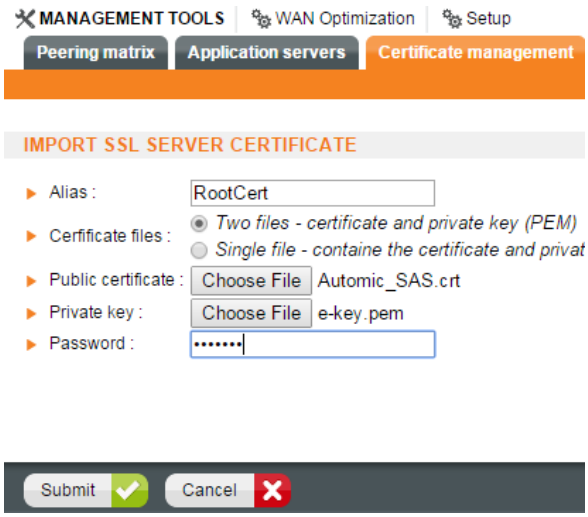


Figure 104 – Importing SSL Server certificate

Figure 105 – Imported certificates

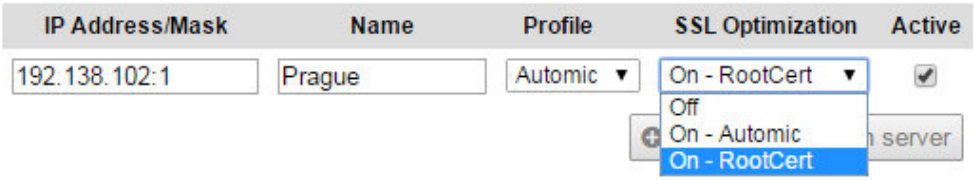


Figure 106 – Applying imported certificate to application server

113 DELETE A SSL CERTIFICATE

To delete a SSL server certificate:

1. Unlock the vault by selecting the **Unlock Vault** button, entering the password, and then clicking **Submit**.

2. Select the SSL server certificate to delete. The row will appear greyed–out.
3. Click the **Apply** button to delete the certificate.

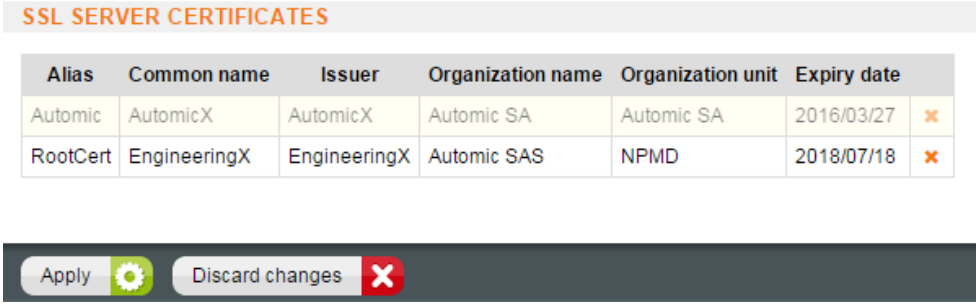


Figure 107– Delete a certificate

114 CHANGE THE SGM VAULT PASSWORD

To change the SGM vault password:

1. Unlock the vault by selecting the **Unlock Vault** button.
2. Click on the **Change vault password** button. To open the vault password modification page.
3. Enter your current password.
4. Enter a new password and enter the same password to confirm.
5. Click the **Submit** button to apply changes to your password.

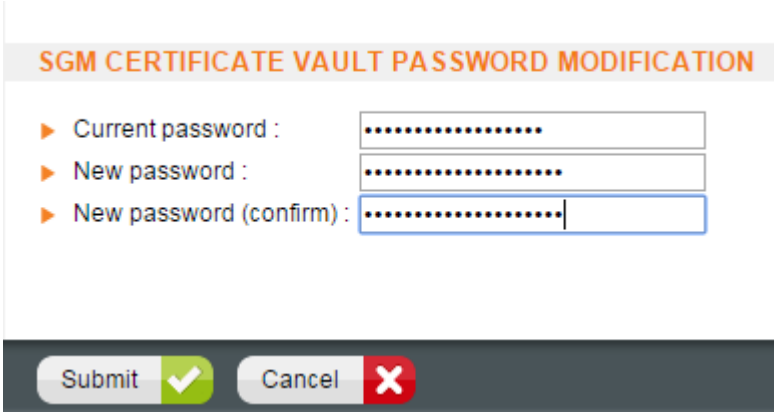


Figure 108 – Change SGM vault password

8.8 *SPEEDAGENT* CLIENT MANAGEMENT

SpeedAgent clients can be installed on clients (PCs or Mobile devices) device that connect to a site can have the ability to utilize the benefits of WAN Optimization.

Refer to the *SpeedAgent* client's setup guide.

SpeedAgent tokens are managed and distributed on a site-to-site basis. They are distributed via the Speed Agent management page. To access this page click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization >Setup** and then select the ***SpeedAgent* management** tab.

Typically, the *SpeedAgent* management page will consist of all sites that have WAN Optimization configured along with their defined maximum SpeedAgent tokens.

Parameter	Description / Values
SpeedAgent Management	

Currently Defined (Label)	Displays total available tokens and the number of tokens that have been allocated to WAN optimized sites.
Site with WAN Optimization	Displays sites that have had WAN Optimization configured.
Max *SpeedAgent* (Tokens)	Displays the maximum amount of *SpeedAgent* tokens that a site has been allocated.
Action	This column allows you to use the *add* or subtract *SpeedAgent* tokens to a site. It is also possible to freely enter a number in the box.

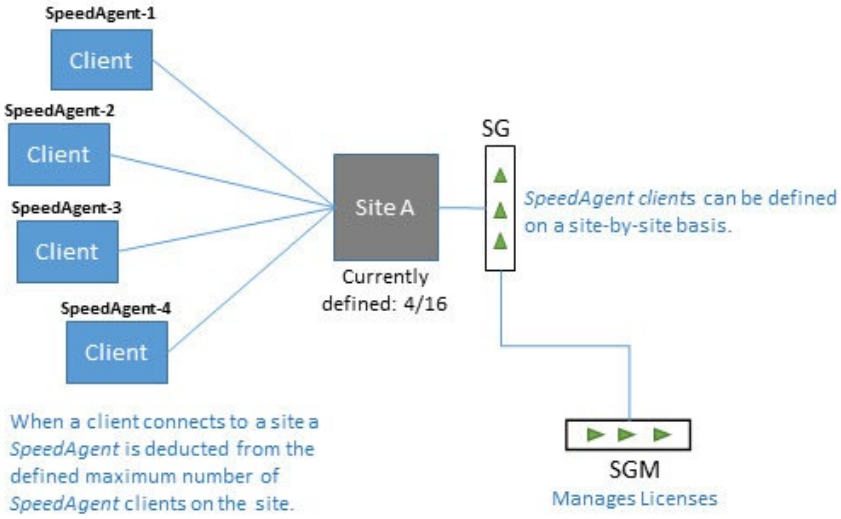
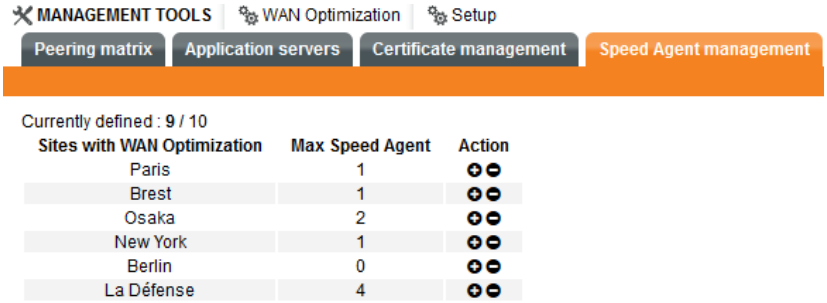


Figure 109 – Clients and SpeedAgent Clients

Note: Licence management is done via the SGM.



Sites with WAN Optimization	Max Speed Agent	Action
Paris	1	
Brest	1	
Osaka	2	
New York	1	
Berlin	0	
La Défense	4	

Figure 110 – Speed Agent management defined

115 ADD A SPEEDAGENT TO A SITE

To add a *SpeedAgent* to a site:

1. Select the site from the listed WAN Optimized sites.
2. Either enter the number of *SpeedAgent* clients you require or use the action button to add Agents.
3. Click the **Submit** button to apply.

Note: If a sites defined “Max SpeedAgent” clients are used, all subsequent clients that connect will not benefit from WAN optimization until a connection becomes available.

116 DELETE A SPEEDAGENT FROM A SITE

To remove a *SpeedAgent* from a site:

1. Select the site from the listed WAN Optimized sites.
2. Either enter "0" to remove all *SpeedAgent* clients associated with the site or use the minus action button to remove Agents one-by-one.
3. Click the **Submit** button to apply.

Note: If a client disconnects from a site the *SpeedAgent* is added back to defined *SpeedAgent* amount for the site.

8.9 PROFILES

The profile contains a set of predefined common protocols with their optimizations fixed. The profile can be applied to any application server using the **Profile** combo box provided in the **Application Server** tab.

8.9.1 The Default Profile - Getting Started

To access the profiles page click on **SERVICES > … > MANAGEMENT TOOLS> WAN Optimization >Profiles**. Streamcore provides a default profile for WAN Optimization. The default profile cannot be edited however; it is possible to duplicate it by clicking the **Duplicate** button located at the bottom of the page.

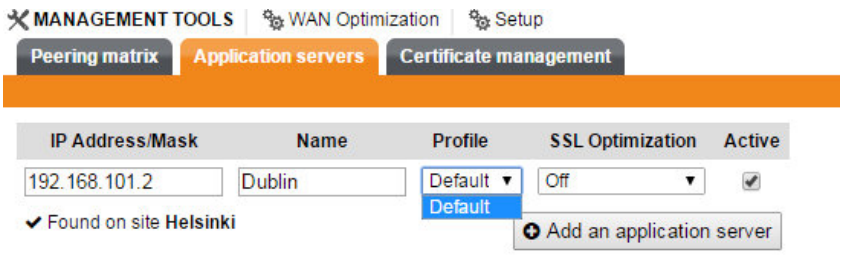


Figure 111 – Applying the default profile to an application server

The following protocols with their common ports and optimizations are listed in the default profile:

- Name : *Default*
- Description : *Default service profile*

Name	Protocol	Port(s)	Optimizations
CIFS	CIFS	139, 445	✔ Protocol ✔ Cache ✔ Compression
DNS	DNS	53	✔ Protocol ✘ Cache ✔ Compression
Double Take	Double Take	1100, 6320	✔ Protocol ✘ Cache ✔ Compression
EqualLogic	EqualLogic	3260	✔ Protocol ✘ Cache ✔ Compression
FTP	FTP	21	✔ Protocol ✔ Cache ✔ Compression
HTTP	HTTP	80, 443, 8080	✔ Protocol ✔ Cache ✔ Compression
MAPI	MAPI	dynamic	✔ Protocol ✔ Cache ✔ Compression
Remote Desktop	Remote Desktop	3389	✔ Protocol ✘ Cache ✘ Compression
Secure IMAP	Secure IMAP	993	✔ Protocol ✘ Cache ✘ Compression
Secure POP3	Secure POP3	995	✔ Protocol ✘ Cache ✘ Compression
Secure SMTP	Secure SMTP	587	✔ Protocol ✘ Cache ✘ Compression
SSH	SSH	22	✔ Protocol ✘ Cache ✘ Compression
Fallback	Default	all	✘ Protocol ✘ Cache ✘ Compression

Figure 112 – Default Profile

Note: If you have recently migrated to Streamcore v6.4 (or above) you will notice that the default profile now includes a Fallback service. If you have existing custom profiles you should modify them if you want to optimize Fallback services. By default Fallback services are not optimized.

Important: If your SGM is using version 6.4 and your SG is in still using version 6.3, there will be a misalignment with regards to existing profiles. Therefore your existing profiles will not be optimized. If this is the case you should align either your SGM or SG to the same version.

8.9.2 Add/Modify/Delete Operations – Profile Customization

117 ADD A PROFILE (DUPLICATE DEFAULT)

As mentioned above it is possible to duplicate the default profile in order to create a custom set of protocols with their specific ports and optimizations. After clicking the duplicate button, a copy of the default profile will be displayed.

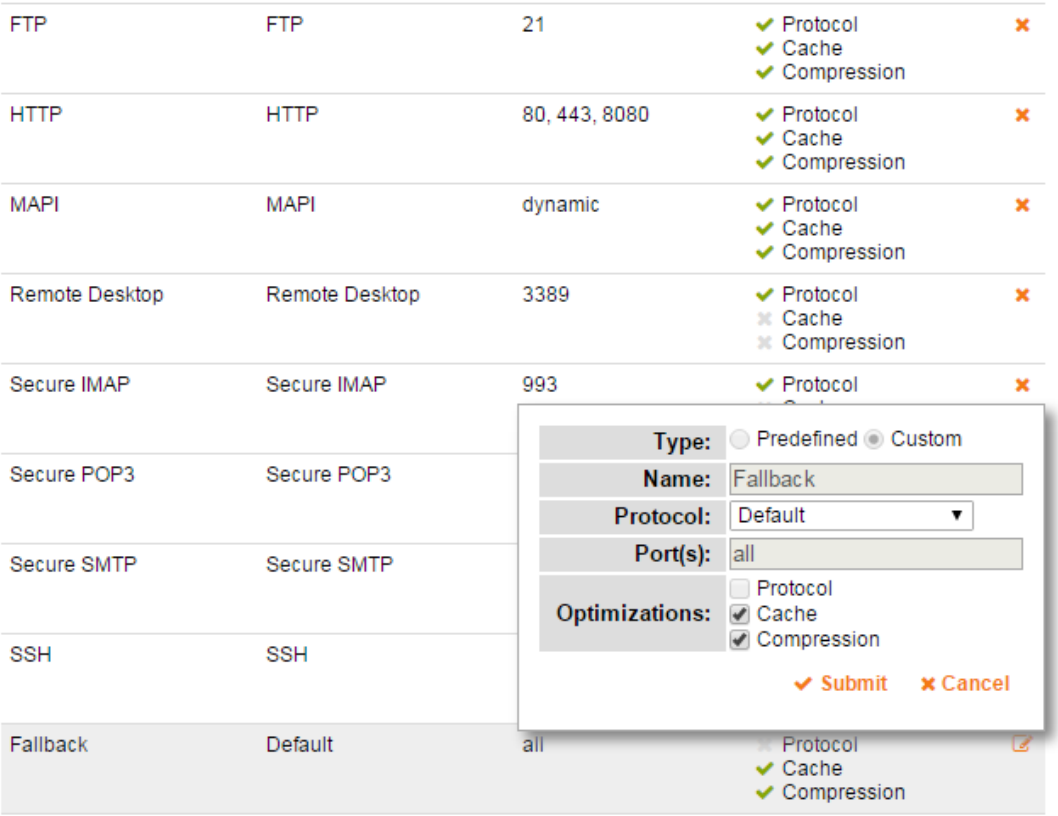


Figure 113 – Duplicated Default Profile and optimizing Fallback traffic

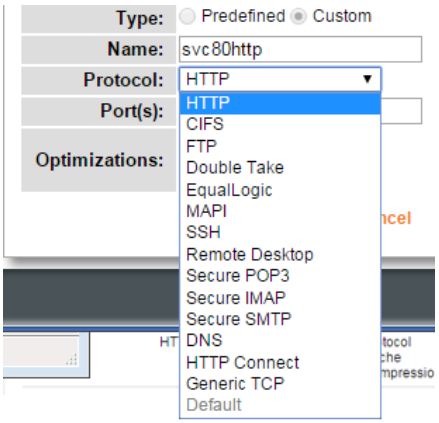


Figure 114 - Adding a protocol

118 MODIFYING

Click the **Modify** button to begin customizing the default profile. The name and description boxes are now active and can be freely edited. The default protocols can be removed and a new service protocols can be added.

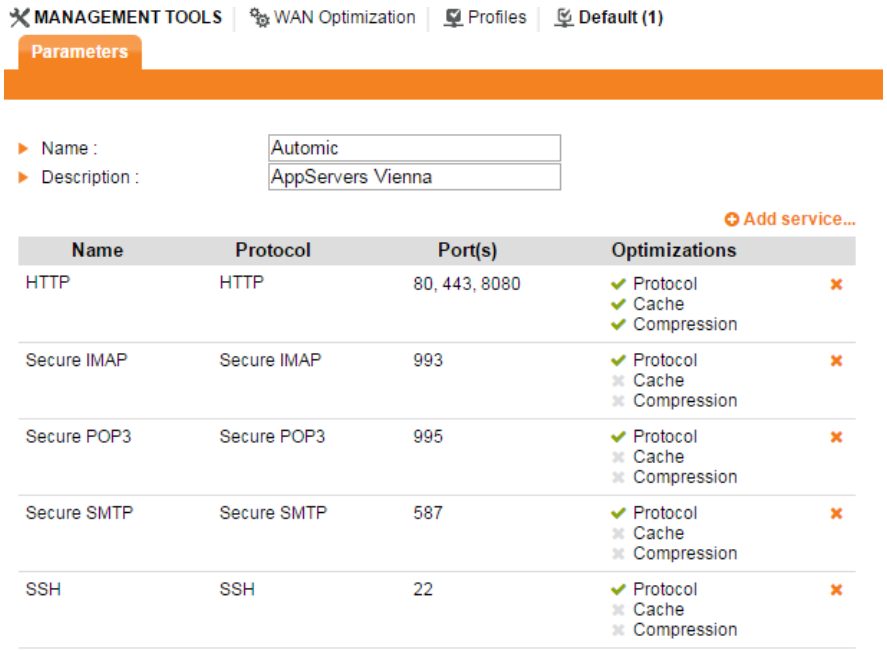


Figure 115 – Modified duplicate default profile

Add a Service Protocol

Adding a service is done by clicking the **Add service** button. There are two options available when using this feature:

- **Predefined**
  - This option provides a combo box with a set of the predefined protocols; however, it is not possible to edit the name, port or optimization sections.

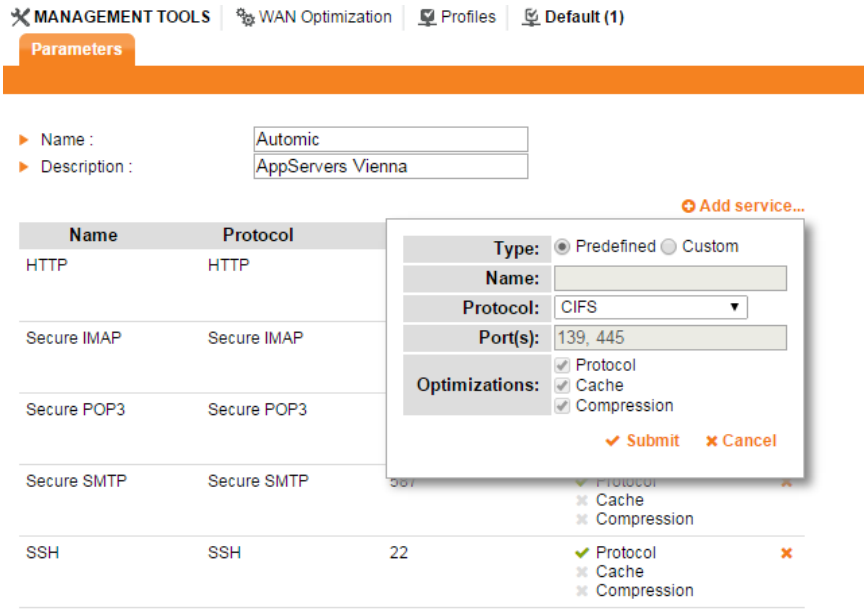


Figure 116 – Predefined Service

- **Custom**
  - This option provides the ability to freely edit all defined selections.

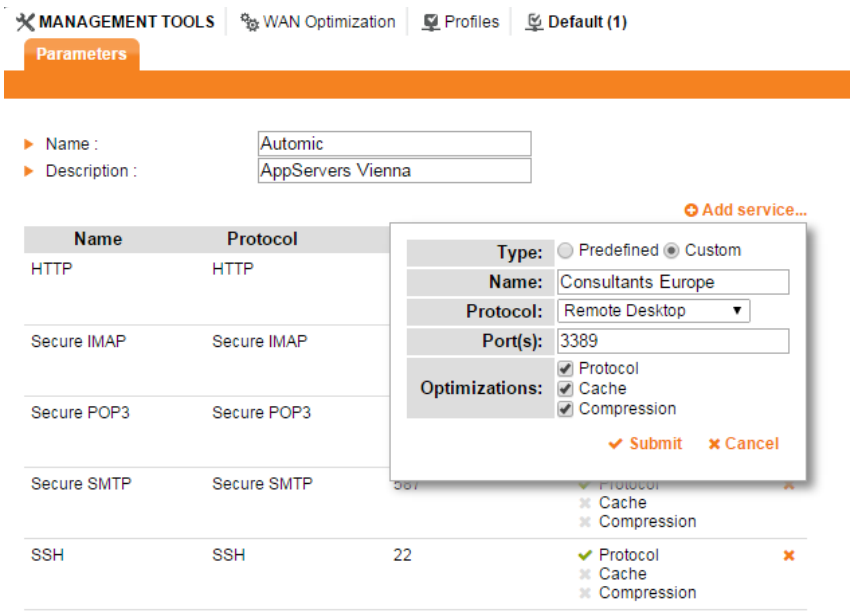


Figure 117 – Custom Service

After creating your new profile, it is possible to apply it to any application servers using the **Application Server** tab.

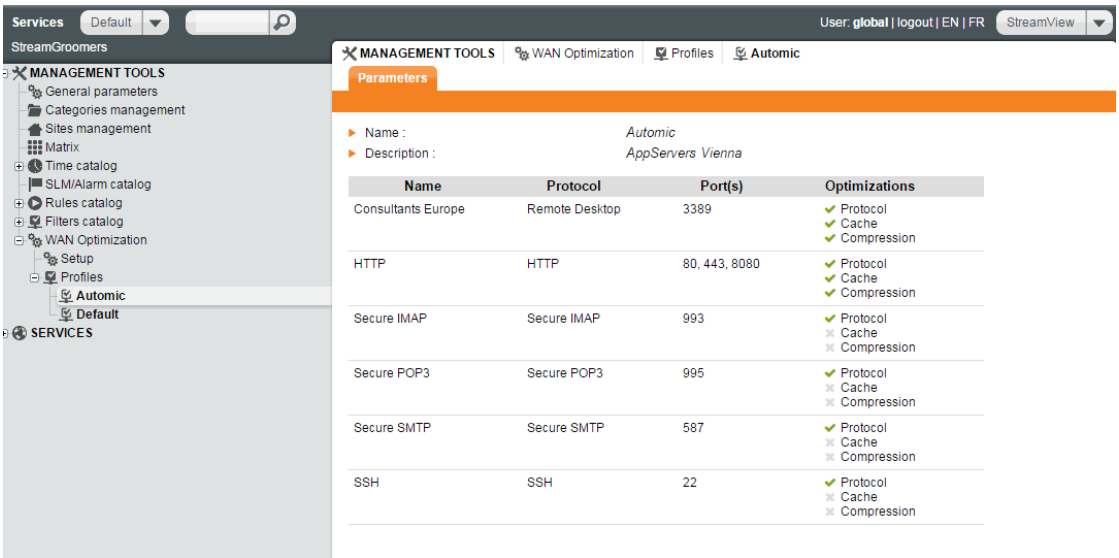


Figure 118 Custom profile

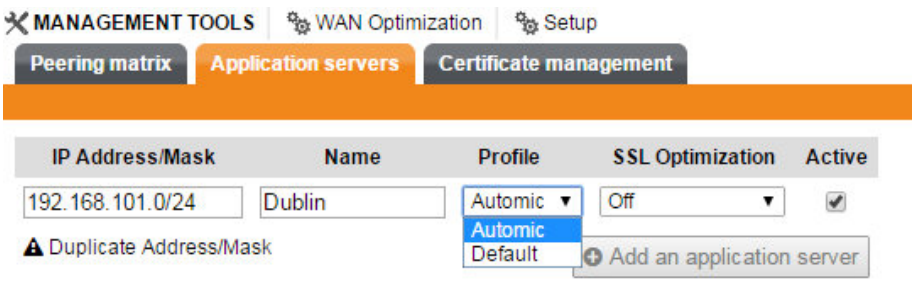


Figure 119 – Apply custom profile to application server

119 DELETE A CUSTOM PROFILE

To delete a custom profile select the profile from the tree menu, right click and select **Delete**.

9 Visibility Services

9.1 OVERVIEW

9.1.1 Types of Visibility Services

Streamcore visibility services are accessed via a system of tabs for each object in the Unified Mapping Tree (*category, site, external probe, and rule*). Some of these tabs have a set of sub-tabs providing access to specific tools.

The tabs differ depending on the type of object selected in the Unified Mapping Tree, as shown in the following table:

		Services Configuration	Visibility Services		
	Category	Parameters	Long-term stats	Alarms	
	Site	Parameters	Real-time stats	Long-term stats	Alarms
	External Probe	Parameters	Netflow		
	Rule	Parameters	Real-time stats	Long-term stats	Troubleshooting

	CATEGORY AND SITE VISIBILITY SERVICES			
	Information granularity	Time span		
	Rule[1]	Last 10 sec. 1 min.	Last 10 min.	Long-term
Real-time stats	X	X	X	
Long-term stats	X		X	X
Alarms	X		X	X

Note: The external probe time span is based on Long-term statistics only.

[1] Visibility services based on statistics aggregated for all traffic classified in a rule

	RULE VISIBILITY SERVICES					
	Information granularity			Time span		
	Rule	Session[2]	Packet[3]	Last 10 sec. 1 min.	Last 10 min.	Long-term
Real-time stats	X			X	X	
Long-term stats	X				X	X
Troubleshooting		X		X	X	X
			X	X		

Note: A tab giving access to LAN troubleshooting tools can also be available for sites with a StreamGroomer.

[2] Visibility services based on statistics per session/communication

[3] Visibility services based on statistics per packet

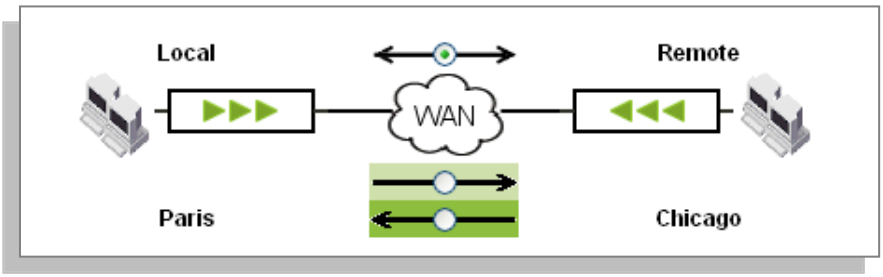
9.1.2 Using the Visibility Services

120 DIRECTION OPTIONS

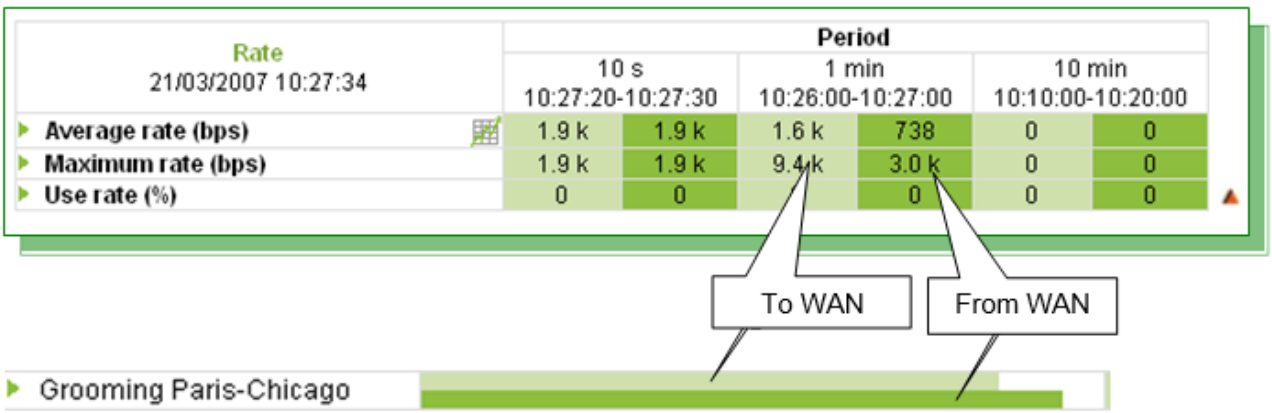
Navigating through the Unified Mapping Tree (UMT) for a site is equivalent to being virtually positioned within the site. This concept is fundamental to an understanding of the concepts of local and remote locations as used on the screens. All references to "local" designate the site where navigation is taking place.

121 REAL-TIME STATS

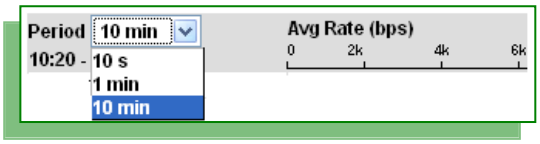
For each sub-tab of the ***Real-time stats*** tab, you can define the traffic direction to be displayed. Selection is done through a diagram that identifies the local and remote sites via a system of radio buttons and a color code:

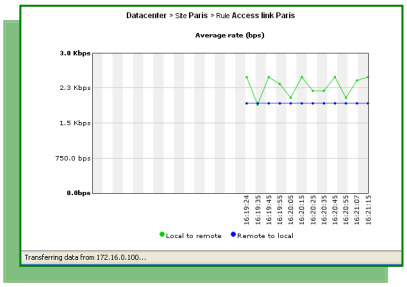


When both directions are chosen, the results are shown according to the two traffic directions using the same color code:



In real time – and apart from the indicator pages for which the 3 periods are displayed automatically – the observed period can be 10 seconds, 1 minute, or 10 minutes. The selection is made via a scroll-down menu in the result zone, and the page is reloaded automatically:

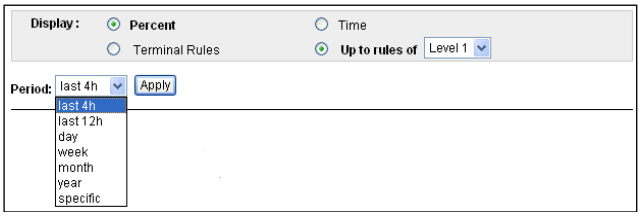


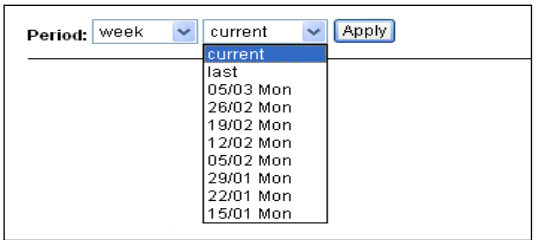


122 LONG-TERM STATS

Period selection

As for the Long-term stats, use the following procedure to select the period:





Graph export

Every graph from the **Long-term stats** tab can be exported into different formats. The available formats are: *png*, *xml*, *csv*.

The export links are available above every graph (mouse on export...).

The StreamDashboard export adds the selected graph in a view from the StreamDashboard application (*cf. StreamAccess/StreamDashboard guide for detailed information*).

Graph type

In SGMConf / System / Configuration, you can define the type of graph displayed in "Long-term stats" between:

- PNG (default choice): light and cacheable graphs without point overcaption
- Flash graph with point overcaption option

Automated display of consolidated graphs

On a site or a category, it can take time to display consolidated graphs in "Long-term stats" if there are a large number of network rules (shaping / grooming).

In Services, select **MANAGEMENT TOOLS>General parameters**, we can configure a limit number of the network rules for the automatic display of graphs. By default, this parameter is 10 network rules.

Graph granularity

- 10 minutes: 7 days
- 30 minutes: 14 days
- 2 hours: 2 months
- 1 day: 2 years

Note: A point in a graph always represents the next period. Example: a point at 4:30 represents statistics for the 4:30-4:40 period (10 minutes granularity) or 4:30-5:00 (30 minutes granularity).

9.2 VISIBILITY PARAMETERS

9.2.1 Real-Time / Long-Term Statistics Provisioning

123 OVERVIEW

Generic indicators are computed by default in all rules by the StreamGroomers, such as Throughput, Load or Frame related indicators.

Additional performance indicators can be computed depending on the type of rule: network, application or VoIP/Video performance.

124 NETWORK PERFORMANCE MEASUREMENTS

Local access link performance monitoring

For sites equipped with a StreamGroomer, the local access link availability can be monitored for backup link management (see chapter 7.3.5), but also to measure network performance. In order to do so, the active probe must be based on the ping mechanism (and not SNMP). The StreamGroomer will measure the availability, latency and packet loss of the network link between the access router and the first service provider node (provider edge router in an MPLS environment for instance).

To configure the active probe to measure network performance:

1. Select the *Parameters – Configuration* sub-tab of an access link rule. Click on the **Modify** button
2. Select the "Ping" active probe, enter the parameters and click on the **Submit** button

Parameter	Description / Values
Access link availability monitoring	
Access link availability detection	Ping
IP address of the router to be polled	IP address of provider edge router
Frequency of the active probe	1, 2, 5, 10 seconds

Note: The ping traffic is launched from the StreamGroomer Administration Ethernet port. A default route must therefore have been configured for the ADMIN port (see chapter 4.2.4).

Grooming/Shaping rules: end-to-end network performance monitoring

The LMP (Link Management Protocol) established between two StreamGroomers that are exchanging traffic within a Grooming rule **automatically** provides network performance measurements (availability, latency, packet loss, jitter). There is no need for specific configuration. The only condition is that the Grooming must be synchronized.

In order to monitor end-to-end network performance in a Shaping rule, an active probe can be launched by the StreamGroomer to measure the availability, latency and packet loss between the StreamGroomer and the remote site access router.

To configure the active probe to measure network performance:

1. Select the *Parameters – Configuration* sub-tab of the shaping rule. Click on the **Modify** button
2. Enter the following parameters and click on the **Submit** button

Parameter	Description / Values
Active probe	
Active probe availability	Ping
Destination address for active probe	IP address of the remote WAN access router
Frequency of active probe	1, 2, 5, 10 seconds

Note: The creation wizard for shaping rules through the tree menu (see chapter 7.4.4.1) or the matrix management tool (see chapter 7.4.5.3) automatically fill the "Destination address for active probe" parameter if the IP address of the WAN access router has been defined on the remote site.

Note: The ping traffic is launched from the StreamGroomer Administration Ethernet port. A default route must therefore have been configured for the ADMIN port (see chapter 4.2.4).

Note: *The shaping active probe can be enabled/disabled on a set of sites:*

- *Select **MANAGEMENT TOOLS > Sites management**, and click on the **Set parameters** tab*
- *Select sites, and the "Active probe shaping" parameter.*
- *Click on the* **Apply** button

Grooming/Shaping rules: network SLM measurements

When network performance monitoring is enabled on shaping or grooming rules, network SLM measurements (available only on long-term statistics) can be activated on the StreamGroomer.

To automatically activate network SLM measurements, add a "Network SLM" (special group of alarms) on the shaping or grooming rule (see chapter 9.2.2.4).

125 APPLICATION PERFORMANCE MEASUREMENTS

In each Terminal data rule, the StreamGroomer computes application performance measurements (response time, LAN and WAN round-trip time…).

These application performance measurements are **automatically** enabled on all Terminal data rules.

126 VOIP/VIDEO PERFORMANCE MEASUREMENTS

Rule parameters

To enable/disable the VoIP/Video performance measurements on a Terminal audio/video rule:

1. Select the *Parameters – Configuration* sub-tab of the Terminal audio/video rule. Click on the **Modify** button
2. Enter the following parameters and click on the **Submit** button

Parameter	Description / Values
Measurements	
VoIP/Video measurements	The possible values are: No, RTP (default), RTP+MOS (for standard VoIP codec: G.711, G.723, G.729)
Jitter buffer	(default=40 ms) This parameter is used to estimate the audio/video end-point jitter buffer discard throughput.

Codec sampling frequency	(default=auto) When set to auto, the StreamGroomer automatically estimates the codec sampling frequency. Enforce this parameter only if the StreamGroomers fails to estimate this value.

Site parameters

The "VoIP/Video measurements" parameter on a site has the following impacts when set to "Yes":

- On the site: enables "Real-time stats - VoIP/Video" and "Long-term stats - VoIP/Video" tabs
- On Terminal audio/video rules: displays RTP performance measurements in real-time and long-term stats tabs, as well as communications in troubleshooting tools.

Note: The "VoIP/video measurements" parameter can be configured on a set of sites:

- *Select **MANAGEMENT TOOLS > Sites management**, and click on the **Set parameters** tab*
- *Select sites, and the "VoIP/Video measurements" parameter.*
- *Click on the* **Apply** button

9.2.2 Alarms Provisioning

127 OVERVIEW

Alarms can be defined on any measurements available in network, application, and VoIP/Video rules. Thresholds are defined on the SGM, and compared after each polling, i.e. every 10 minutes.

There are two types of alarms:

- Site-specific alarms

  Specific alarms are valid only for the concerned site. Specific alarms can be added, modified, or deleted.

- Alarms distributed from a reference group of alarms

  A distributed alarm must necessarily be part of a distributed instance of a Group of alarms. It appears in italics and starts with the name of the reference Group of alarms in square brackets. There are 4 types of group of alarms, each type being available on specific rules:

Type	Available only on rules
Network SLM (special group of alarms)	Shaping, Grooming
Network	Access link, Shaping, Grooming
Application	Terminal data
VoIP/Video	Terminal audio/video

Alarms can be exported by email, SNMP trap or syslog.

128 ALARM - PARAMETERS

The parameters of an alarm are:

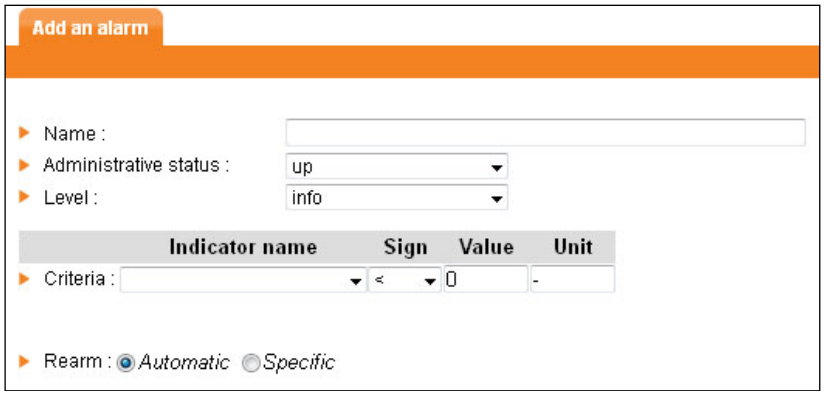


Figure 120 – Alarm parameters

Parameter	Description / Values
Name	Alarm name (automatically filled if left blank)
Administrative status	Up (default), Down
Level	Select the criticality level: Info (default), minor, major, critical
Criteria	Enter the threshold criteria
Rearm	Enter the ream criteria (if automatic is selected, then it is the same as the threshold criteria)

Note: The list of threshold and rearm criteria varies:

-Specific alarm: it depends on the type of rule on which the alarm is created

-Distributed alarm: it depends on the type of group on which the alarm is created (network, application, VoIP/Video)

129 ALARM - ADD/MODIFY/DELETE OPERATIONS

To add a specific alarm (directly in a site traffic tree) or a distributed alarm (within a reference group of alarms):

1. **Specific alarm**: click on the rule in the tree menu and on the *Parameters - Alarms* sub-tab, and then on the "*Add*" button
2. **Distributed alarm**: right-click on the reference Group of alarms, and select **"Add… > Alarm"**.

To modify an alarm, click on it and then on the **Modify** button, enter the modifications, and then click on the **Submit** button.

To delete an alarm, click on it and then on the **Delete** button. Validate the confirmation message.

130 REFERENCE GROUP OF ALARMS MANAGEMENT

Generic Group of Alarms

To create a reference Group of alarms, open the **MANAGEMENT TOOLS,** right-click on **SLM/Alarms catalog**, and then select **Add…** → **Group of alarms**. Enter the group name, select the type (network, application, VoIP/Video), and click on the **Submit** button.

The alarms in a reference group of alarms are created in exactly the same way as for a rule. When all the alarms have been defined, an overview can be displayed by opening the tree menu, or by clicking on the Group and then selecting the *Group of alarms* tab.

All alarms in a group of alarms can also be deleted by clicking on the **Delete all** button".

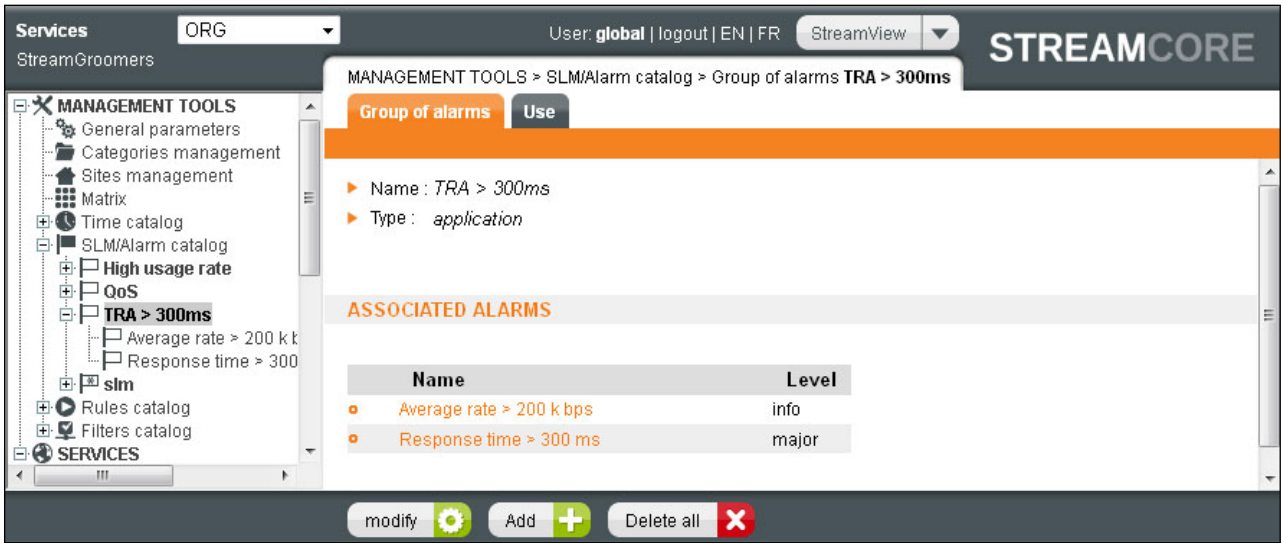


Figure 121 – Group of alarms parameters

Parameter	Description / Values
Name	Name of the group
Type	Network, Application or VoIP/Video
Associated alarms	
	List of alarms

To modify the name, click on it and then on the **Modify** button, enter the modifications, and then click on the **Submit** button.

To delete a group, click on it and then on the **Delete** button (displayed only if the group is not used anywhere).

Special group: Network SLM

To create a reference Network SLM, open the **MANAGEMENT TOOLS,** right-click on **SLM/Alarms catalog**, and then select **Add…** → **Network SLM**. Enter the group name, enter the parameters, and click on the **Submit** button.

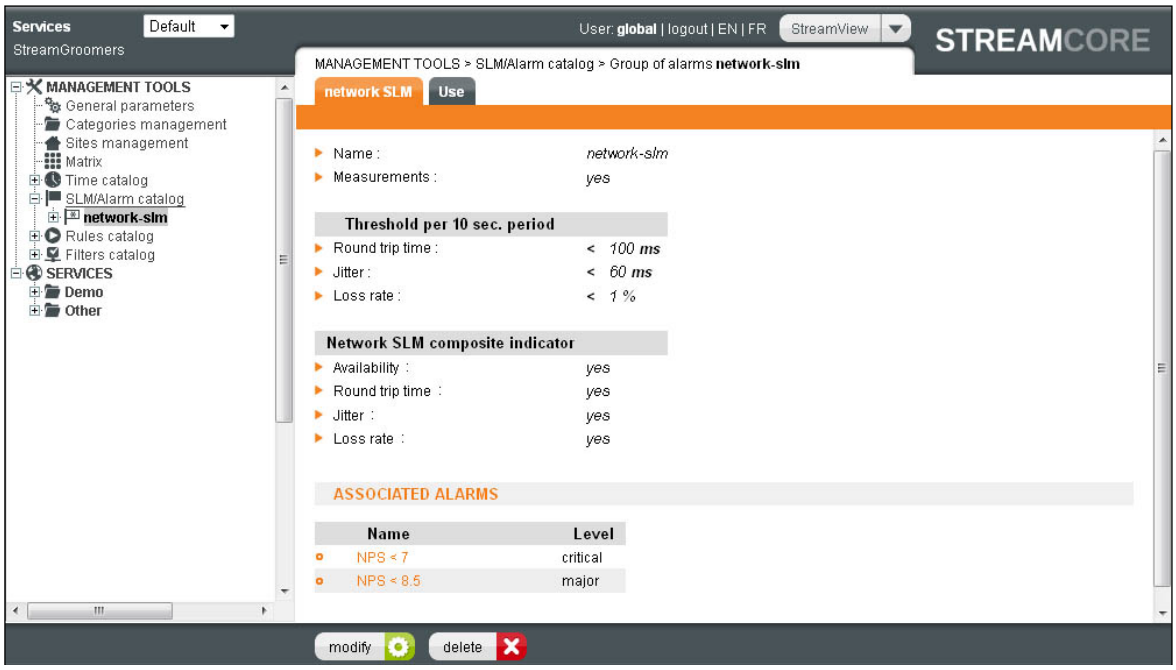


Figure 122 – Network SLM parameters

Parameter	Description / Values	
Name	Name of the group	
Measurements	Yes (default), No	
Threshold per 10 sec. period		
Round trip time	(default=100 ms)	For each indicator, the StreamGroomer classifies 10 sec. samples: - Excellent: Indicator < Threshold/2 - Good: Threshold/2 < Indicator < Threshold - Average: Threshold < Indicator < Threshold x 2 - Poor: Threshold x 2 < Indicator < Threshold x 4 - Unacceptable: Threshold x 4 < Indicator
Jitter	(default=60 ms)	
Loss throughput	(default= 1%)	
Network SLM composite indicator		
Availability	Select the criteria that will be into account when the StreamGroomer computes the network SLM. The StreamGroomer classifies each 10 sec. network SLM sample: the network SLM "performance class" is the worst of all selected criteria 10 sec. "performance class". Example: all indicators are "Excellent" but Latency is "Poor" -> Network SLM is "Poor"	
Round trip time		
Jitter		
Loss throughput		
Associated alarms		
	List of alarms (cannot be changed) The following Network Performance Score (NPS) is computed and compared to 7 and 8.5 thresholds: 10 x (Excellent samples + Good samples + (Average samples)/2)/Total samples	

To modify the name or other parameters, click on it and then on the *"Modify"* button, enter the modifications, and then click on the "*Submit*" button.

To delete a group, click on it and then on the "*Delete*" button (displayed only if the group is not used anywhere).

131 GROUP OF ALARMS – ADD/DELETE OPERATIONS

Distribution Summary

All of the distributed instances of a reference Group of alarms can be displayed by clicking on **SLM/Alarm catalog > Group xx**, and then selecting the *Use* tab.

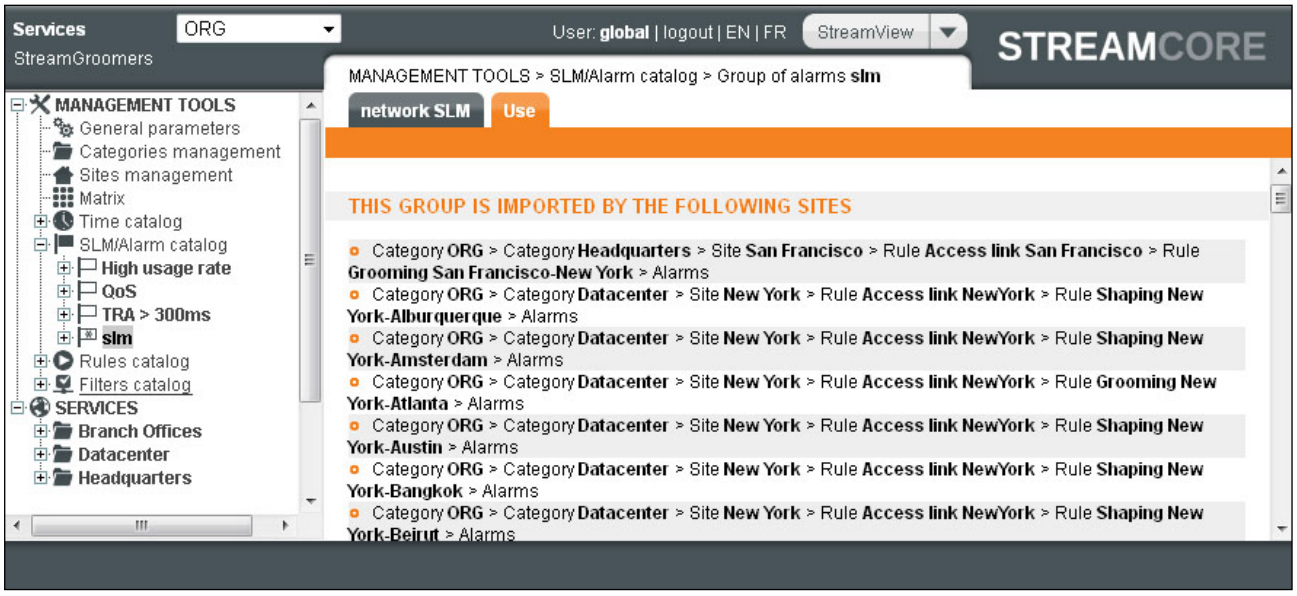


Figure 123 – Group of alarms use summary.

"Network group of rules" or "Network SLM" distribution – Tree menu

A group of alarms can be inserted directly on an access link, shaping or grooming rule:

1. Click on the rule in the tree menu and on the *Parameters - Alarms* sub-tab, and then on the **Add** button.
2. Instead of creating a single local alarm, select the Group of rules radio button, and the reference group of alarms, then click on the **Submit** button.

Figure 124 – Adding a network group of alarms.

To delete a distributed instance of a group of alarms, click on **one of the alarm** in the instance, and then select "*Delete*". Validate the confirmation message.

Note: When Shaping or Grooming rules are created (single instance, or multiple instances through the network rules matrix), the wizard offer the possibility to distribute one or more reference Network Groups of alarms, and a single Network SLM.

"Network group of rules" or "Network SLM" distribution – Matrix Management Tool

In order to display a matrix summary of the network group of alarms used per site:

1. Open the **MANAGEMENT TOOLS**, select **Matrix** in the tree menu and click on the *Alarms* tab
2. Select a subset of sites to be displayed by choosing categories (optional)
3. Click on the *"Submit"* button

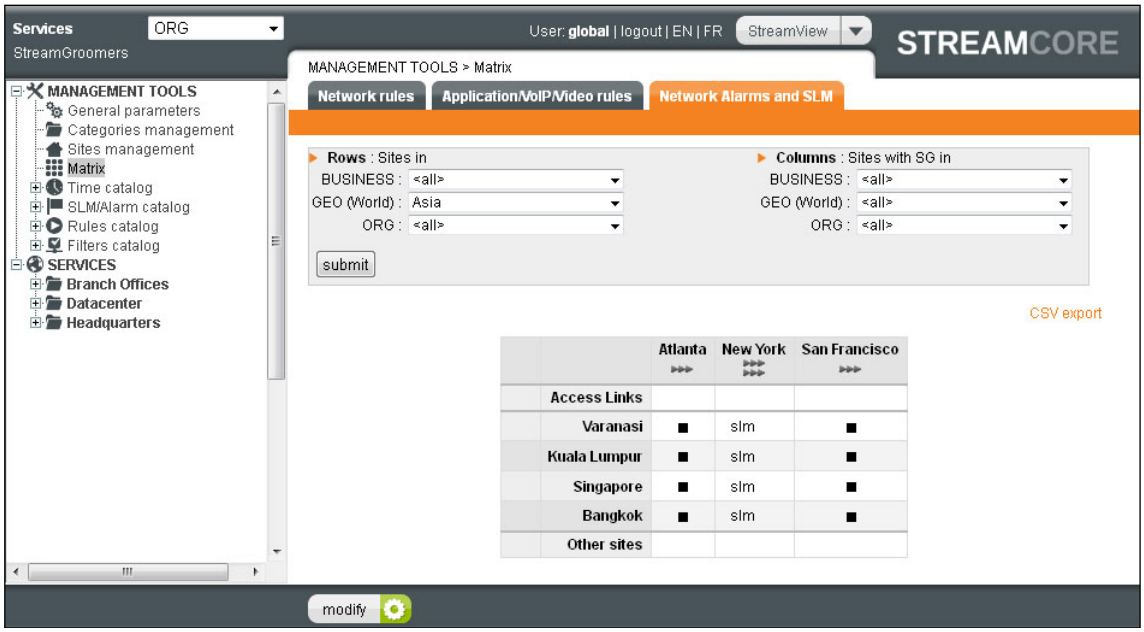


Figure 125 – Network Group of alarms matrix summary

In order to create or delete instances of group of alarms through the matrix:

1. Display the alarms matrix as explained previously
2. Click on the **Modify** button
3. Click on the intersection between the sites for which a group of alarms has to be managed, or use the **Create all** or **Delete all** buttons to apply several changes in a single click.

"Application or VoIP/Video group of alarms" distribution

A group of alarms can be inserted directly on rule belonging to a group of rules or on an existing site:

1. Click on the rule in the tree menu (group of rules or in tree menu of the site) and on the *Parameters - Alarms* sub-tab, and then on the **Add** button.
2. Instead of creating a single local alarm, select the Group of rules radio button, and the reference group of alarms, then click on the **Submit** button.

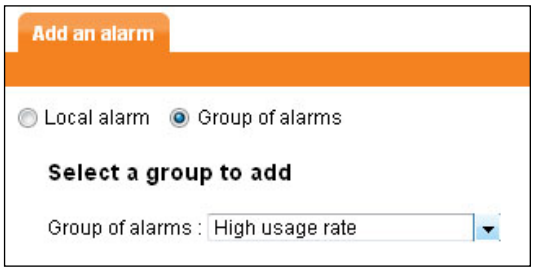


Figure 126 – Adding an application or VoIP/Video group of alarms

To delete a group of alarms, click on **one of the alarms** in the instance, and then select **Delete**. Validate the confirmation message.

132 ALARMS EXPORT

Different options can be provisioned to export Services alarms:

	Available perimeters	Provisioning page

Email	All sites	Management tools>General parameters Alarm export tab (see chapter 14.1)
	Category or single site	Services>Category or site xx Parameter – Alarms tab (see chapter 14.1)
SNMP trap **Syslog**	All sites	Management tools>General parameters Alarm export tab (see chapter 14.1)

Note: An export will be performed when the alarm is triggered and again when the alarm is rearmed.

9.2.3 Troubleshooting Tools Provisioning

133 OVERVIEW

Real-time session-based and packet-based troubleshooting tools (*Traffic discovery, TopN, Live Connections/Communications, Traffic capture*) are available by default on all sites.

Back-in-time session-based troubleshooting tools (*Traffic discovery, TopN, Connections, / Communications*) need to be activated and configured: in order to keep a per session history, the smart NetFlow export must be activated on a per site basis. Advanced export filtering mechanisms can be used in order to restrict the export to specific applications.

Active and LAN troubleshooting tools (LAN inventory, VoIP/Video agent…) need to be activated as well.

134 BACK-IN-TIME TROUBLESHOOTING (NETFLOW EXPORT)

StreamGroomer parameters

In order to configure any NetFlow export on a StreamGroomer, click on **StreamGroomers > System Parameters** in the tree menu, select the ***NetFlow parameters*** tab, then on the **Modify** button. Select the SGM as collector (default) and define the parameters related to the NetFlow export process, and then click on the **Submit** button.

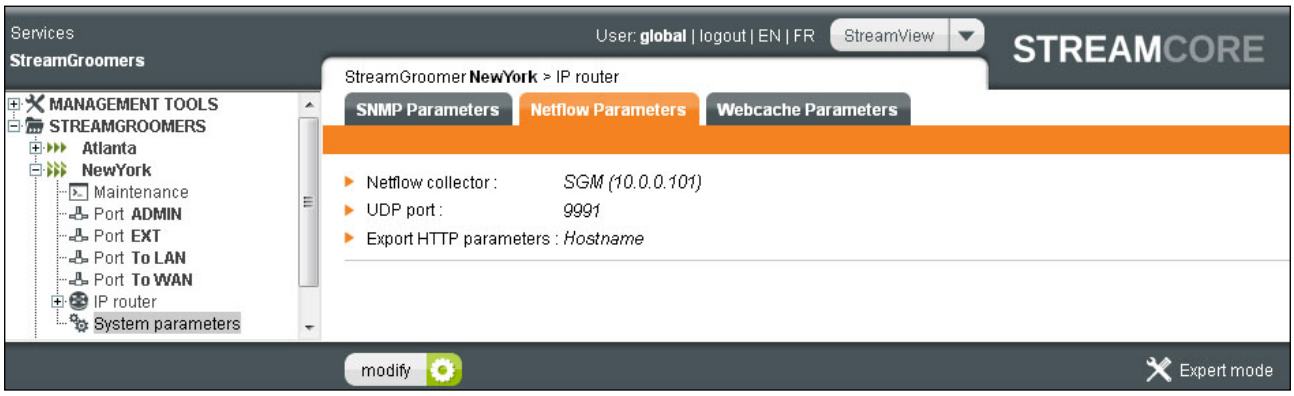


Figure 127 – Adding an application or VoIP/Video group of alarms

Parameter	Description / Values
NetFlow collector	Two possible values: external collector, integrated collector on the SGM
IP address	IP address towards which NetFlow tickets will be exported (required for an external collector or a SGM in a NAT environment)
UDP port	(Default=9991) UDP port towards which NetFlow tickets will be exported
Format	(Default=v9) defines the NetFlow ticket format (v5 or v9) (required for an external collector only since v9 is used by default for the SGM collector)

Export HTTP parameters	When a HTTP traffic is detected by the StreamGroomer, the NetFlow v9 generated ticket will carry hostname and URL information. URL can be quite large, and therefore the URL export parameters can be as follows: - Hostname: only the hostname will be exported - Hostname + URL XX: the hostname and url will be exported (up to XX characters)

The following parameters are available in Expert mode on a StreamGroomer:

Expert parameter	Description / Values
Active timeout	(default=10 min.) Timer enforcing a NetFlow export for a session with very long duration. (forced to 10 min. when the SGM is selected as the collector)
Max number of tickets to export per second	(default=150) Value to limit the amount of NetFlow tickets exported by the StreamGroomer.

Note: A session information will be exported by a StreamGroomer if the following conditions are met:

- It is classified in a rule with NetFlow export enabled AND
- There is new information to export AND
- An end of TCP session has been detected (TCP FIN or RST)
- The inactive timeout has expired (15 seconds)
- The active timeout has expired (10 minutes by default)

Note: The StreamGroomer NetFlow parameters can be configured on a set of StreamGroomers:

- Select MANAGEMENT TOOLS > StreamGroomer configuration, and click on the Set parameters tab
- Select StreamGroomers, and the "NetFlow parameters" and enter the parameters.
- Click on the **Apply** button

Site parameters

The NetFlow export is turned off by default on all sites (whether equipped or not with a StreamGroomer). In order to activate the NetFlow export on a site, click on **Services > Site xx** in the tree menu, on the *Parameters - Configuration* sub-tab, then on the **Modify** button. Change the parameter related to the NetFlow export process, and then click on the **Submit** button. The three available values are:

- No : the NetFlow export is turned off
- Per application : the NetFlow export is turned on only for specific terminal rules (depending on the value of the per rule associated parameter)
- Audio/Video: the NetFlow export is turned on only for all terminal audio/video rules
- Shaping other sites: the NetFlow export is turned on only for all traffic classified in the Shaping other sites rule
- Total : the NetFlow export is turned on for all terminal rules (whatever the value of the per rule associated parameter)

Note: The NetFlow export parameter can be enabled/disabled on a set of sites:

- Select **MANAGEMENT TOOLS > Sites management**, and click on the Set parameters tab
- Select sites, and the "NetFlow export" parameter.
- Click on the **Apply** button.

Rule parameters

When the "Per application" NetFlow export is turned on, a per rule NetFlow parameter is taking into account. To change this parameter, click on the rule in tree menu, on the *Parameters - Configuration* sub-tab (Expert mode), then on the **Modify** button.

Note: The NetFlow export per rule summary can be checked by clicking on **SERVICES > Site xx** or **MANAGEMENT TOOLS > Rules Catalog> Rule xx** in the tree menu, on the Parameters - Rules sub-tab.

Note: If the NetFlow export is set to "Total" on a site with a StreamGroomer with shaping rules towards remote sites, then NetFlow export and long-term troubleshooting tools are automatically enabled on remote sites (whatever the NetFlow parameters on these sites).

135 LAN INVENTORY TOOLS

In order to have access to *Active Discovery* and *Host Analysis* within LAN inventory tools on a site with a StreamGroomer:

1. Click on **Services > Site xx** in the tree menu, on the ***Parameters - Configuration*** sub-tab (Expert mode), then on the **Modify** button.
2. Change the parameter related to the Active LAN inventory tools.
3. Click on the **Submit** button.

9.3 CATEGORY VISIBILITY SERVICES

9.3.1 Overview

The following table provides a summary of the visibility services accessed through sub-tabs.

9.3.2 Long-Term Stats

136 OVERVIEW

The ***Long-term stats*** visibility service on a category provides high-level views of network, application or VoIP/Video use and performance.

Figure 128 – Long-term stats on a category

137 NETWORK STATISTICS

The *Long-term Stats – Network* sub-tab displays the following graphs:

Graph		Description
Volume	Consolidated	Total volume exchanged by sites belonging to the category
	Top applications and sites	Total volume allocation between up to 10 different kinds of objects. These objects can be sites or applications.
Usage throughput	Most loaded sites	Top 10 sites with the highest or lowest usage throughput (according to the distribution of 10-second samples over the period). Low = usage throughput between 0 et 25% Medium = usage throughput between 25 and 50% High = usage throughput between 50 and 75% Very high = usage throughput between 75 and 90% Full = usage throughput between 90 and 100%
	Least loaded sites	
	Consolidated	Overall network quality for all sites belonging to the category (according to the distribution of 10-second samples over the period)

Network SLM[4]	Top sites	Top 10 sites with the worst network SLM (according to the distribution of 10-second samples over the period)

138 APPLICATIONS STATISTICS

After having selected an application, the ***Long-term Stats – Applications*** sub-tab displays the following graphs:

Graph		Description
Volume	Consolidated	Total volume exchanged by sites belonging to the category
	Top sites	Total volume allocation between up to 10 sites belonging to the category for this application
	Top sub-rules (intermediate rule only)	Total volume allocation between up to 10 sub-rules for the sites belonging to the category
Number of connections (terminal data rule only)	Consolidated	Average number of connections observed on the sites belonging to this category for this application
	Top sites	Top 10 sites with the most connections for this application
Application Response time (terminal data rule only)	Consolidated	Measures TCP client-server interactions for all sites belonging to the category: Total time = average time elapsed on the client between the transmission of a client request till the complete reception of the server answer Server time = average time elapsed on the server between the reception of a client request till the beginning of the server answer Data transfer time = total time – average server time The data transfer time includes both the round-trip time between the client and the server, and the amount of data to be transmitted WAN RTT = round-trip time over the WAN
	Top sites	Top 10 sites belonging to the category with the worst average response time or worst response time distribution (10-second samples) for this application

139 VOIP/VIDEO STATISTICS

After having selected a codec, the ***Long-term stats – VoIP/Video*** sub-tab displays the following graphs:

Graph		Description
Volume	Consolidated	Total volume exchanged by sites belonging to the category
	Top sites	Total volume allocation between up to 10 sites belonging to the category
	Top sub-rules (intermediate rule only)	Total volume allocation between up to 10 sub-rules for the sites belonging to the category

[4] Displayed if activated on sites in the category

Number of communications or sessions (terminal A/V rule only)	Consolidated	Average number of communications observed on the sites belonging to this category
	Top sites	Top 10 sites belonging to the category with the most communications
MOS (terminal A/V rule only and G.711, G.723, G.729)	Consolidated	VoIP average Mean Opinion Score (MOS) for the sites belonging to the category MOS-CQ = MOS Conversational Quality (takes into account latency, loss, jitter) MOS-LQ = MOS Listener Quality (takes into account loss, jitter but not latency)
	Top sites	Top 10 sites belonging to the category with the worst average MOS or worst MOS-LQ distribution

Note: This sub-tab is available only if there is at least one site with VoIP/Video measurements enabled in the category.

9.3.3 Alarms

140 OVERVIEW

To supervise any indicator, alarms to automatically warn people in case of service level degradation. Those alarms can be seen in the *Alarms* tab, through tree sub-tabs.

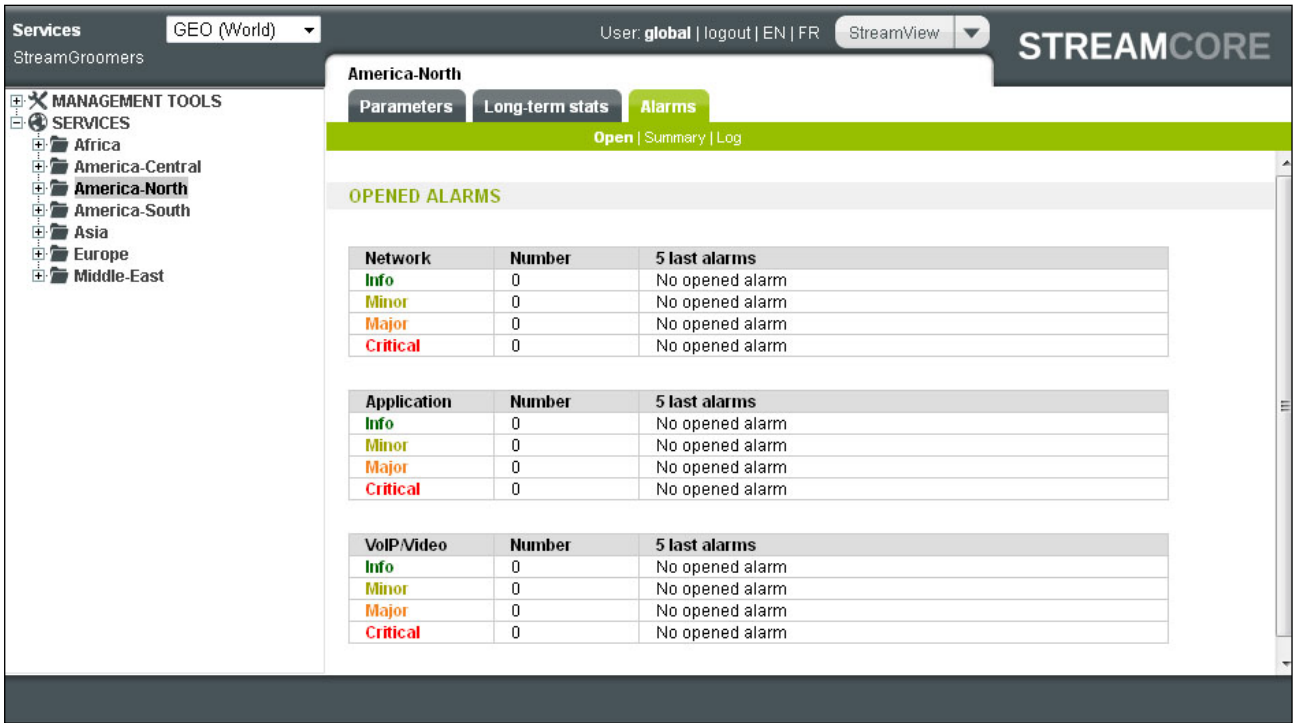


Figure 129 – Alarms on a category

141 OPEN/SUMMARY

All alarms in dashboards are displayed per type:

- Network alarms (defined on access link, shaping and grooming rules)
- Application alarms (defined on terminal data rules)
- VoIP/Video alarms (defined on terminal audio/video rules)

The available dashboards of alarms are:

- **Alarms - Open:** an administrator can check if alarms are currently triggered for all sites belonging to the category.
- **Alarms - Summary:** *a*n administrator can check in a summary if alarms have been triggered in the past for all sites belonging to the category. Select the period to display:
  - Long-term graphs showing the number of alarms per criticality.
  - Tables showing the total number as well as highlighting the top alarms in quantity or duration.

142 LOG

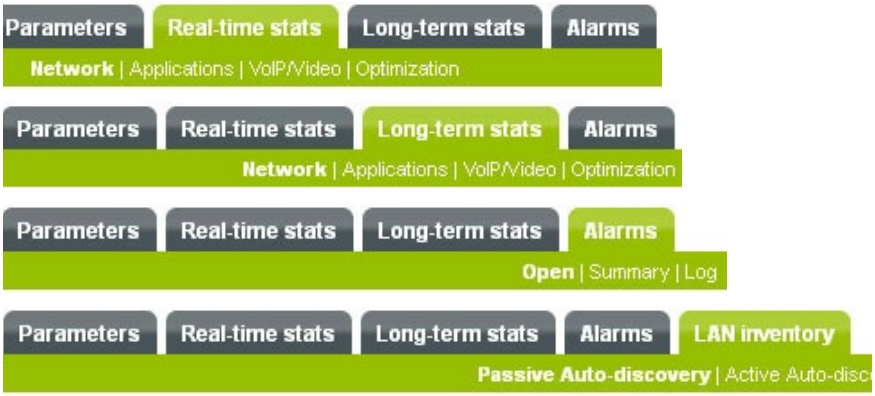
All alarms and their criticality level (**info**, **minor**, **major**, **critical**) are displayed in this log. Filtering criteria are:

- Type : Network, Application, VoIP/Video
- Alarm name
- Rule name

9.4 SITE VISIBILITY SERVICES

9.4.1 Overview

The following table provides a summary of the visibility services accessed through sub-tabs.



(site with StreamGroomer only)

9.4.2 Real-Time Stats

143 OVERVIEW

The ***Real-time Stats*** visibility service on a site provides dashboards over the last 10 sec., 1 min. and 10 min. periods:

- overview of traffic classification into the rules tree
- summary of network, application or VoIP/Video use and performance
- overview of optimization statistics (available only for a site with a StreamGroomer)

144 NETWORK, APPLICATION, VOIP/VIDEO STATISTICS

The ***Real-time Stats - Network***, ***Application,*** or ***VoIP/Video*** sub-tab displays a summary of the rules tree:

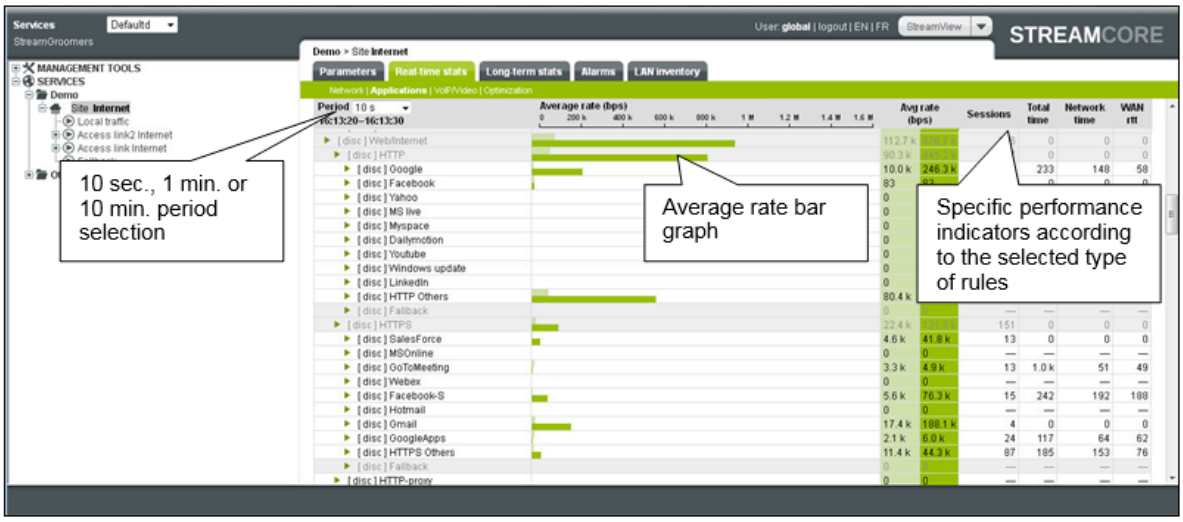


Figure 130 – Real-time stats – Applications sub-tab

The following information is available:

- Breakdown of traffic into the tree with the average throughput per rule displayed in bar graphs.
- Highlight of the rules selected (for example network and VoIP/Video rules are grayed if the "Applications" sub-tab has been selected).
- Specific performance indicators depending on the type of rules selected:

Network	Applications	VoIP/Video
Sessions Status Delay Loss Jitter	Sessions Total time Network time WAN RTT	Nb communications MOS-LQ Delay RTP loss Discard throughput Jitter

Specific case: Application sub-tab on a Data Center

If the "Data Center parameter" is set to yes on a site, then the *Applications* sub-tab displays a table per application, showing the average throughput and performance per remote site.

145 OPTIMIZATION STATISTICS (SITE WITH STREAMGROOMER)

The *Real-time stats – Optimization* sub-tab displays a summary of optimization statistics:

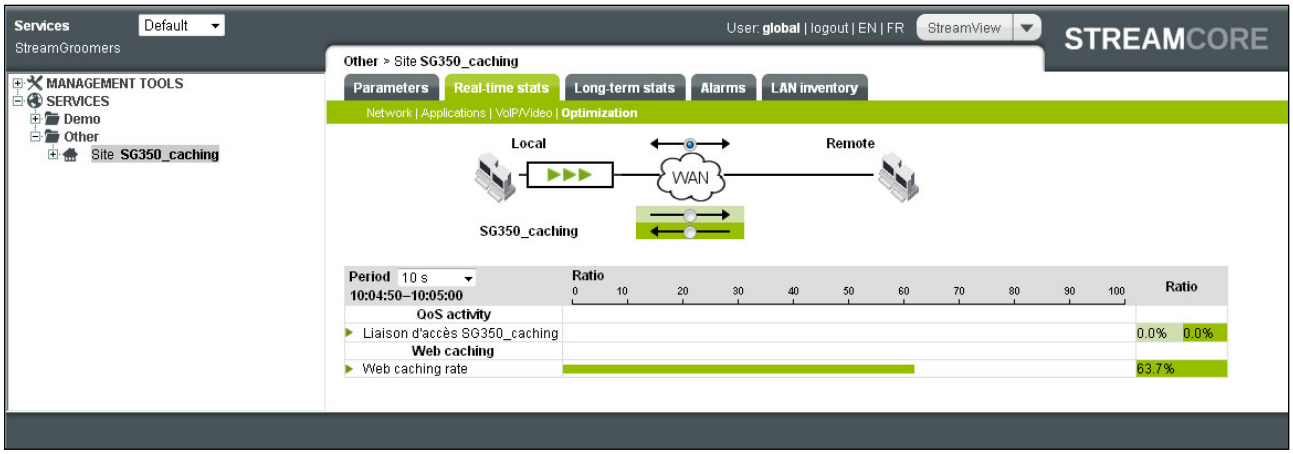


Figure 131 – Real-time stats – Optimization sub-tab

The following information is available:

- **QoS activity:**
  - Per access link
  - Per shaping/grooming rule
- **Compression ratio:**
  - Per access link
  - Per shaping/grooming rule
- **Web caching ratio**

9.4.3 Long-Term Stats

146 OVERVIEW

The *Long-term Stats* visibility service on a site provides overviews of network, application or VoIP/Video use and performance.

Figure 132 – Long-term stats on a site

147 NETWORK STATISTICS

The *Long-term Stats – Network* sub-tab displays the following graphs depending on the type of site:

Graph	Description	
	Site with at least 2 Shaping/Grooming rules	Site with less than 2 Shaping/Grooming rules
Data throughput/Volume	Average throughput or volume observed on the site	
Top traffic	Bandwidth allocation between up to 10 different applications	
	Bandwidth allocation between up to 10 remote sites or categories	-
Usage throughput	Percentage of time (% of 10-second samples over the period) during which the network load is: Low = usage throughput between 0 et 25% Medium = usage throughput between 25 and 50% High = usage throughput between 50 and 75% Very high = usage throughput between 75 and 90% Full = usage throughput between 90 and 100%	
Network SLM (if activated)	Overall network quality observed on the site	
	Top 10 Shaping/Grooming rules with the worst network SLM (according to the distribution of 10-second samples over the period)	-

148 APPLICATION STATISTICS

After having selected an application, the ***Long-term Stats – Applications*** sub-tab displays the following graphs depending on the type of site:

Graph	Description	
	Site with at least 2 Shaping/Grooming rules	**Site with less than 2 Shaping/Grooming rules**
Data throughput/Volume	Average throughput or volume observed on the site	
Top traffic	Bandwidth allocation between up to 10 different sub-rules *(intermediate rule only)*	
	Bandwidth allocation between up to 10 remote sites or categories for this application	-
Number of connections (terminal data rule only)	Average number of connections for this application	
	Top 10 remote sites or categories with the worst average response time for this application	-
Response time (terminal data rule only)	Measures TCP client-server interactions: Total time = average time elapsed between the transmission of a client request till the complete reception of the server answer Server time = average time elapsed on the server between the reception of a client request till the beginning of the server answer Network time = total time – average server time (The network time includes both the round-trip time between the client and the server, and the amount of data to be transmitted) WAN RTT = round-trip time over the WAN	
	Top 10 remote sites or categories with the worst response time distribution (10-second samples)	-

149 VOIP/VIDEO STATISTICS

After having selected a codec, the ***Long-term Stats – VoIP/Video*** sub-tab displays the following graphs:

Graph	Description
Data throughput/Volume	Average throughput or volume observed on the site
Top traffic (Intermediate rule only)	Bandwidth allocation between up to 10 different sub rules
Number of communications (terminal A/V rule only)	Average number of communications observed on the site
MOS (terminal A/V rule only)	VoIP average Mean Opinion Score for the site MOS-CQ = MOS Conversational Quality (takes into account latency, loss, jitter) MOS-LQ = MOS Listener Quality (takes into account loss, jitter but not latency)

150 OPTIMIZATION STATISTICS (SITE WITH STREAMGROOMER)

The ***Long-term Stats – Optimization*** sub-tab displays the following graphs:

Graph	Description
QoS activity	
QoS activity throughput per access link	QoS activity throughput per access link
QoS per shaping/grooming	Top 10 Shaping/Grooming access links with the most QoS activity
Compression	
Compression throughput per link	Compression throughput for all traffic in grooming rules below the access link
Compression throughput per grooming	Top 10 Grooming rules with the highest compression ratio
Web caching	
Caching ratio	Web caching ratio for HTTP traffic on the site
HTTP volume	HTTP volume sent to LAN (including cached objects)

9.4.4 Alarms

151 OVERVIEW

To supervise any indicator, alarms to automatically warn people in case of service level degradation. Those alarms can be seen in the *Alarms* tab, through tree sub-tabs.

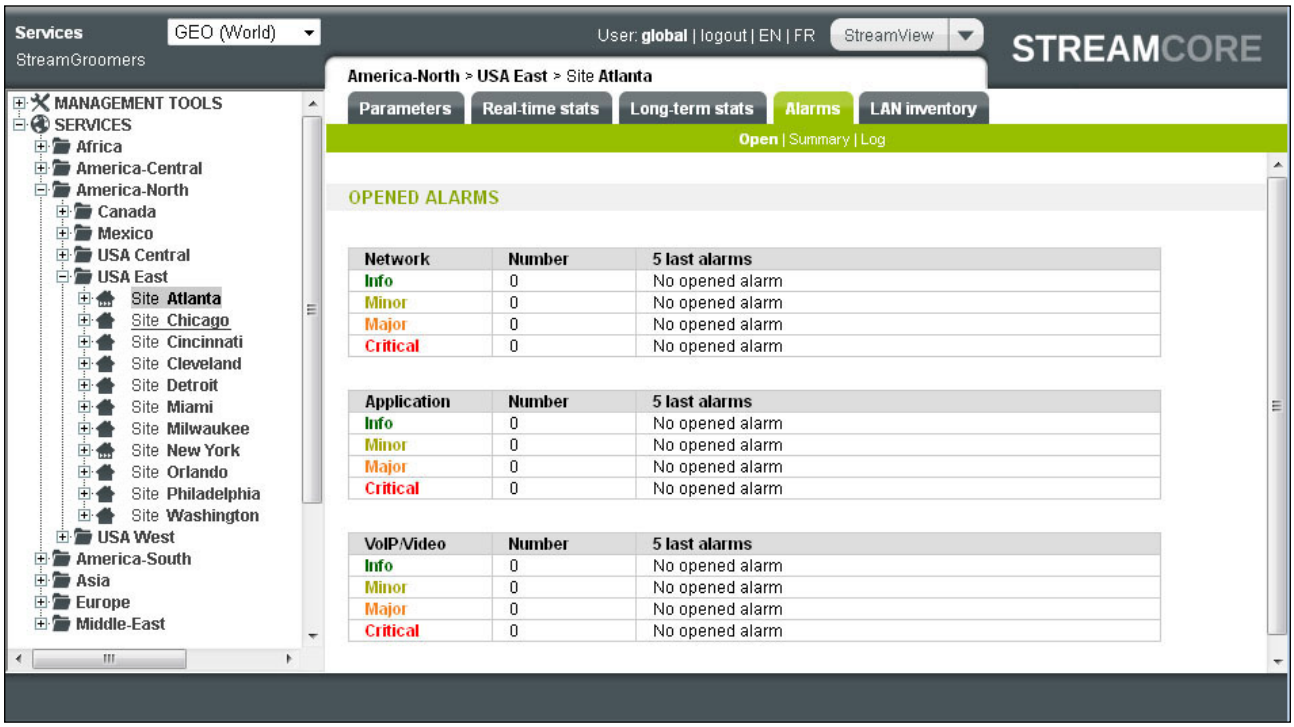


Figure 133 – Alarms on a site

152 OPEN/SUMMARY

All alarmed in dashboards are displayed per type:

- Network alarms (defined on access link, shaping and grooming rules)
- Application alarms (defined on terminal data rules)

- VoIP/Video alarms (defined on terminal audio/video rules)

The available dashboards of alarms are:

- *Alarms - Open*: an administrator can check if alarms are currently triggered on the site.
- *Alarms - Summary*: an administrator can check in a summary if alarms have been triggered in the past on the site. Select the period to display:
  - Long-term graphs showing the number of alarms per criticality.
  - Tables showing the total number as well as highlighting the top alarms in quantity or duration.

153 LOG

All alarms and their criticality level (**info**, **minor**, **major**, **critical**) are displayed in this log. Filtering criteria are:

- Type : Network, Application, VoIP/Video
- Alarm name
- Rule name

9.4.5 LAN Inventory

154 OVERVIEW

The *LAN inventory* visibility service on a site with a StreamGroomer provides tools to discover the endpoints, PC or servers using IP addresses on the LAN side of the StreamGroomer.

Two types of tools are available:

- The *Passive auto-discovery* tool displays all IP addresses seen by the ADMIN and LAN/WAN interfaces of the StreamGroomer.
- The *Active auto-discovery* and *Host analysis* tools generate traffic through scanning technologies to discover all endpoints connected over the LAN, and to analyze the host properties (opened TCP/UDP ports, PC or server…).

Note: Active auto-discovery and Host analysis sub-tabs are available only if the "Active LAN inventory parameter" is set to "Yes" on the site.

155 PASSIVE AUTO-DISCOVERY

The *Passive auto-discovery* tool displays the table of IP addresses discovered through the ARP process on the ADMIN and LAN/WAN interfaces of the StreamGroomer.

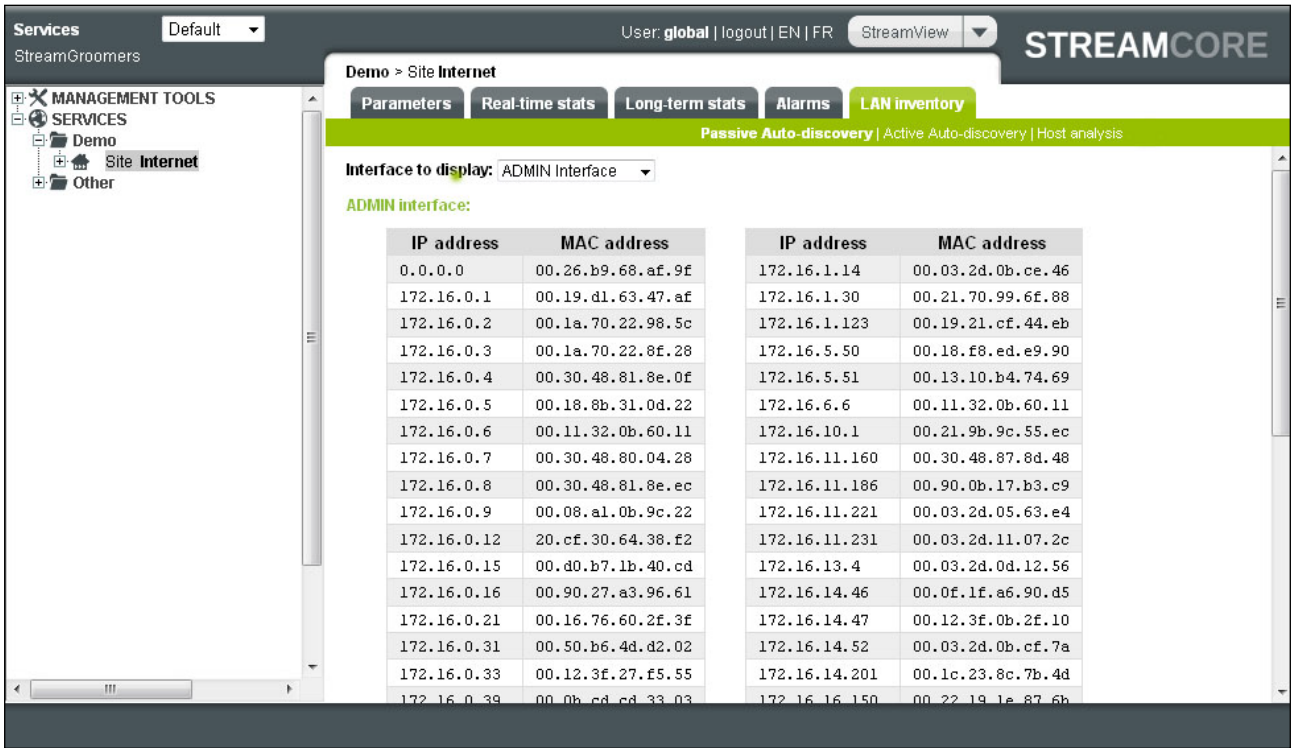


Figure 134 – LAN inventory – Passive discovery

156 ACTIVE AUTO-DISCOVERY / HOST ANALYSIS

The *Active auto-discovery* and *Host analysis* tools use scanning technology to discover the hosts connected on the LAN.

The scanning process is performed from the ADMIN interface, and is limited to 1 hop only. When launching a discovery, results can be directly displayed and saved optionally. When saving a discovery, it can be compared with other discoveries performed and saved in the past.

Note: This tool can be used only on sites with a StreamGroomer SG250e, SG350e, SG850e.Check that scanning technologies are allowed on the LAN before using these tools.

New discovery

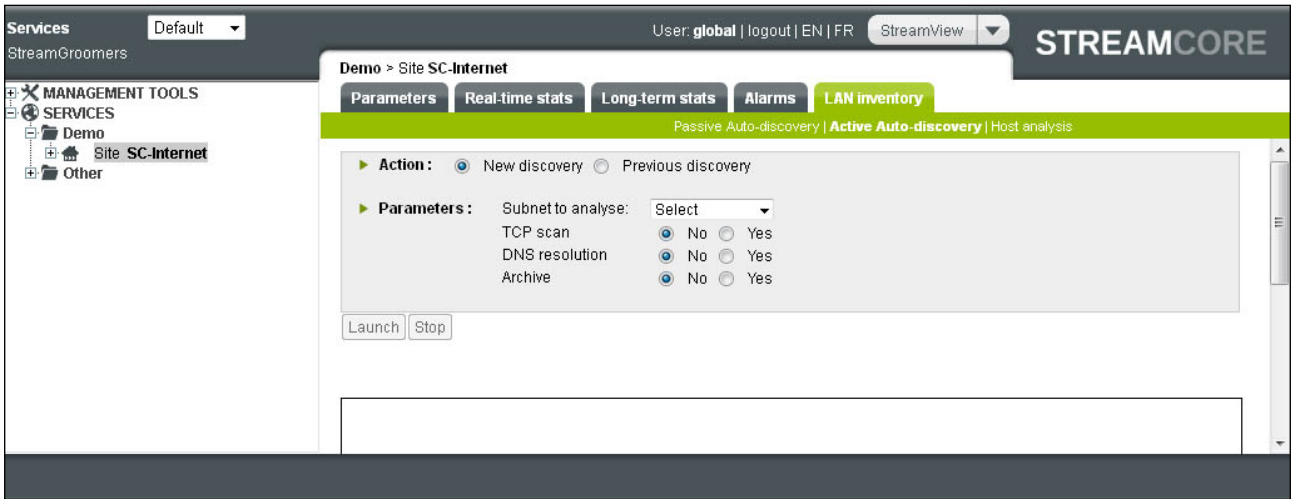


Figure 135 – LAN inventory – Active discovery

Discovery parameter	Description	
	Active auto-discovery (subnet analysis)	**Host analysis**
Action	Launch a new discovery	
Subnet or IP address	Subnets defined on the site are automatically displayed. Specific subnet can be entered (it must be less than 1 hop from the ADMIN subnet)	IP address of the host to analyze (it must be less than 1 hop from the ADMIN subnet)
Scan type options:		
TCP scan	(Default=No) To detect open TCP ports	*Enabled by default*
DNS resolution	(Default=No) To look up for DNS name for each discovered IP address	*Enabled by default*
OS detection	N/A	To try to detect the version of software stacks detected on the host (TCP, OS…)
Archive	Select whether to archive the discovery (a button to archive is also always displayed at the end of a scan)	

Previous discovery

When selecting "Previous discovery", results of past discoveries can be displayed and compared between each other (for example if a discovery process is launched every month).

Note: All files generated when saving discoveries can be managed by clicking on **MANAGEMENT TOOLS > General parameters**, and selecting the Files management tab.

9.5 NETFLOW VISIBILITY SERVICES

9.5.1 Overview

The following tables provide a summary of the visibility services accessed through the Netflow sub-tabs.

9.5.2 Netflow

157 GRAPHS

The *Graphs* sub-tab permits you to select a connection period (minutes (10), hour, day, week, month, or year) and display it either by:

- Bytes
- Frames
- Flows

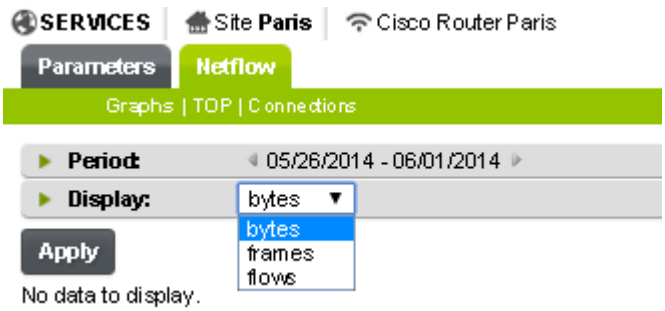


Figure 136 – Netflow Graphs

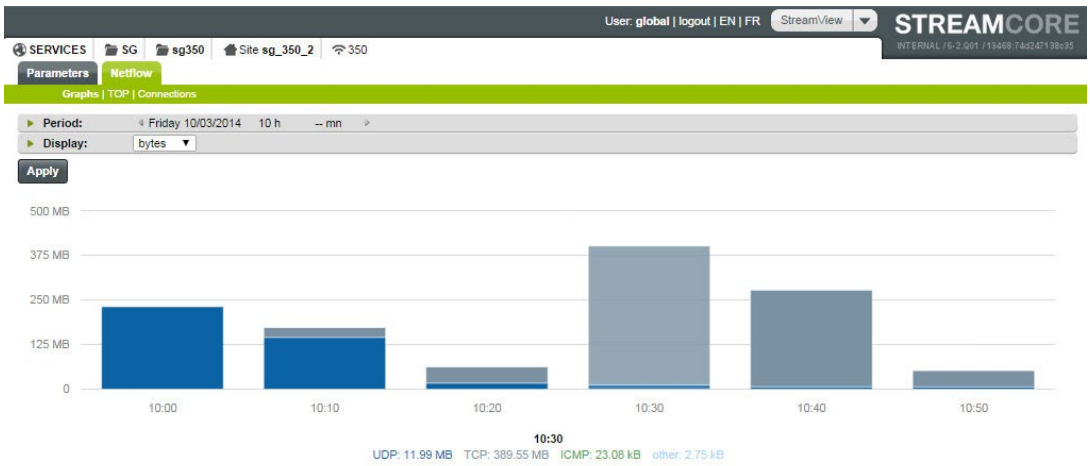


Figure 137 – Netflow Graphs – Bytes

Figure 138– Netflow Graphs - Frames

Label	Description
Period	Enables you to select a "period" for connections.
Display	Using the drop-down list, graphs can be displayed by *Bytes, Frames, and Flows*

158 TOP

The *Top* sub-tab displays top consuming connections between the device and the WAN and vice versa. There are several ways to display and filter results, based on long-term period.

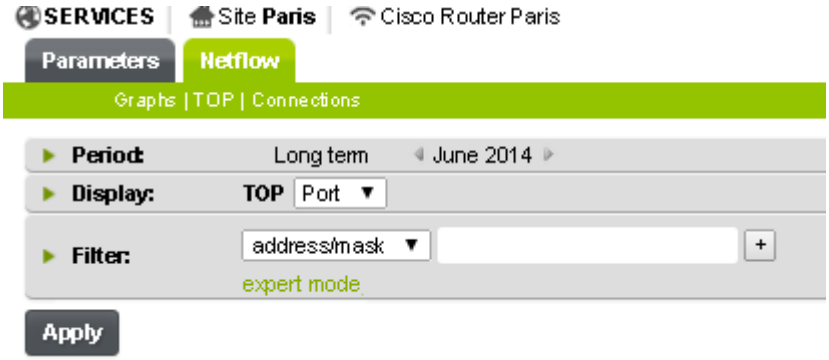


Figure 139 – Netflow TOP

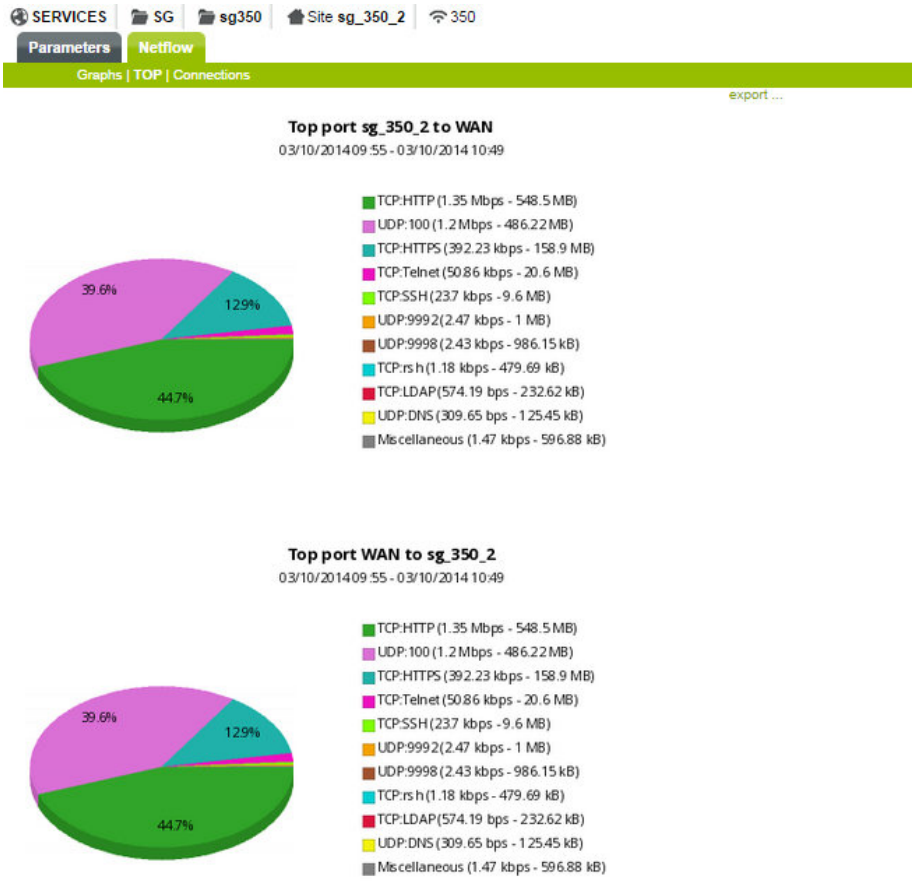


Figure 140 – Top based on Port

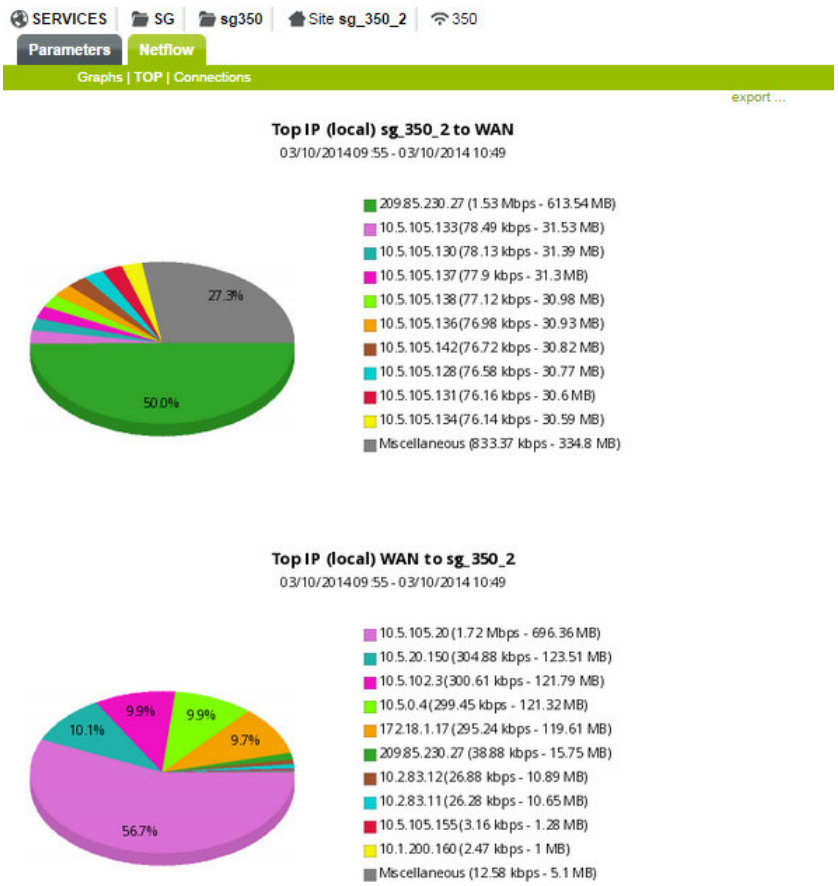
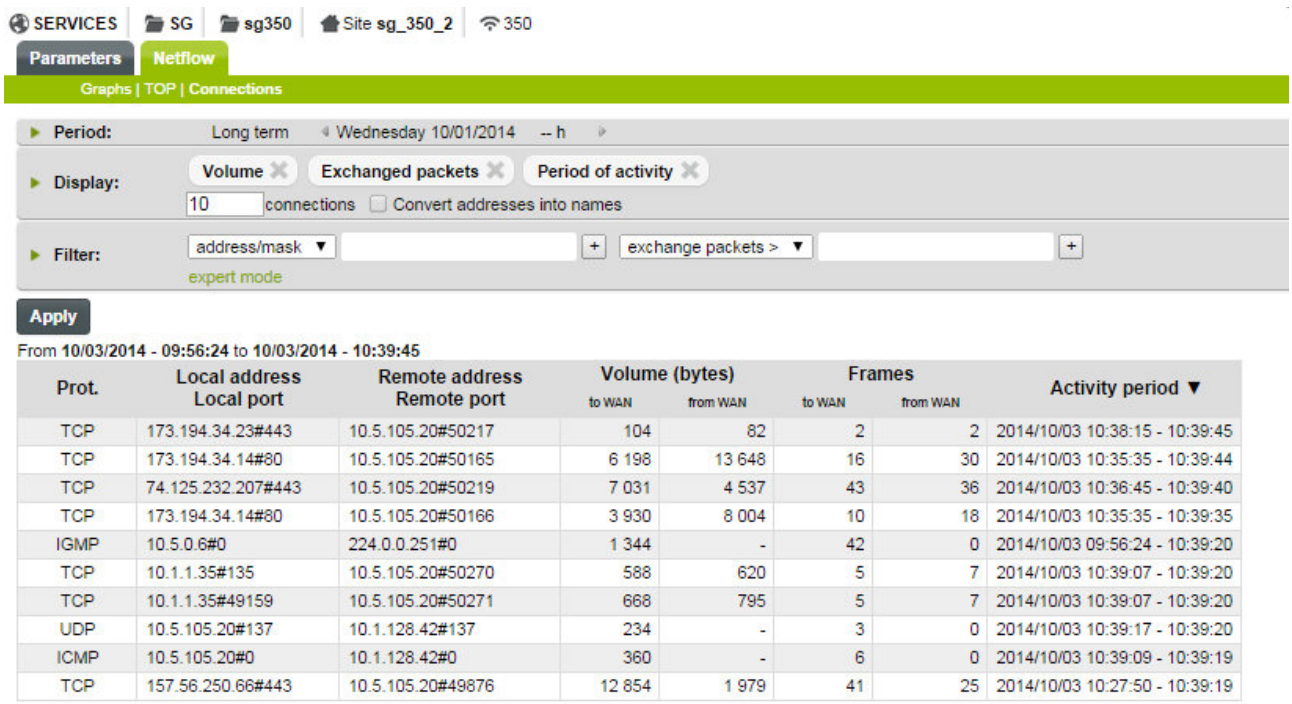


Figure 141 – Top based on IP

Label	Description
Period	Allows you to specify a connection period
Display	Using the drop-down list graphs can be displayed by port or IP address
Filter	Allows you to view your results either by: address/mask, port or protocol
Expert Mode	Allows you to manually add an address/mask, port or protocol

159 CONNECTIONS

The ***Connections*** sub-tab displays connections based on a number of connection objects for example the number of "*packets exchanged*" during set period. Several available methods permit you to display and filter results, based on long-term period.



Prot.	Local address Local port	Remote address Remote port	Volume (bytes) to WAN	Volume (bytes) from WAN	Frames to WAN	Frames from WAN	Activity period ▼
TCP	173.194.34.23#443	10.5.105.20#50217	104	82	2	2	2014/10/03 10:38:15 - 10:39:45
TCP	173.194.34.14#80	10.5.105.20#50165	6 198	13 648	16	30	2014/10/03 10:35:35 - 10:39:44
TCP	74.125.232.207#443	10.5.105.20#50219	7 031	4 537	43	36	2014/10/03 10:36:45 - 10:39:40
TCP	173.194.34.14#80	10.5.105.20#50166	3 930	8 004	10	18	2014/10/03 10:35:35 - 10:39:35
IGMP	10.5.0.6#0	224.0.0.251#0	1 344	-	42	0	2014/10/03 09:56:24 - 10:39:20
TCP	10.1.1.35#135	10.5.105.20#50270	588	620	5	7	2014/10/03 10:39:07 - 10:39:20
TCP	10.1.1.35#49159	10.5.105.20#50271	668	795	5	7	2014/10/03 10:39:07 - 10:39:20
UDP	10.5.105.20#137	10.1.128.42#137	234	-	3	0	2014/10/03 10:39:17 - 10:39:20
ICMP	10.5.105.20#0	10.1.128.42#0	360	-	6	0	2014/10/03 10:39:09 - 10:39:19
TCP	157.56.250.66#443	10.5.105.20#49876	12 854	1 979	41	25	2014/10/03 10:27:50 - 10:39:19

Figure 142 – Netflow Connections

Label	Description	
Period	Allows you to select a period for connections	
Display	This option enables you to select which information to display within selected connections. *Volume:* This corresponds to the volume of packets exchanged over the specified period. *Period of Activity:* This corresponds to the period of activity over the specified period. *Exchanged Packets:* This corresponds to the number of packets exchanged during the specified period.	
Filter	Address/mask	Allows you to select the connections established to and from an address, or between two addresses, hostnames or subnets are allowed. If hostname is used this implies that the DNS is configured on the SGM.
	Port	Allows you to established connections on a given port. TCP/UDP ports or service numbers are allowed (port 80 or HTTP for example)
	Protocol	Allows you to select the connections using a given protocol. The protocol name or number can be used, for example TCP, UCP, ICMP or 6,17 and so on)
Expert Mode	The mode allows you to manually add an address/mask, port, or protocol. The keywords are case independent and *expr* can be linked together using the following format: expr **and** expr, expr **or** expr, **not** expr and **(** expr **)**. **protocol** proto <protocol> where <protocol> can be any known protocol such	

	as tcp, udp, icmp, icmp6, gre, esp, ah, etc. or a valid protocol number: 6, 17 etc. **IP address** *[SourceDestination]* ip <ipaddr> *[SourceDestination]* host <ipaddr> with <*ipaddr*> as any valid IPv4, IPv6 address, or a full qualified hostname. In case of a hostname, theIP address is looked up in DNS. If more than a single IP address is found, all IP addresses are chained together. (ip1 or ip2 or ip3 ...) The direction qualifier *SourceDestination* may be omitted. To check an IP address against a known IP list *[SourceDestination]* ip in [<iplist>] *[SourceDestination]* host in [<iplist>] <iplist> is a space separated list of individual <ipaddr> or full qualified hostnames, which are looked up in DNS. If more than a single IP address is found, all IP addresses are put into the list. **Port** [SourceDestination] port [comp] <num> with <num> as any valid port number. If comp is omitted, '=' is assumed. comp is explained more detailed below. [SourceDestination] port in [<portlist>] A port can be compared against a know list, where <portlist> is a space separated list of individual port numbers.

10 Rules Tree Visibility Services

10.1.1 Overview

The following tables provide a summary of the visibility services accessed through sub-tabs.

Access link **Shaping/Grooming** **Intermediate rule**	Parameters | Real-time stats | Long-term stats | Troubleshooting **Indicators** | Breakdown | Top traffic Parameters | Real-time stats | Long-term stats | Troubleshooting **Indicators** | Top traffic Parameters | Real-time stats | Long-term stats | Troubleshooting TOP | Connections
Terminal rule	Parameters | Real-time stats | Long-term stats | Troubleshooting Parameters | Real-time stats | Long-term stats | Troubleshooting Parameters | Real-time stats | Long-term stats | Troubleshooting TOP | Connections | Traffic capture

10.1.2 Real-time Stats

160 OVERVIEW

The **Real-time Stats** visibility service on a rule provides statistics over the last 10 second, 1 minute and 10 minute periods:

- On any rule: *Indicators* displays statistics computed for all traffic classified in the rule. Some of these indicators are common for all rules while others are specific to the type of rule (access link, shaping, grooming, terminal data, terminal audio/video…)
- On access link, shaping, grooming and intermediate rule: additional *Breakdown* and *Top Traffic* tools provide an overview of traffic classification and bandwidth consumption by the rules in the sub-tree.

161 INDICATORS

The *Real-Time Stats - Indicators* sub-tab displays statistics computed for all the traffic classified in the rule. These statistics are classified into the following themes:

Theme	Description	Availability
Throughput	Set of indicators related to bandwidth consumption	All
WAN Optimization	Set of indicators detailing WAN Optimization (if WAN Optimization is enabled) For Live Traffic and other stats, refer to Reports via WAN Optimization tab on p194.	All
Compression	Set of indicators detailing compression performance (if compression is enabled)	Grooming rules and sub-tree rules

QoS	Set of indicators related to the load in terms of QoS	Access link, shaping, grooming, intermediate rules[5]
Frames	Set of indicators for detailed analysis of frame size	All
Performance	Set of indicators related to performance (network, application, VoIP/Video)	Access link, shaping, grooming, terminal data, terminal audio/video

Each theme and the associated indicators are displayed in the following way:

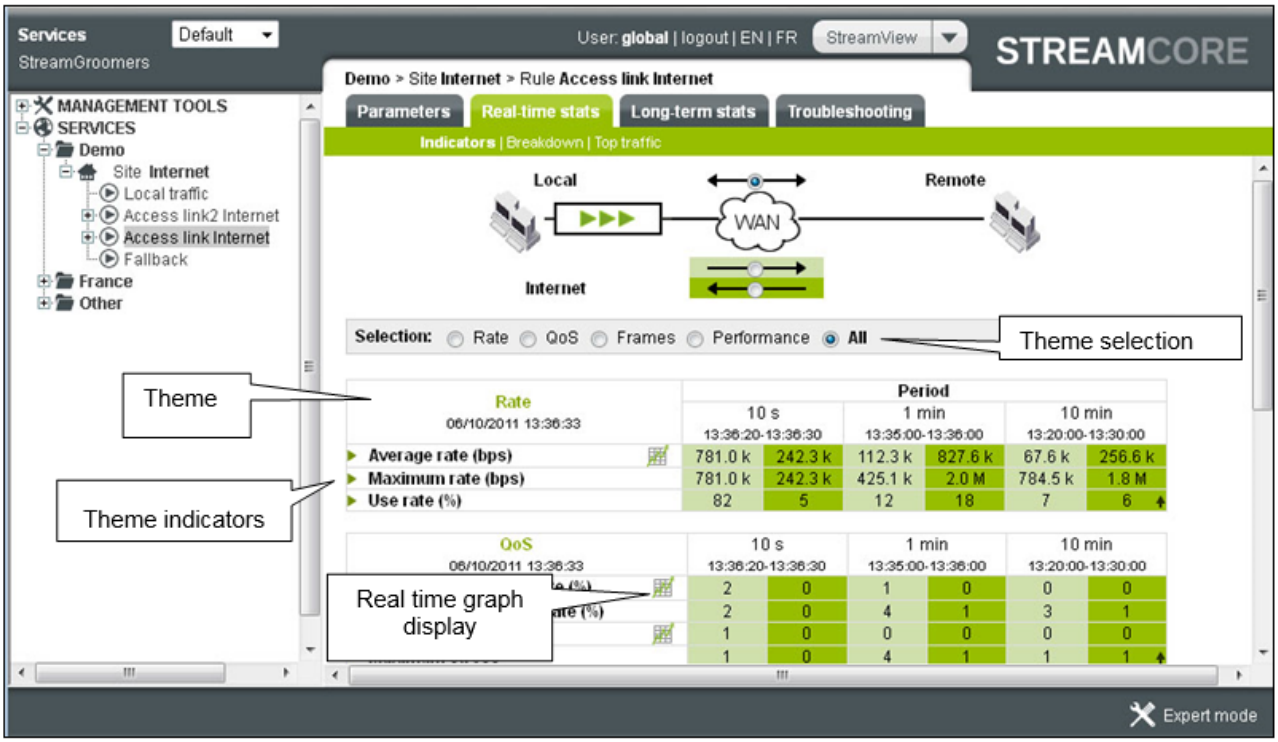


Figure 143 – Real-time stats - Indicators

The generic themes are:

Indicator	Description
Throughput	
Average throughput	Average throughput observed during the period The max. throughput and average throughput are equal during the last 10-second period
*Max.*throughput	Peak throughput over 10 seconds, as observed during the period Over 1 minute, the max. throughput is the maximum of the six 10-second samples Over 10 minutes, the max. throughput is the maximum of the sixty 10-second samples
Use throughput	Represents the use percentage, as defined according to the shaping throughput
Compression (for grooming rules and sub-tree rules)	
Compression throughput	A compression throughput of P% implies that the network was able to carry 1/(1-P%) additional traffic:

[5] Except if QoS actions type is set to Transparent

	- 50 % → x2 - 66 % → x3 - 75 % → x4 - 80 % → x5
Max. uncompressed throughput	Peak throughput over 10 seconds carried on the network due to compression (observed during the period) Over 1 minute, the max. throughput is the maximum of the six 10-second samples Over 10 minutes, the max. throughput is the maximum of the sixty 10-second samples
QoS	
Average QoS activity throughput	Indicates the time percentage during which the StreamGroomer QoS engine was active during the period
Maximum QoS activity *throughput*	Activity peak over 10 seconds, as observed during the period Over 1 minute, the maximum activity throughput is the maximum of the six 10-second samples taken over 1 minute. Likewise over 10 minutes.
Average stress	Unique indicator used to measure the application load. High values of stress indicate that business application sessions were competing to get bandwidth.
Max. stress	Stress peak over 10 seconds, as observed during the period Over 1 minute, the max. stress is the maximum of the six 10-second samples Over 10 minutes, the max. stress is the maximum of the sixty 10-second samples
Frames	
Nr. of frames	Number of frames observed
% frames < 128 bytes	Percentage of the number of frames per size
% frames 128 – 1200 bytes	
% frames > 1200 bytes	
Maximum frames size	Maximum frame size observed

The performance theme differs depending on the type of rule:

Indicator	Description
Network Performance (access link, shaping rule)	
Link status	Two statuses: available, unavailable. A 10 sec. period is considered as unavailable if at least half of the pings are lost.
Active Probe round trip time (min, avg, max)	Round-trip time measured by ping between the StreamGroomer administration interface and a remote network element (router…)
Active probe loss throughput	Measurements of ping packet loss
Link availability throughput	Availability ratio of the active probe (% of 10s-second available periods). A 10 sec. period is considered as unavailable if at least half of the ping are lost.
Average number of cnx	Average number of connections observed within the rule This number is not necessarily an integer, since the connections are not necessarily set up throughout the entire period
Instantaneous number of cnx	Instantaneous number of connections observed within the rule
Network Performance (grooming rule)	
Status Grooming	Operation status of the grooming and duration of this status

	Used to confirm the grooming synchronization
Grooming round-trip time (min, avg, max)	Round-trip time between 2 StreamGroomers
Grooming jitter (avg, max)	Jitter between two StreamGroomers
Grooming availability ratio	Availability ratio of the grooming (% of 10s-second available periods). The availability ratio equals the status grooming on a 10s period
Grooming loss ratio	Loss throughput between two StreamGroomers. Beware, this throughput may be negative in grooming mode without tunnel: from WAN flows are classified in the Grooming rule although they were not seen in transmission in the Grooming rule of the opposite StreamGroomer
Average number of cnx	Average number of connections observed within the rule This number is not necessarily an integer, since the connections are not necessarily set up throughout the entire period
Instantaneous number of cnx	Instantaneous number of connections observed within the rule
Application Performance (terminal data rule)	
Total time	Average time elapsed between the transmission of a client request till the complete reception of the server answer
Server time	Average time elapsed on the server between the reception of a client request till the beginning of the server answer
Network time	Total time – average server time (the network time includes both the round-trip time between the client and the server, and the amount of data to be transmitted)
WAN round-trip time	Round-trip time between the output of a TCP packet with Push bit on the WAN interface and reception of acknowledgment of this packet
LAN round-trip time	Round-trip time between the output of a TCP packet with Push bit on the LAN interface and reception of acknowledgment of this packet
TCP calls	Number of TCP calls observed per minute The value over 10 seconds is extrapolated to 1 minute
Average number of cnx	Average number of connections observed within the rule This number is not necessarily an integer, since the connections are not necessarily set up throughout the entire period
Instantaneous number of cnx	Instantaneous number of connections observed within the rule
TCP throughput retransmission	Evaluation of packets retransmitted on the TCP connections Retransmission is often due to packet loss.
Available throughput	Indicates the data throughput that a new session would be get in this rule Available only for an SG in Monitoring&Control mode
VoIP/Video Performance (terminal audio/video rule)	
MOS-CQ	Average Mean Opinion Score for VoIP traffic MOS-CQ = MOS Conversational Quality (takes into account latency, loss, jitter)
MOS-CQ min	MOS-CQ minimum over 10 seconds, as observed during the period Over 1 minute, the min MOS is the minimum of the six 10-second samples Over 10 minutes, the min MOS is the minimum of the sixty 10-second samples
MOS LQ	Average Mean Opinion Score for VoIP traffic MOS-LQ = MOS Listener Quality (takes into account loss, jitter but not latency)

MOS LQ min	MOS-LQ minimum over 10 seconds, as observed during the period Over 1 minute, the min MOS is the minimum of the six 10-second samples Over 10 minutes, the min MOS is the minimum of the sixty 10-second samples
Network delay RTCP	Latency of the network estimated by analyzing RTCP traffic
Network loss RTP	Packet loss due to the network estimated by analyzing RTP headers
Network loss RTP max.	Peak loss over 10 seconds, as observed during the period Over 1 minute, the max loss is the maximum of the six 10-second samples Over 10 minutes, the max loss is the maximum of the sixty 10-second samples
Discard throughput	Packet loss related to the buffer jitter of the phone, estimated by analyzing RTP headers. Usually a packet is discarded by a phone if it is received with too much jitter.
Discard throughput max	Peak discard throughput over 10 seconds, as observed during the period Over 1 minute, the max discard throughput is the maximum of the six 10-second samples Over 10 minutes, the max discard throughput is the maximum of the sixty 10-second samples
Jitter	Jitter due to the network estimated by analyzing RTP headers.
Jitter max	Peak jitter over 10 seconds, as observed during the period Over 1 minute, the max jitter is the maximum of the six 10-second samples Over 10 minutes, the max jitter is the maximum of the sixty 10-second samples
Burst density	Characterizes loss as being burst or random
Number of communications	Number of communications observed within the rule
WAN Optimization (access link)	
WAN Optimized throughput (bps)	The optimized throughput between the LAN and WAN in bits per second (bps) over 1 minute, and 10 minutes. **Note:** At 10 seconds, WAN Optimization is negligible and a meaningful interpretation cannot be deduced, therefore this data is not presented on this page.
Optimization Factor	Represents the WAN optimization effectiveness during an optimization period over 1 minute, and 10 minutes. **Note:** At 10 seconds, WAN Optimization is negligible and a meaningful interpretation cannot be deduced, therefore this data is not presented on this page.
Performance (other rules)	
Average number of cnx	Average number of connections observed within the rule This number is not necessarily an integer, since the connections are not necessarily set up throughout the entire period
Instantaneous number of cnx	Instantaneous number of connections observed within the rule

Note: Three other themes are available by clicking on Expert mode at the bottom of the sub-tab page: Queues (terminal rules only), Fragmentation, and ToS field + Expert indicators in a grooming rule.

162 BREAKDOWN

The *Real-time Stats - Breakdown* sub-tab displays traffic classification and bandwidth consumption by the rules in a sub-tree.

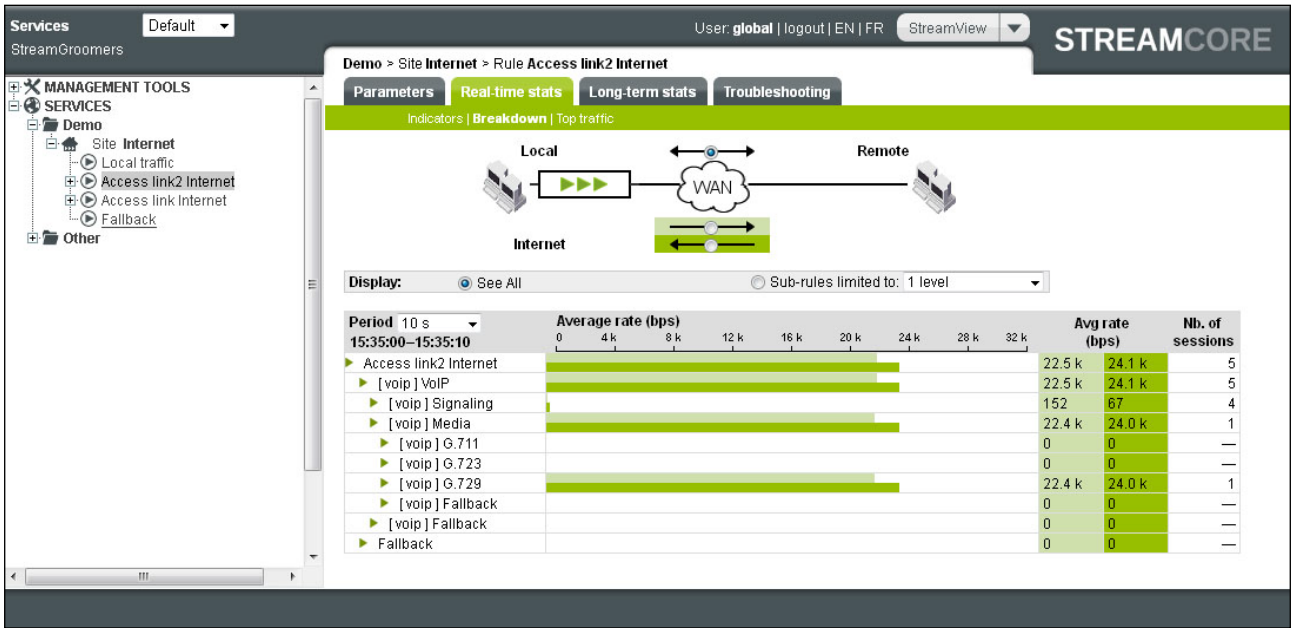


Figure 144 – Real-time stats - Breakdown

163 TOP TRAFFIC

The *Real-Time Stats – Top Traffic* sub-tab displays terminal rules in a sub-tree consuming the most bandwidth.

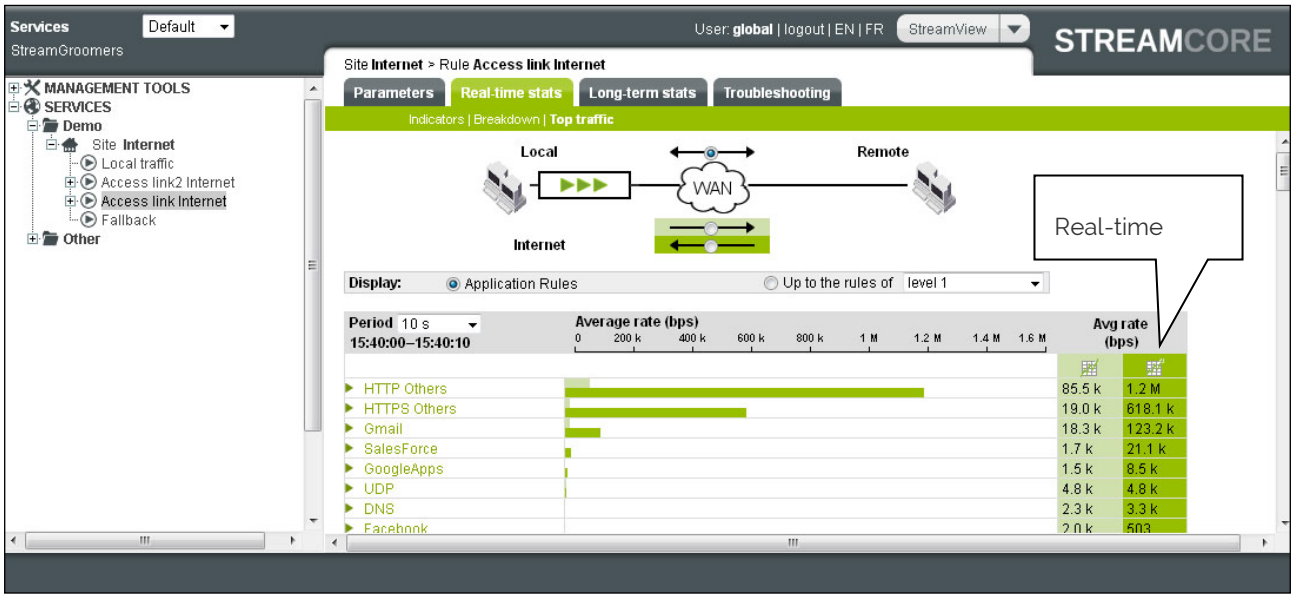


Figure 145 – Real-time stats – Top traffic

10.1.3 Long-term Stats

164 OVERVIEW

The *Long-term Stats* visibility service on a rule provides statistics over the long-term (day, week, month, year):

- **For any rule:** *Indicators* computed for all traffic classified in the rule. Some of these indicators are common between all rules while others are specific to the type of rule (access link, shaping, grooming, terminal data, terminal audio/video…)

- **For access link, shaping, grooming and intermediate rules:** additional *Breakdown* and *Top traffic* tools provide an overview of traffic classification and bandwidth consumption by the rules in the sub-tree.

165 INDICATORS

The *Real-time Stats - Indicators* sub-tab displays statistics computed for all the traffic classified within the rule. These statistics are classified into the following themes:

Theme	Description	Availability
Throughput	Set of indicators related to bandwidth consumption	All
WAN Optimization	Set of indicators detailing WAN Optimization (if WAN Optimization is enabled)	Access link, shaping, grooming, intermediate rules
QoS	Set of indicators related to the load in terms of QoS	Access link, shaping, grooming, intermediate rules[6]
Compression	Set of indicators detailing compression performance (if compression is enabled)	Grooming rules and sub-tree rules
Performance	Set of indicators related to performance (network, application, VoIP/Video)	Access link, shaping, grooming, terminal data, terminal audio/video

Each theme and the associated indicators are displayed in the following way:

[6] Except if the type of QoS actions is set to Transparent

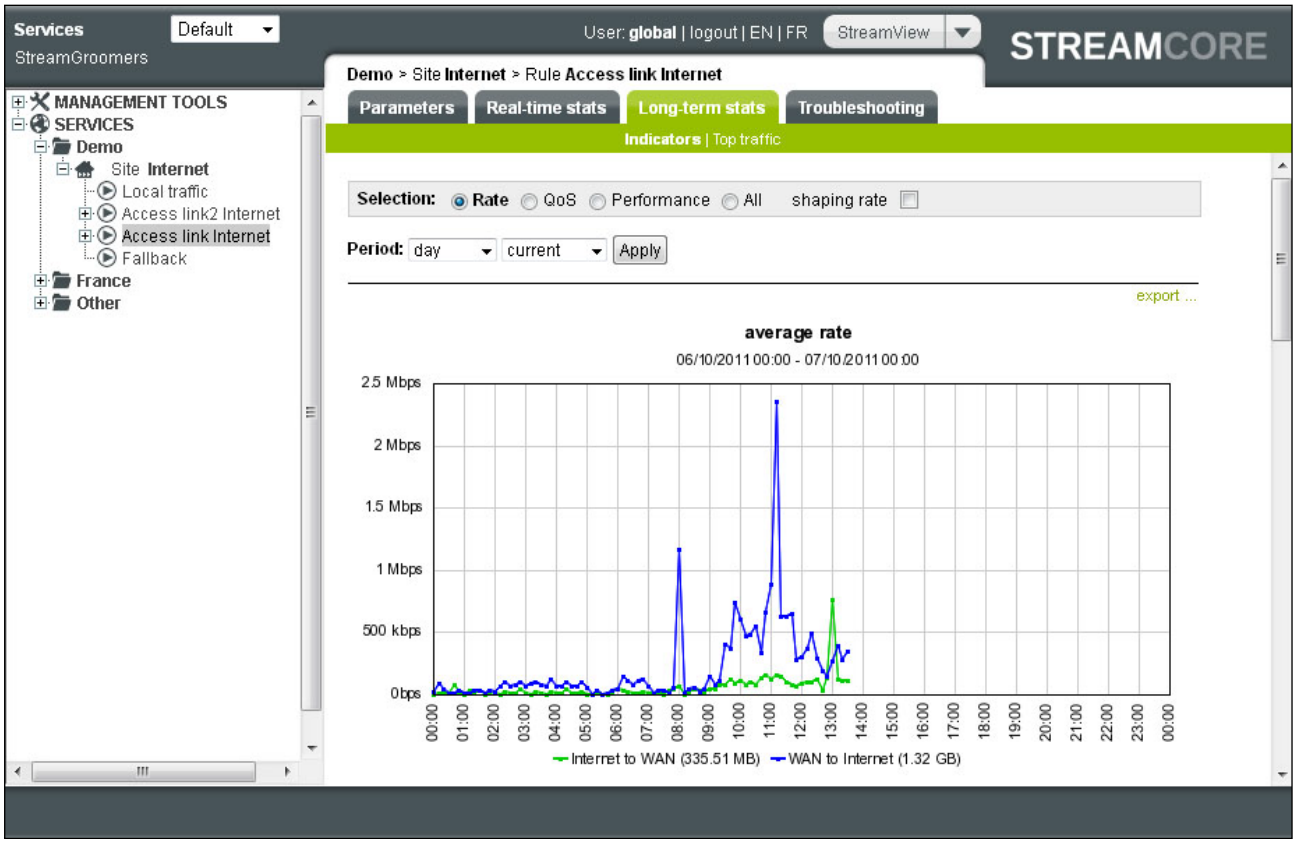


Figure 146 – Long-term stats – Indicators

The generic themes are:

Indicator	Description
Throughput	
Average throughput	Average throughput observed on the rule
Max. throughput	Maximum peak throughput observed among all 10-second samples taken over the period (10 min., 30 min…)
Use- throughput distribution	Percentage of time (i.e., % of 10-second samples over the period) during which the network load is: Low = usage throughput between 0 et 25% Medium = usage throughput between 25 and 50% High = usage throughput between 50 and 75% Very high = usage throughput between 75 and 90% Full = usage throughput between 90 and 100%
WAN Optimization (access link)	
WAN Optimized throughput (bps)	The optimized throughput between the LAN and WAN in bits per second (bps).
Optimization Factor	Represents the WAN optimization effectiveness during an optimization period.
QoS	
Average QoS activity	Percentage of time during which the StreamGroomer QoS engine was active during the period
Maximum QoS activity	QoS activity peak, among all 10-second samples taken over the period (10 min., 30 min…)

Average stress	Unique indicator used to measure the application load. High values of stress indicate that business application sessions were competing to get bandwidth.
Maximum stress	Stress peak, among all 10-second samples taken over the period (10 min., 30 min…)
Compression	
Compression throughput	A compression throughput of P% implies that the network was able to carry 1/(1-P%) additional traffic: - 50 % → x2 - 66 % → x3 - 75 % → x4 - 80 % → x5
Maximum uncompressed throughput	Maximum peak throughput carried on the network due to compression, among all 10-second samples taken over the period (10 min., 30 min…).
Compression-throughput distribution	Top 10 applications with the highest compression throughput (grooming rule only)

The performance theme differs depending on the type of rule:

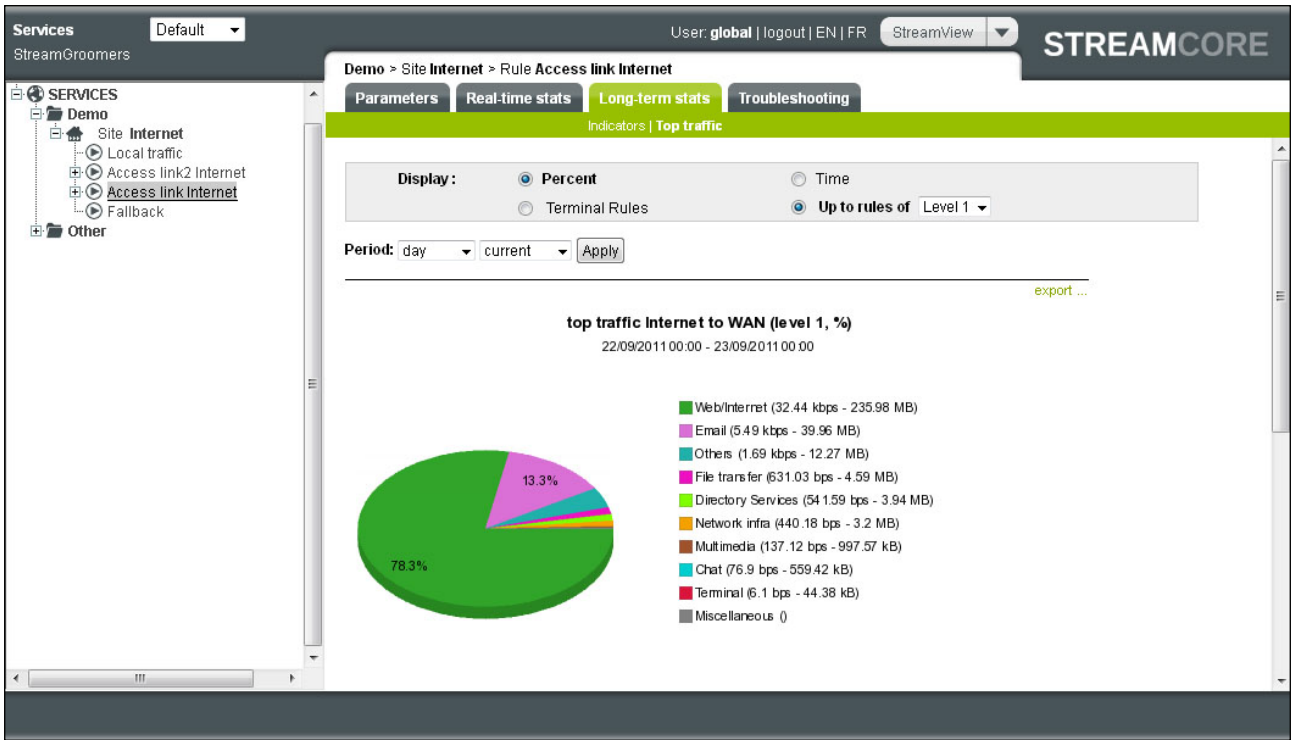
Indicator	Description
Network Performance (access link, shaping)	
Network SLM distribution	Network quality with 10 sec. granularity. Available only if a Network SLM group of alarm is defined on the shaping rule (see chapter 9.2.2.4)
Active Probe round trip time (min, avg, max)	Round-trip time measured by ping between the StreamGroomer administration interface and a remote network element (router…)
Active probe availability	Availability ratio of the active probe (% of 10s-second available periods). A 10 sec. period is considered as unavailable if at least half of the ping are lost.
Active probe loss throughput	Active probe packet loss throughput
Average number of cnx	Average number of connections observed within the rule
Network Performance (grooming)	
Network SLM distribution	Network quality with 10 sec. granularity. Available only if a Network SLM group of alarm is defined on the grooming rule (see chapter 9.2.2.4)
Grooming link round-trip time	Round-trip time between 2 StreamGroomers
Grooming availability	Availability ratio between two StreamGroomers (% of 10s-second available periods). A 10 sec. period is considered as unavailable if the grooming has been desynchronized at least once.
Grooming jitter (avg, max)	Jitter between two StreamGroomers
Grooming link loss ratio	Loss throughput between two StreamGroomers. Beware, this throughput may be negative when in grooming mode without a tunnel: "from WAN" flows may be classified within the Grooming rule although they were not detected in the Grooming rule by the opposite StreamGroomer
Average number of cnx	Average number of connections observed within the rule

Application Performance (terminal data rule)	
Application response time	Measures TCP client-server interactions : Total time = average time elapsed on the client between the transmission of a client request till the complete reception of the server answer Server time = average time elapsed on the server between the reception of a client request till the beginning of the server answer Network time = total time – average server time (the network time includes both the round-trip time between the client and the server, and the amount of data to be transmitted) WAN RTT = round-trip time over the WAN
Breakdown of response-times	Percentage of time (i.e., % of 10-second samples over the period) during which the response time ranges between the following values: 0-100 ms 100-300 ms 300-600 ms 600-1000 ms More than 1000 ms
WAN round-trip time	Average time between the emission of a TCP packet with a Push bit on the WAN interface and reception of acknowledgment of this packet
Available throughput	Indicates the data throughput that a potential new session would be get in this rule. Available only for an SG in Monitoring&Control mode
Average number of cnx	Average number of connections observed within the rule
TCP calls	Number of TCP calls per minute
TCP retransmission throughput	Evaluation of TCP packets retransmitted (usually due to packet loss)
VoIP/Video Performance (terminal audio/video rule)	
MOS CQ & LQ	Average Mean Opinion Score for VoIP traffic MOS-CQ = MOS Conversational Quality (takes into account latency, loss, jitter) MOS-LQ = MOS Listener Quality (takes into account loss, jitter but not latency)
MOS distribution	Percentage of time (i.e., % of 10-second samples over the period) during which the MOS-LQ ranges between the following values: 1 – 2.6 2.6 – 3.1 3.1 – 3.6 3.6 – 4 4 – 5
Network delay RTCP	Latency of the network estimated by analyzing RTCP traffic
Network loss RTP	Packet loss due to the network estimated by analyzing RTP headers
Discard throughput	Packet loss related to the buffer jitter of the phone, estimated by analyzing RTP headers. Usually a packet is discarded by a phone if it is received with too much jitter.
Jitter	Jitter due to the network estimated by analyzing RTP headers.
Number of communications	Number of communications (a communication is usually a RTP session + a RTCP session)
Performance (other rules)	

Average number of cnx	Average number of connections observed within the rule

166 TOP TRAFFIC

The ***Long-term Stats – Top Traffic*** sub-tab displays terminal rules in a sub-tree consuming the most bandwidth.



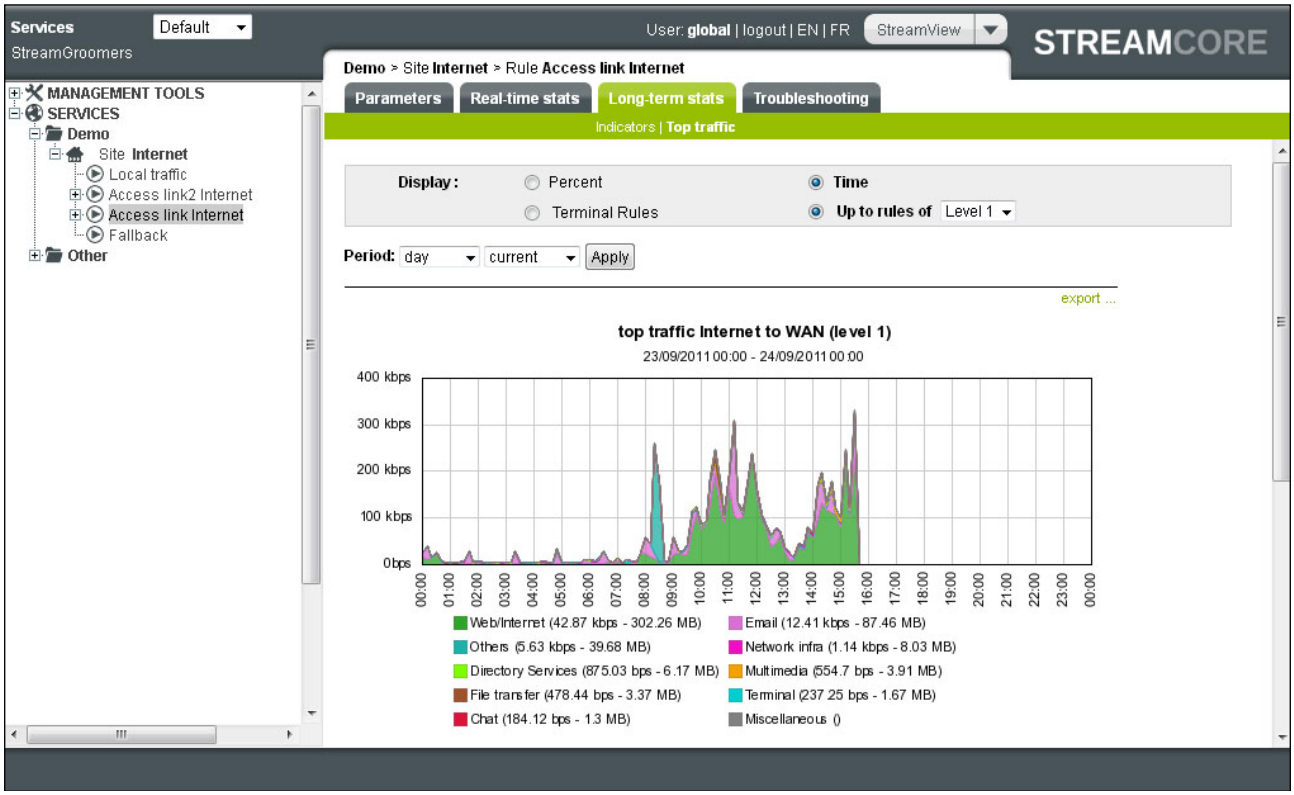


Figure 147 – Long-term stats – Top traffic

10.1.4 Troubleshooting Tools

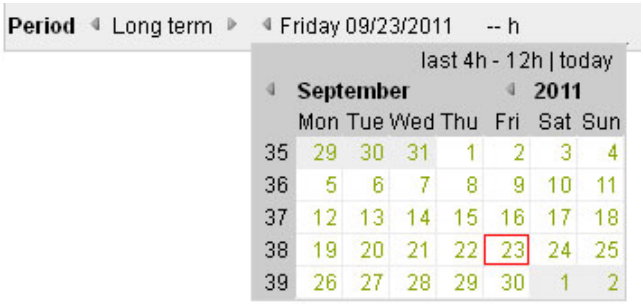
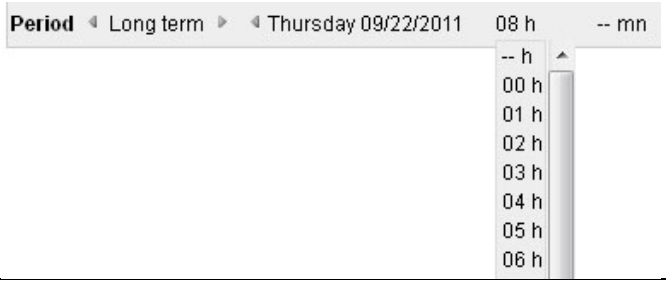
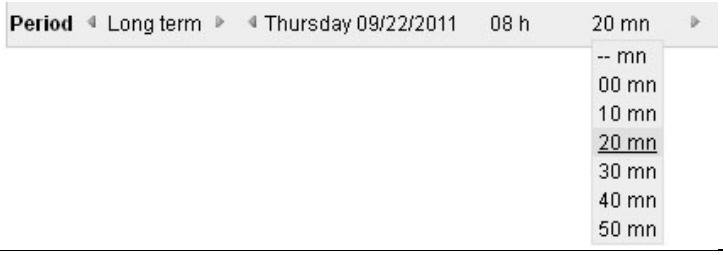
167 OVERVIEW

The **Troubleshooting** visibility services on a rule provide granular information down to the session or even the packet level:

- Packet-based Troubleshooting tools (**Traffic Capture**) is available **only** on terminal rules, and only in **real-time** (no packet-based data storage): a traffic capture can be displayed live within the Graphical User Interface, or can be saved to be analyzed in specialized applications such as Wireshark.
- Session-based Troubleshooting tools (*Traffic Discovery*, *Top*, ***Live Connections / Communications***) are available by default on all rules. They are always offered over the short-term (last 10 sec, 1 min., 10 min.)

Last 10 sec., 10 sec., 10 min. period selection	

To have long-term visibility, the smart NetFlow export must be activated on a per site basis. See chapter 9.2.3 for more information. When activated on the rule, an additional long-term period selection menu is available:

Specific month, week or day selection	
Specific 1 hour period selection	
Specific 10 min. selection	

168 TOP

The **Troubleshooting – *Top*** sub-tab displays the top hosts consuming the most bandwidth among all the traffic classified in the rule.

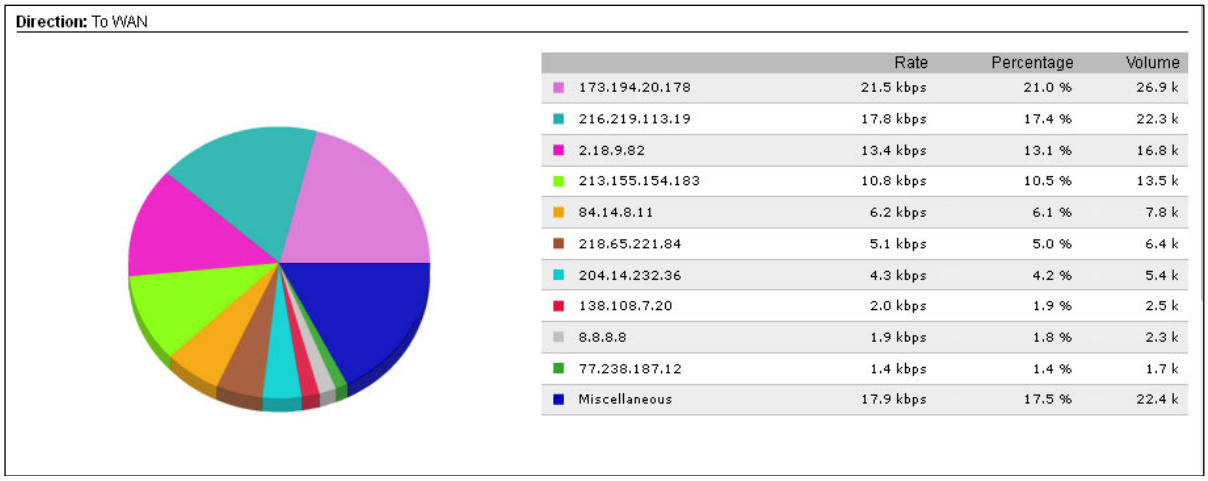


Figure 148 – Troubleshooting – TOP

Selection Parameters (TOP)	Description	Short-term
Period	Enables you to set the period for which TOPs are measures. In order to get long term period, NetFlow must be activated on a rule	X
Duration	It is possible to display TOPs for the following durations: 10 seconds, 1 minute and 10 minutes	X

Display Parameters (TOP)	Description	Short-term
Port	Enables you to display TOPs according to PORT	X
IP	Enables you to display TOPs according to Local and Remote IP addresses	X
Convert addresses into names (Checkbox)	Not checked by default. Enables IP addresses to be converted to names	X

169 CONNECTIONS / COMMUNICATIONS

The **Troubleshooting** – *Connections* or *Communications* sub-tab displays all connections or communications classified in the rule. The *Communications* sub-tab replaces the *Connections* sub-tab only on Terminal audio/video rules with VoIP/Video measurements enabled (RTP or RTP+MOS).

Connections Troubleshooting Tool

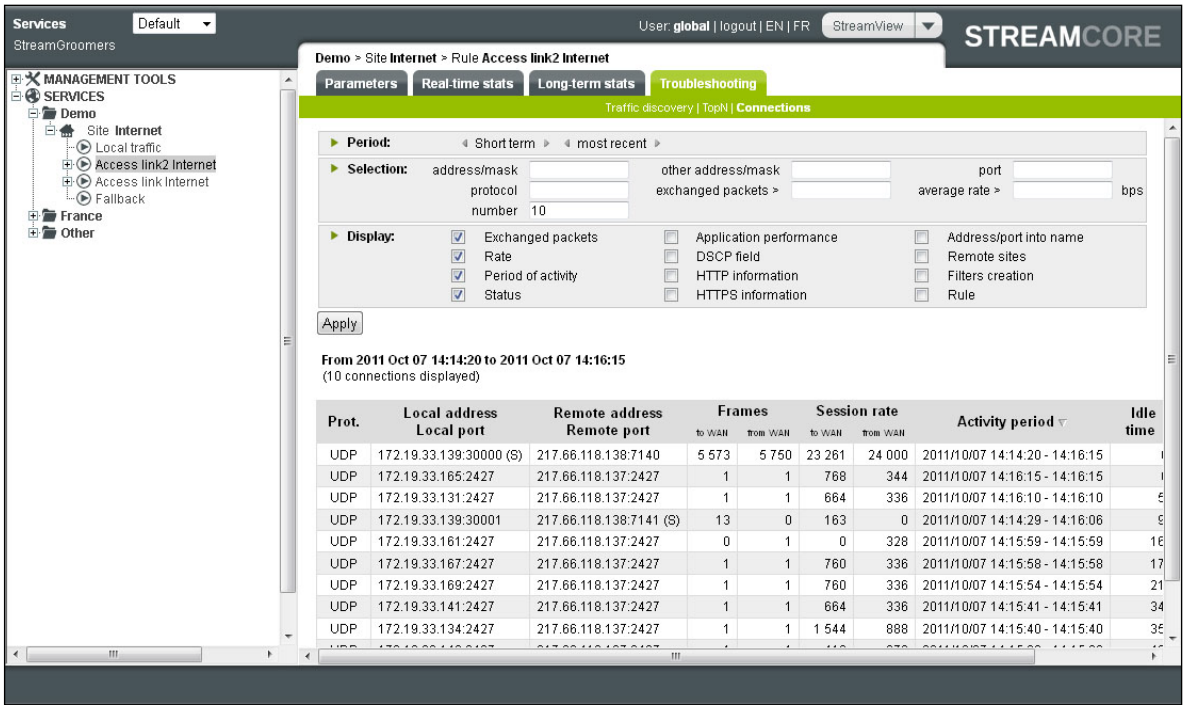


Figure 149 – Troubleshooting – Connections

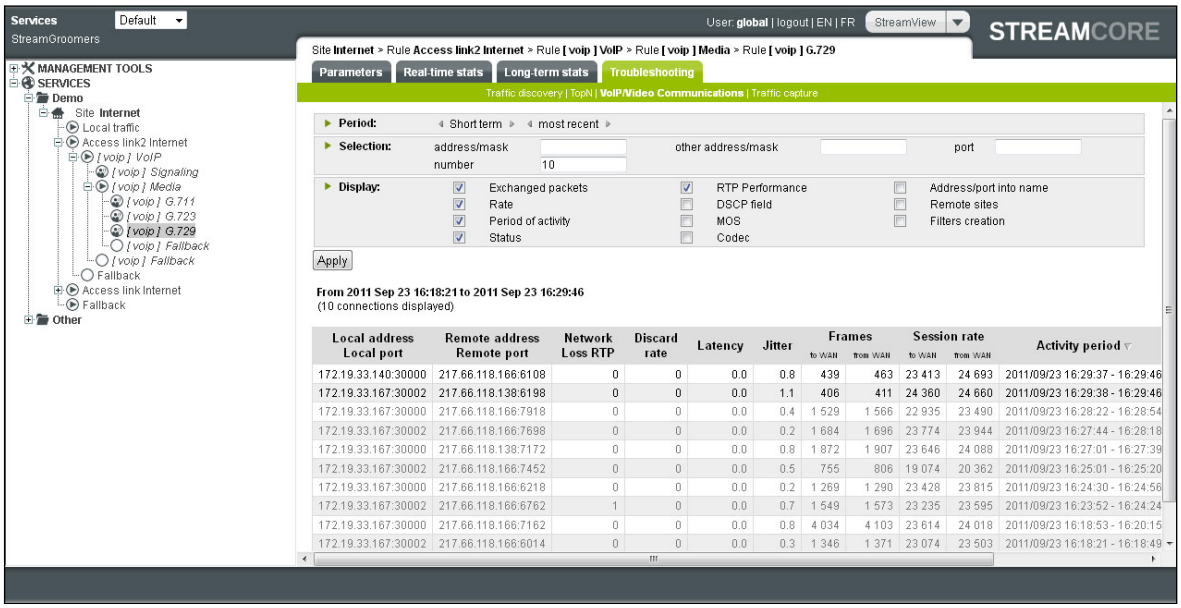
Selection Parameters (Connections)	Description	Short-term	Long-term
Address(es)/Mask	Used to filter the connections set up from or to an @IP, or between 2 @IPs, or for a specific subnet (format aaaa.bbbb.cccc.dddd/N)	X	X
Port	Used to select the connections set up on a particular port. You can indicate a TCP or UDP port number (e.g.: 80) or a name (e.g.: http)	X	X
Protocol	Used to select the connections which used the given protocol. For example: 'TCP', 'UDP', 'ICMP' or IP protocol number	X	X
Exchanged Packets	Used to take into account the connections for which the number of packets exchanged is at least equal to the designated value	X	X
Average throughput	Used to take into account the connections for which the average throughput, as observed, is at least equal to the designated value	X	
Number	Allows to limit to the last N connections matching the selected criteria	X	X

Note: When selecting the 10 sec, 1 min or 10 min period, only active connections during the selected period are displayed. When selecting the most recent connections, the closed connections are displayed but grayed.

Display Parameters (Connections)	Description	Short-term	Long-term
Exchanged Packets	To display the number of packets exchanged during the entire connection	Most recent	X
Application Performance	To display the application response time:	X	X

	- Short-term: observed during the activity period (most recent) or during the selected period (10 seconds, 1 minute, or 10 minutes) - Long-term: observed during the activity period		
Address/port into names	To display host names and services rather than addresses and ports	X	X
Throughput	To display the session throughput: - Short-term: observed during the activity period (most recent) or during the selected period (10 seconds, 1 minute, or 10 minutes) - Long-term: observed during the activity period	X	x
DSCP Field	To display the last DSCP field seen	X	X
Remote Sites	To display site name based on subnets declared per site on the SGM	X	X
Period of Activity	To display: - the dates of the first and last packets observed on the connection - the idle time (short-term only), i.e. the time elapsed between observation of the last packet	X	X
HTTP information	To display the hostname and URL for HTTP connections. This information can also be displayed directly in overcaption by placing the mouse over the TCP protocol.	X	X
HTTPS information	To display the SSL certificate information for HTTPS connections. This information can also be displayed directly in overcaption by placing the mouse over the TCP protocol.	X	X
Filter Creation	To display button to create a filter based on connection information (see chapter 7.5.3.3)	X	X
Status	To display the status of the connection. The statuses are: call, established, disconnection, failed, closed, silence	X	
Rule	To display the terminal rule into which the connection has been classified	X	X

Communications Troubleshooting Tool



Local address Local port	Remote address Remote port	Network Loss RTP	Discard rate	Latency	Jitter	Frames to WAN	Frames from WAN	Session rate to WAN	Session rate from WAN	Activity period
172.19.33.140:30000	217.66.118.166:6108	0	0	0.0	0.8	439	463	23 413	24 693	2011/09/23 16:29:37 - 16:29:46
172.19.33.167:30002	217.66.118.138:6198	0	0	0.0	1.1	406	411	24 360	24 660	2011/09/23 16:29:38 - 16:29:46
172.19.33.167:30000	217.66.118.166:7918	0	0	0.0	0.4	1 529	1 566	22 935	23 490	2011/09/23 16:28:22 - 16:28:54
172.19.33.167:30002	217.66.118.166:7698	0	0	0.0	0.2	1 684	1 696	23 774	23 944	2011/09/23 16:27:44 - 16:28:18
172.19.33.167:30000	217.66.118.138:7172	0	0	0.0	0.8	1 872	1 907	23 646	24 088	2011/09/23 16:27:01 - 16:27:39
172.19.33.167:30002	217.66.118.166:7452	0	0	0.0	0.5	755	806	19 074	20 362	2011/09/23 16:25:01 - 16:25:20
172.19.33.167:30000	217.66.118.166:6218	0	0	0.0	0.2	1 269	1 290	23 428	23 815	2011/09/23 16:24:30 - 16:24:56
172.19.33.167:30002	217.66.118.166:6762	1	0	0.0	0.7	1 549	1 573	23 235	23 595	2011/09/23 16:23:52 - 16:24:24
172.19.33.167:30000	217.66.118.166:7162	0	0	0.0	0.8	4 034	4 103	23 614	24 018	2011/09/23 16:18:53 - 16:20:15
172.19.33.167:30002	217.66.118.166:6014	0	0	0.0	0.3	1 346	1 371	23 074	23 503	2011/09/23 16:18:21 - 16:18:49

Figure 150 – Troubleshooting – Communications

Selection Parameters (Communications)	Description	Short-term	Long-term
Address(es)/mask	Used to filter the communications set up from or to an @IP, or between 2 @IPs, or for a specific subnet (format aaaa.bbbb.cccc.dddd/N)	X	X
Port	Used to select the communications set up on a particular port.	X	X
Number	Allows to limit to the last N communications matching the selected criteria	X	X

Note: When selecting the 10 sec, 1 min or 10 min period, only active communications during the selected period are displayed. When selecting the most recent connections, the closed connections are displayed but grayed.

Display Parameters (Communications)	Description	Short-term	Long-term
Exchanged packets	To display the number of packets exchanged during the entire communication	Most recent	X
RTP performance	To display the RTP performance (jitter, latency, packet loss…): - Short-term: observed during the activity period (most recent) or during the selected period (10 seconds, 1 minute, or 10 minutes) - Long-term: observed during the activity period	X	X
Address/port into names	To display host names and services rather than addresses and ports	X	X
Throughput	To display the session throughput: - Short-term: observed during the activity period (most recent) or during the selected period (10 seconds, 1 minute, or 10 minutes) - Long-term: observed during the activity period	X	x
DSCP field	To display the last DSCP field seen	X	X
Remote sites	To display site name based on subnets declared per site on the SGM	X	X
Period of activity	To display: - the dates of the first and last packets observed on the communication - the idle time (short-term only), i.e. the time elapsed between observation of the last packet	X	X
MOS	To display the MOS per communication.	X	X
Filters creation	To display button to create a filter based on communication information (see chapter 7.5.3.3)	X	X
Status	To display the status of the communication. The statuses are: established, closed, silence	X	
Codec	To display codec information. This information can also be displayed directly in overcaption by placing the mouse over the UDP protocol.	X	X

The *Troubleshooting – Traffic Capture* sub-tab (available in all terminal rules) offer integrated traffic capture capabilities, to be displayed directly in the Graphical User Interface or to be saved so they may be analyzed in specialized applications such as Wireshark.

Note: The **status** area below the start button displays the traffic capture state. If a capture is running on another LAN/WAN interface or rule, it will displayed with a link to the running capture.

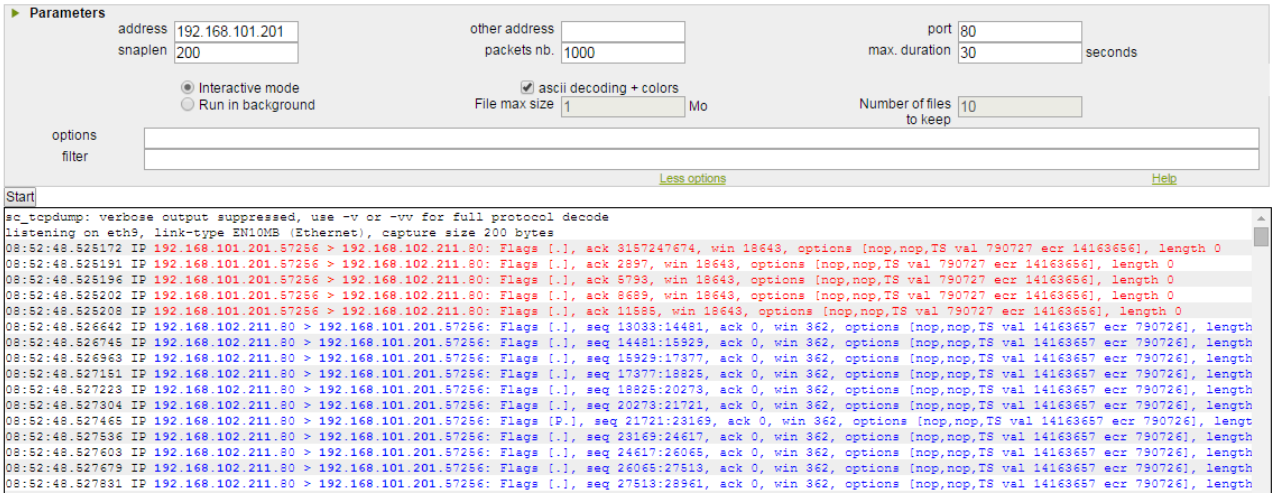


Figure 151 – Troubleshooting – Traffic Capture

Selection Parameters (Traffic Capture)	Description
IP address	Used to filter packets based on IP addresses
Other IP address	Used if you want filter from another IP address
Port	Used to filter packets on a particular port
Data length	To select the packet size being captured for each packet (max = 1500). The default value is set to 200 per packet
Packets nb.	The default packet capture value is 1000
Capture for	The default duration of traffic capture packet is set to 5 minutes. However you can change this by selecting another value in the combo box. Durations available: **Unlimited time** **Seconds:** 5,10 or 15 **Minutes:** 1,5,10 or 30 **Hours:** 1h or 2hr
Interactive Mode and Decode ASCII and use colors	This mode enables you to view traffic capture directly in StreamView. Use the ascii decoding + color checkbox to enhance the displayed results
File Size	You can specify the traffic capture file size you want to download. If you specify a large file size, it is advised that you use the **Check** button to verify that your SG can handle the files size in compliance to the number of files.
Number of files	You can specify the number of files you want to store on the SG. However you should be aware that there is a file storage size limited. If you specify a large amount of files to keep, it is advised that you use the **Check** button. This is to verify that your SG will be in compliance to the file size. The file size will change accordingly and vice-versa.
Check	The **Check** button allows verifies that your SG can store an adequate number of files according to your file size.

Run in background	This mode lets you configure and run the traffic capture tool in the background. It is possible to by specify the maximum file size (packets being transmitted or received) and the number of files to keep. This is particularly helpful if you want to finish other tasks in the interface and come back at a later stage to download a collection of traffic captures. If you want to download multiple traffic captures from the interface, they will be download in a zip format. It is also possible to specify the run in background mode for a specified duration of time using the "capture for" combo box.. Files are stored in a cyclical way meaning that when the file size has reached its limit, old files will be deleted to make way for new files. After the Traffic Capture process has finished the result will be displayed in a table with the following information: • Name of ".pcap" file • Traffic capture date • Capture file size • Download checkbox and Download button See Figure 23 - Traffic Capture tool using run in background mode A traffic capture is complete when one of the two parameters (packets nb or max.duration) has been satisfied. **Note:** If you download the ".pcap" file, it will only be viewable when imported into a packet analyzer (for example Wireshark) for further analysis. **Note:** It is only possible to make one traffic capture at a time and therefore you can only capture the traffic for 1 rule at a time.
More options	Options and Filters See Traffic Capture Options and Filters in the Appendix.
Start (Button)	Start traffic capture according to your set parameters.
Stop (Button)	Let's you stop a traffic capture if you need to change a parameter or cancel.

11 Performance Control Services

11.1 INTRODUCTION

The Rules Tree is useful for visibility purposes but also for QoS and traffic shaping. QoS actions can be defined for each rule of the tree in order to:

- Prevent congestion over the WAN within access and edge routers
- Prioritize business critical traffic
- Reserve bandwidth for real-time communications
- Control the impact of bandwidth hungry and recreational flows (Internet, software updates…)

The type of QoS actions is fixed for specific rules (access link, shaping, grooming, and fallback). For other types of rules:

- The type of QoS actions can be selected among various options.
- Optional QoS policy parameters can be defined and are automatically applied in case of events:
  - Time-based QoS: parameters change according to time of the day
  - Backup QoS: for site with redundant access links, parameters change when one of the links is down

A summary of the available QoS actions types per type of rule is displayed below:

		QOS ACTIONS TYPE	BACKUP QOS	TIME-EXCEPTION QOS
	Local Traffic	-	-	-
	Access link	**LIMITED:** Limited bandwidth	-	-
	Shaping	**AGR-LIMITED:** Limited weight and bandwidth	-	-
	Grooming	**AGR-LIMITED:** Limited weight and bandwidth	-	-
	Intermediate	**TRANSPARENT (default):** QoS defined in sub-rules **RESERVED:** Strict priority with max throughput **AGR-LIMITED:** Limited weight and bandwidth	Yes	Yes
	Terminal data	**UCP-DATA (default):** User Competition Prioritization for data traffic **RESERVED:** Strict priority with max throughput for data traffic **AGR:** Limited weight for non-business traffic **AGR-LIMITED:** Limited weight and bandwidth for non-business traffic **DROP:** All traffic is discarded	Yes	Yes
	Terminal audio/video	**UCP-A/V (default):** User Competition Prioritization for audio/video traffic **RESERVED+UCP:** Strict priority with max throughput and UCP for audio/video traffic **RESERVED:** Strict priority with max throughput for audio/video traffic **AGR:** Limited weight for non-business traffic	Yes	Yes
	Fallback	AGR: Limited weight for non-business traffic	-	-

11.2 NETWORK CONGESTION CONTROL

11.2.1 Overview

The first step when applying traffic shaping and QoS policies is to limit traffic congestion within WAN access or edge routers. Such congestion induces arbitrary bandwidth allocation between flows, as well as latency, packet loss, jitter which seriously impact the performance of interactive applications and real-time communications.

Traffic classified in "Access link rules", "Shaping rules" and "Grooming rules" is throughput limited in both-directions (inbound and outbound) in order to achieve this objective.

11.2.2 Local Access Link (Access Link Rules)

The QoS actions type of an "Access link rule" is fixed to **LIMITED**.

The **main** QoS parameters of an access link rule are:

Parameter	Description / Values
Max shaping throughput	Inbound and outbound local access link data throughput (automatically inherited from the site network parameters, see chapter 7.3.4.1)

The **expert** QoS parameters of an access link rule are:

Expert parameter	Description / Values
Throughput correction	% of the max shaping throughput (used mainly to shape inbound traffic)
WAN encapsulation	(automatically inherited from the site network parameters, see chapter 7.3.4.1)
IPSEC encapsulation performed by the router	

11.2.3 Remote Access Link (Shaping / Grooming Rules)

The QoS actions type of a "Shaping/Grooming rule" is fixed to **AGR-LIMITED**.

The **main** QoS parameters of a shaping/grooming rule are:

Parameter	Description / Values
Relative weight (displayed on site with SG)	(default=100) This parameter is used to allocate bandwidth between multiple shaping and grooming rules competing for bandwidth on the local access link. Set the parameter to N x 100 for shaping/grooming rules requiring N times more bandwidth than shaping/grooming rules with default values.
Max shaping throughput	Inbound and outbound remote access link data throughput (automatically inherited from the site network parameters, see chapter 7.3.4.1)

The **expert** QoS parameters of an access link rule are:

Expert parameter	Description / Values
Throughput correction	% of the max shaping throughput (used mainly to shape inbound traffic)
WAN encapsulation	(automatically inherited from the site network parameters, see chapter 7.3.4.1)
IPSEC encapsulation performed by the router	

11.2.4 Expert Mode – Advanced Congestion Control

171 SITE WITHOUT A SG: MULTI-SHAPING FEATURE

When the access link for a site without StreamGroomers is being managed remotely by multiple StreamGroomers, the Multi-Shaping function can be activated so that the SGM coordinates the traffic management performed by StreamGroomers.

By default, the Multi-Shaping mechanism is enabled globally on the SGM, but is disabled individually for each site. When Multi-Shaping is enabled globally and on a site, the SGM checks on a regular basis (10 sec. per default) that the total traffic exchanged with a remote site does not exceed the access link bandwidth. If it does, then the SGM reduces dynamically the shaping throughput of each shaping rule.

Each site without a StreamGroomer and at least two shaping rules has Multi-Shaping parameters. Click on **SERVICES > ... > Site xx** and then select the *Parameters–Configuration* sub-tab. Click on the **Modify** button, turn on the Multi-Shaping and click the **Apply** button.

The dynamic shaping throughput can be checked at any time by clicking on the *Real-time stats-indicators* sub-tab of a shaping rule.

Note: By default, bandwidth allocation is performed on a fair basis between each shaping rule (relative weight of 100). Advanced provisioning can be performed by clicking on Expert mode, for instance if more bandwidth should be allocated to a specific shaping rule.

To change the global status of the Multi-shaping for all sites (and advanced multi-shaping parameters), open the **MANAGEMENT TOOLS**, select General parameters, click on the **Modify** button to perform changes in the related section, and then on the **Submit** button.

Parameter	Description / Values
Multi-shaping status	(default = Up) To enable/disable the multi-shaping coordinated by the SGM
Dynamic shaping throughput update timer	(default=10 sec.) Dynamic shaping throughput refresh performed by the SGM
Dynamic shaping throughput disabling if SGM unreachable	(default= 30 sec.) Period after which the StreamGroomer will apply the nominal shaping throughput if the SGM has not refreshed it
Minimum throughput (absolute)	(default=20 kbps) Minimum shaping throughput
Minimum throughput (relative)	(default=10%) Minimum shaping throughput in% of the nominal shaping throughput

172 SITE WITH A SG: GROOMING THROUGHPUT MATCHING

When a grooming rule is in tunnel mode, a throughput matching algorithm can be enabled to automatically "sense" the available end-to-end bandwidth.

Select the *Parameters–Configuration* sub-tab of the Grooming rule. Click on the **Modify** button, set the synchronization parameter to "Yes with throughput matching", and click the **Apply** button.

The throughput matching feature is available only if:

- The grooming is synchronized
- The grooming is in tunnel mode

Since the tunnel mode must be enabled, **we recommend to use the throughput matching feature only as a complement to compression or WAN load balancing**.

Note: The only case when the default parameters should be changed is over international or satellite links with very high latency. In order to do so, display the expert parameters on the grooming rule:

Expert parameter	Description / Values
Min. round trip delay	(default = 100 ms) Change the round trip delay according to ping measurements performed when the network is empty.

11.3 QOS POLICIES FOR APPLICATION TRAFFIC

11.3.1 Recommendations

Business-critical applications compete for WAN bandwidth with recreational traffic, file transfers or software updates. QoS policies must be defined based on business-criticality to ensure proper prioritization.

Moreover, most business applications have variable behaviors: some sessions may be interactive and require a small data throughput with a very low latency, whereas other sessions may be bandwidth-hungry and require as much bandwidth as possible. Competition between users of the same application must be managed to ensure fair access and low latency for interactive sessions.

In order to do so, the following policies are recommended:

- **Business-critical application traffic (ERP, CRM…)** needs to be classified in rules with **UCP-DATA** QoS actions and a **high** relative weight in order to ensure:
  - a high priority vs other data traffic
  - automated prioritization between application users (interactive vs bandwidth-intensive)
- **Normal application traffic (mail, intranet Website…)** needs to be classified in rules with **UCP-DATA** QoS actions and a **medium** or **low** relative weight in order to ensure:
  - priority vs recreational traffic
  - automated prioritization between application users (interactive vs bandwidth-intensive)
- **Recreational application traffic (youtube, software updates…)** needs to be classified in rules with **AGR** or **AGR-LIMITED** QoS actions and a **medium** relative weight in order to ensure they do not disrupt business-critical and normal application traffic.

Note: The DROP QoS Actions can also be selected in very specific cases to block flows, for example to prevent traffic from a PC with virus to exchange traffic over the WAN.

11.3.2 QoS Parameters

173 QOS ACTIONS SUMMARY

As a reminder, the possible QoS actions per type of rule are:

	Intermediate	**TRANSPARENT (default):** QoS defined in sub-rules
		RESERVED: Strict priority with max throughput (not recommend for application traffic)
		AGR-LIMITED: Limited weight and bandwidth
	Terminal data	**UCP-DATA (default):** User Competition Prioritization for data traffic
		RESERVED: Strict priority with max throughput for data traffic (not recommend for application traffic)
		AGR: Limited weight for non-business traffic
		AGR-LIMITED: Limited weight and bandwidth for non-business traffic
		DROP: All traffic is discarded

When using "Intermediate rules", the following QoS Actions are equivalent:

> Intermediate (**TRANSPARENT**) > Terminal data (*XXX*)	> Terminal data (*XXX*)
> Intermediate (**AGR-LIMITED**) > Terminal data (**AGR**)	> Terminal data (**AGR-LIMITED**)
> Intermediate (**AGR-LIMITED, unlimited**) > Terminal data (**AGR**)	> Terminal data (**AGR**)

174 UCP-DATA

The main QoS parameter of UCP-DATA QoS actions is:

Parameter	Description / Values
Relative weight per session	(default=100) This is the default type of QoS actions for terminal data rules. Set the relative weight according to the business criticality of the traffic classified in the rule. For example: • 1000 for high priority rule • 100 for medium priority rule • 10 for low priority rule In that case, a session in the high priority rule will get: • 10 times more bandwidth than a session in the medium priority rule • 100 times more bandwidth than a session in the low priority rule The total bandwidth allocated to a rule with UCP-DATA QoS actions will depend on the number of sessions classified in the rule.

175 AGR

The main QoS parameter of AGR QoS actions is:

Parameter	**Description / Values**
Relative weight	(default=100) The allocated bandwidth is limited with an aggregated weight whatever the number of sessions classified in the rule. For example, if the relative weight is 100, all traffic in the rule will get: • 10 times less bandwidth than each session in a rule with UCP-DATA and a weight per session of 1000 • The same bandwidth than each session in a rule with UCP-DATA and a weight per session of 100

176 AGR-LIMITED

The main QoS parameters of AGR-LIMITED QoS actions are:

Parameter	**Description / Values**
Relative weight	(default=100) The allocated bandwidth is limited with an aggregated weight whatever the number of sessions classified in the rule. For example, if the relative weight is 100, all traffic in the rule will get:

	• 10 times less bandwidth than each session in a rule with UCP-DATA and a weight per session of 1000 • The same bandwidth than each session in a rule with UCP-DATA and a weight per session of 100
Max shaping throughput	The allocated bandwidth is always limited by the defined shaping throughput.

177 DROP

This type of QoS actions can be selected to block traffic (for security purpose for instance).

11.3.3 Examples

178 PREDEFINED GROUP OF RULES: STANDARD APPLICATIONS

Rule	QoS actions type	Max. rate	Relative weight	Reserved rate
▶ Thin client				
▶ VDI	UCP-DATA		2000	
▶ Remote access	UCP-DATA		2000	
▶ Fallback	AGR		100	
▶ Web				
▶ Intranet	UCP-DATA		200	
▶ Proxy	UCP-DATA		50	
▶ Fallback	AGR		100	
▶ Lotus Notes	UCP-DATA		100	
▶ Mail	UCP-DATA		20	
▶ File transfer	UCP-DATA		20	
▶ Print	UCP-DATA		20	
▶ Network	UCP-DATA		1000	
▶ Unclassified				
▶ TCP	AGR		10	
▶ UDP	AGR		10	
▶ Fallback	AGR		100	
▶ Fallback	AGR		100	

Figure 152 – Predefined Standard applications group of rules – QoS action summary

179 PREDEFINED GROUP OF RULES: STANDARD SSL

Rule	QoS actions type	Max. rate	Relative weight	Reserved rate
SSL				
SaaS				
GoogleApps	UCP-DATA		2000	
MSOnline	UCP-DATA		2000	
SalesForce	UCP-DATA		2000	
Fallback	AGR		100	
WebConferencing				
GoToMeeting	UCP-DATA		5000	
AdobeConnect	UCP-DATA		5000	
AttConnect	UCP-DATA		5000	
Webex	UCP-DATA		5000	
LotusLive	UCP-DATA		5000	
Fallback	AGR		100	
WebMail				
Hotmail	UCP-DATA		100	
Gmail	UCP-DATA		100	
Yahoo	UCP-DATA		100	
Fallback	AGR		100	
Social networks				
Facebook-S	UCP-DATA		100	
Linkedin-S	UCP-DATA		100	
Fallback	AGR		100	
Others SSL	AGR		100	
Fallback	AGR		100	
Fallback	AGR		100	

Figure 153 – Predefined Standard SSL group of rules – QoS action summary

11.4 QOS POLICIES FOR VOIP/VIDEO TRAFFIC

11.4.1 Recommendations

Audio and Video communications require a dedicated bandwidth with a minimum latency, jitter and packet loss. Moreover, it becomes critical to distinguish and apply tailored policies for traditional IP telephony traffic, room-based videoconferencing, or desktop video software clients.

In order to do so, the following policies are recommended:

- **VoIP and room-based videoconferencing** traffic needs to be classified in rules with **RESERVED** QoS actions to reserve bandwidth and ensure the best possible performance. Enough bandwidth should be guaranteed so that there is no competition between communications within a rule.
- **Video desktop traffic** needs to be classified in rules with **RESERVED** and **UCP-A/V** QoS actions in order to ensure:
  - a reserved amount of bandwidth for all desktop video.
  - automated prioritization between video users when the maximum reserved bandwidth is reached.
- **Signaling traffic** needs to be classified in rules with **UCP-A/V** QoS actions and a high relative weight in order to ensure:
  - a high priority vs other data traffic
  - automated prioritization between signaling users (interactive vs bandwidth-intensive)

Note: VoIP/Video traffic can be managed only on sites with StreamGroomers. VoIP/video rules are always located below the Access link rules to manage any-to-any communications.

Note: The bandwidth reservation mechanisms provided by StreamGroomers can be combined with Call Admission Control (CAC) on the Communication/Call Manager from the IP Telephony or UC provider.

11.4.2 QoS Parameters

180 QOS ACTIONS SUMMARY

As a reminder, the possible QoS actions per type of rule are:

	Intermediate	**TRANSPARENT (default):** QoS defined in sub-rules
		RESERVED: Strict priority with max throughput
		AGR-LIMITED: Limited weight and bandwidth (not useful for VoIP/Video traffic)
	Terminal audio/video	**UCP-A/V (default):** User Competition Prioritization for audio/video traffic
		RESERVED+UCP: Strict priority with max throughput and UCP for audio/video traffic
		RESERVED: Strict priority with max throughput for audio/video traffic
		AGR: Limited weight for non-business traffic (used mostly in fallback rules)

When using "Intermediate rules", the following QoS Actions are equivalent:

> Intermediate (**TRANSPARENT**) > Terminal audio/video (*XXX*)	> Terminal audio/video (*XXX*)
> Intermediate (**RESERVED**) > Terminal audio/video (**AGR**)	> Terminal audio/video (**RESERVED**)
> Intermediate (**RESERVED**) > Terminal audio/video (**UCP A/V**)	> Terminal audio/video (**RESERVED+UCP**)

181 RESERVED AND RESERVED+UCP

The main QoS parameters of RESERVED QoS actions are:

Parameter	Description / Values
Max reserved bandwidth (bps)	Traffic will be granted a strict priority until a maximum throughput when competing with other flows on the upper QoS scheduler (usually the access link rule)
Max reserved bandwidth (% max throughput)	Same as above, but the maximum throughput is automatically computed according to the shaping throughput of the upper QoS scheduler (usually the access link throughput)

182 UCP-A/V (USER COMPETITION PRIORITIZATION)

The main QoS parameter of UCP QoS actions is:

Parameter	Description / Values
Relative weight per session	(default=100) In case the reserved bandwidth in an upper scheduler is shared between various terminal audio/video rules with different types of traffic (for example different types of users), then various relative weights can be set. For example: • 1000 for high priority rule • 100 for medium priority rule

	• 10 for low priority rule In that case, a communication in the high priority rule will always get: • 10 times more bandwidth than a communication in the medium priority rule • 100 times more bandwidth than a communication in the low priority rule

11.4.3 Examples

183 PREDEFINED GROUP OF RULES: AUDIO+VIDEO

Rule	QoS actions type	Max. rate	Relative weight	Reserved rate
Audio+Video				
Signaling	UCP-A/V		1000	
Audio	RESERVED			20 %
G.711	UCP-A/V		100	
G.722	UCP-A/V		100	
G.723	UCP-A/V		100	
G.728	UCP-A/V		100	
G.729	UCP-A/V		100	
audio-Microsoft	UCP-A/V		100	
audio	UCP-A/V		100	
Fallback	AGR		100	
Video	RESERVED			30 %
H.261	UCP-A/V		100	
H.263	UCP-A/V		100	
video-Microsoft	UCP-A/V		100	
video	UCP-A/V		100	
Fallback	AGR		100	
Fallback RTP	AGR		100	
Fallback	AGR		100	
Fallback	AGR		100	

Figure 154 – Predefined Audio+Video group of rules – QoS action summary

184 PREDEFINED GROUP OF RULES: STANDARD VOIP

Rule	QoS actions type	Max. rate	Relative weight	Reserved rate
VoIP				
Signaling	UCP-A/V		1000	
Media	RESERVED			35 %
G.711	UCP-A/V		100	
G.723	UCP-A/V		100	
G.729	UCP-A/V		100	
Fallback	AGR		100	
Fallback	AGR		100	
Fallback	AGR		100	

Figure 155 – Predefined standard VoIP group of rules – QoS action summary

11.5 EXPERT MODE

185 BACKUP QOS

When 2 access links have been defined on a site and one of the access links is detected as down by the StreamGroomer (see chapter 7.3.5), a backup QoS policy can be automatically implemented by the StreamGroomers for all application and VoIP/video rules.

In order to define backup QoS parameters per rule:

1. Click on **SERVICES > ... > site xx > ... > rule xx** in the tree menu for the site. Select the ***Parameters – Configuration*** **sub-tab.**
2. Click on the **Modify** button, display Expert mode parameters and set the backup QoS parameters.
3. Click on the **Submit** button.

186 TIME-EXCEPTION QOS

Time-exceptions policies management

QoS parameters can be changed automatically by the StreamGroomer according to Time-exception policies.

To manage Time-exception policies, open the **MANAGEMENT TOOLS** in the tree menu, click on **Time catalog > QoS time-exceptions**. You can add/modify/delete Time exceptions policies.

The parameters are:

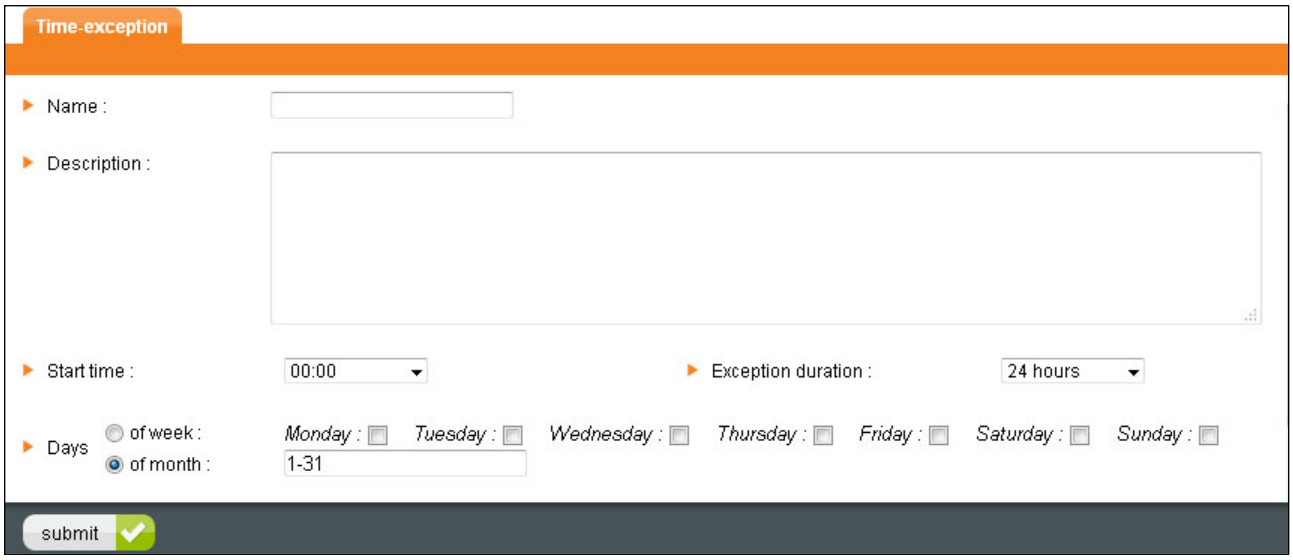


Figure 156 – Time-Exception parameters

Parameter	Description / Values
Name	Name of the Time-exception
Description	Description of the Time-exception
Start time / Exception duration	(default=00:00 / 24 hours) When the QoS time-exception parameters need to be applied at specific time of the day, select when and for how long.
Days	Select the days during which the QoS time-exception parameters should be applied

Note: The timezone parameter needs to be defined on the StreamGroomer.

Examples:

	Week end	Night periods	End of month
Start time / Exception duration	00:00 / 24 hours	20:00 / 12 hours	00:00 / 24 hours
Days	Saturday, Sunday	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	25-31

Time exception QoS parameters per rule

In order to define Time-exception QoS parameters per rule:

1. Click on **SERVICES > ... > site xx > ... > rule xx** in the tree menu for the site. Select the *Parameters – Configuration* sub-tab.
2. Click on the **Modify** button, display Expert mode parameters:
3. Select one of the available Time-exception policies
4. Set the Time-exception QoS parameters
5. Click on the **Submit** button

Note: You can apply different Time-exception policies on different rules, for instance:
-change the QoS parameters of business applications during non-business hours or at the end of the month
-change the QoS parameters of database backup replication traffic during week ends

11.5.1.1 MONITOR QOS PARAMETERS IN USE

The QoS parameters being used can be checked on any rule, by clicking on the *Real-time stats - Indicators* sub-tab. The possible values are:

- Nominal
- Backup
- Time-exception

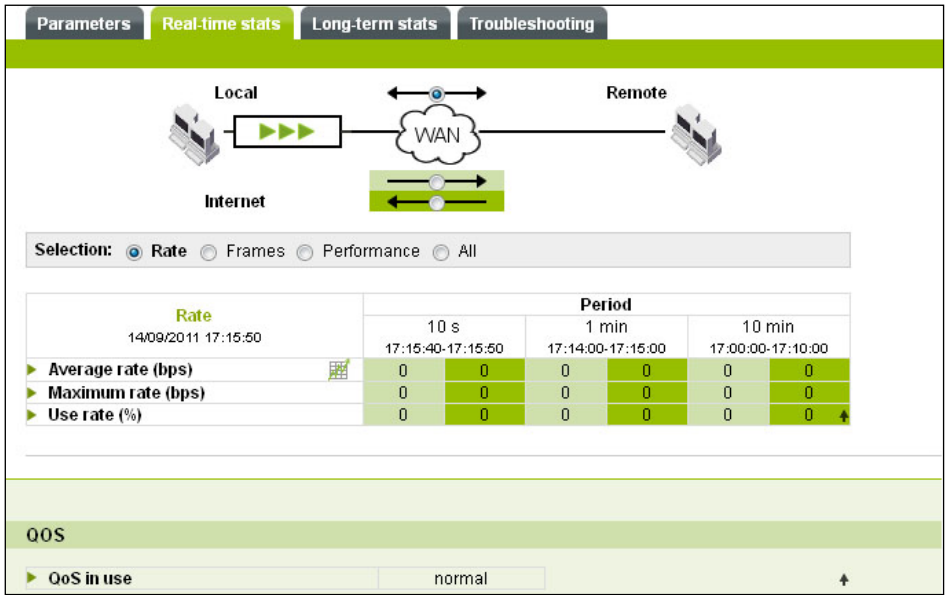


Figure 157 – Monitor QoS parameters in use

11.5.2 DSCP Field Marking and Queuing Management

187 DSCP FIELD MARKING

StreamGroomers can be used to enforce the DSCP value of IP headers of packets exchanged through the StreamGroomer towards the LAN or the WAN. An administrator can do so to interoperate with Class of Service mechanisms defined in WAN routers, to benefit for the DPI and flexible classification engine offered by StreamGroomers.

The following expert parameters for DSCP field management are available in **Terminal rules:**

Expert parameter	Description / Values
DSCP marking to LAN	(default=Transparent) Select the DSCP/ToS field value to be enforced
DSCP marking to WAN	(default=Transparent) Select the DSCP/ToS field value to be enforced

188 QUEUING MANAGEMENT

When schedulers are activated to shape traffic, packets are buffered in queues before being selected according to their priority and QoS settings. There is:

- One queue per session if the QoS action type is
  - UCP-A/V
  - UCP-DATA
  - RESERVED+UCP
- One queue for all sessions if QoS action type is
  - RESERVED
  - AGR
  - AGR-LIMITED

Note: We do not recommend changing default Queuing settings. Only in very specific cases, the following expert parameters for queuing management are available in Terminal rules:

Expert parameter	Description / Values
Size (bytes)	The default values are: • 64 kbytes (UCP-A/V, UCP-DATA, RESERVED+UCP) • 128 kbytes (RESERVED, AGR, AGR-LIMITED)
Queue drop policy	The default values are: • "Tail drop" for Terminal data rules (UCP-DATA) • "RED" for Terminal data rules (RESERVED, AGR, AGR-LIMITED) • "Video-WRED" for Terminal audio/video rules

11.6 QOS STATISTICS

11.6.1 Site Statistics

The *Real-time stats – Optimization* and *Long-term stats - Optimization* sub-tabs display a summary of QoS statistics by selecting the "QoS activity" theme:

	Real-time statistics	***Long-term statistics***
QoS activity throughput per access link	QoS activity throughput per access link	
QoS activity throughput per shaping/grooming	List of all shaping/grooming rules	Top 10 Shaping/Grooming access links with the most QoS activity

11.6.2 Rule Statistics

On access link and shaping/grooming rules, the ***Real-Time stats - Indicators*** and ***Long-term stats - Indicators*** sub-tabs display QoS statistics for the traffic classified in the rule, by selecting the "QoS activity" theme:

	Real-time statistic	**Long-term statistics**
Average QoS activity throughput	Indicates the time percentage during which the StreamGroomer QoS engine was active during the period	
Maximum QoS activity throughput	Activity peak over 10 seconds, as observed during the period Over 1 minute, the maximum activity throughput is the maximum of the six 10-second samples taken over 1 minute. Likewise over 10 minutes.	QoS activity peak, among all 10-second samples taken over the period (10 min., 30 min…)
Average stress	Unique indicator used to measure the application load. High values of stress indicates that business application sessions were competing to get bandwidth.	
Max. stress	Stress peak over 10 seconds, as observed during the period Over 1 minute, the max. stress is the maximum of the six 10-second samples Over 10 minutes, the max. stress is the maximum of the sixty 10-second samples	Stress peak, among all 10-second samples taken over the period (10 min., 30 min…)

12 Optimization Services

12.1 COMPRESSION / WAN LOAD BALANCING

12.1.1 Overview

When application traffic is exchanged between 2 sites equipped with a StreamGroomer, advanced traffic management can be enabled in grooming rules:

- **Compression:** this feature can help to increase capacity without modifying the existing infrastructure. The average throughput gain ranges between 1.5 and 4 and can be as high as 10 for certain types of traffic. The StreamGroomers generate a shared dictionary and can then exchange labels that symbolize repetitive sequences carried over the WAN. Then, traffic can be decompressed and delivered over the LAN. This method is transparent for servers and client computers and works for all IP flows.
- **WAN load balancing:** when different paths are available, it is possible to create two Grooming rules and activate load balancing between these two Grooming rules to route traffic over the 2 paths. This feature is especially useful when an enterprise has branch offices with dual WAN access links, and wants to manage / control bandwidth for both links, with much more granularity than with traditional load balancing capabilities found in routers

In order to enable compression or WAN load balancing, **a grooming rule must be in tunnel mode**. The StreamGroomer will need to route traffic when de-encapsulated from the tunnel, and therefore proper configuration must be done.

12.1.2 Prerequisite: Grooming Tunneling

Whenever a Grooming tunnel is turned on (for instance, when changing a StreamGroomer mode to "Monitoring + Control"), the SGM automatically checks that routing parameters are correct. Still, it is very important to be aware of the following principle: **when a subnet is added on a site, the StreamGroomer defined on the site should be able to route locally this subnet.**

Several cases can be envisioned:

	Subnet directly connected to the WAN router	Subnet reachable through a LAN router or switch-router
Requisite	The StreamGroomer should have an IP address on the LAN / WAN interface in this subnet.	The StreamGroomer should have a route toward this subnet.
Initial configuration	When a StreamGroomer is created, an IP address can be defined in each subnet defined as directly connected to the WAN router.	When a StreamGroomer is created, a default route to the gateway on the LAN side can be defined.
Modification	To add an IP address, right-click on **STREAMGROOMERS > xx > IP router > addresses**. Select **"Add… → Address**. Fill in the various fields, select the To LAN / To WAN interface, and then click on the "Apply" button.	To add a route, right-click on **STREAMGROOMERS > xx > IP router > routes**. Select **"Add… → Route"**. Fill in the various fields and then click on the "Submit" button.

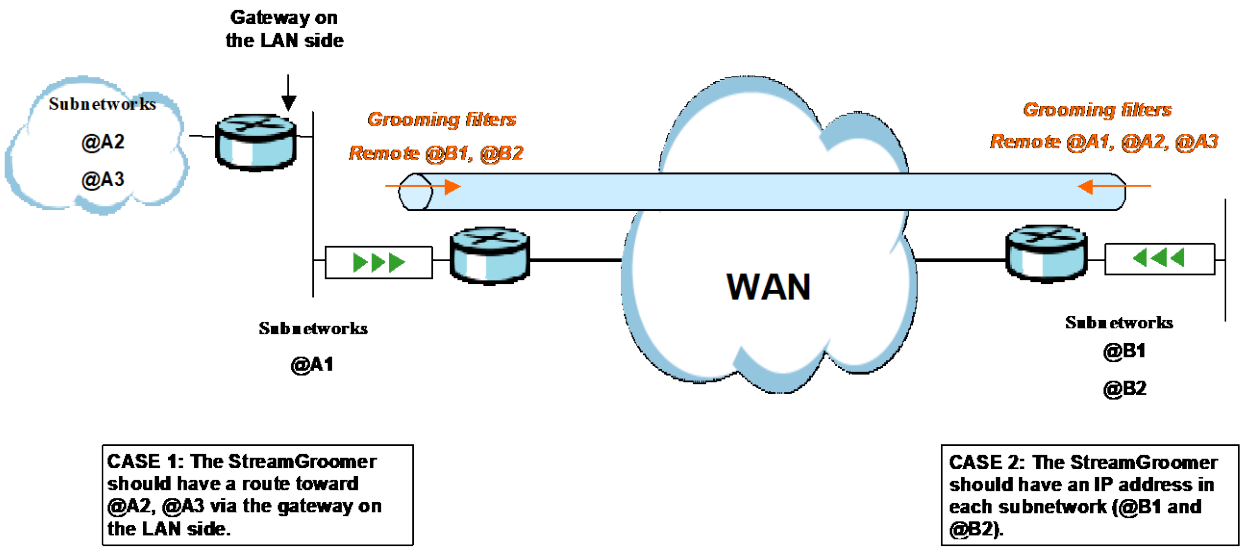


Figure 158 – Example of IP routing provisioning

To display the IP routing table for a StreamGroomer, right-click on **StreamGroomers > xx > IP router** and then on the **Routing table** tab. A tab that enables the display of the **ARP Table** (MAC addresses associated with IP addresses by the StreamGroomer) is also available.

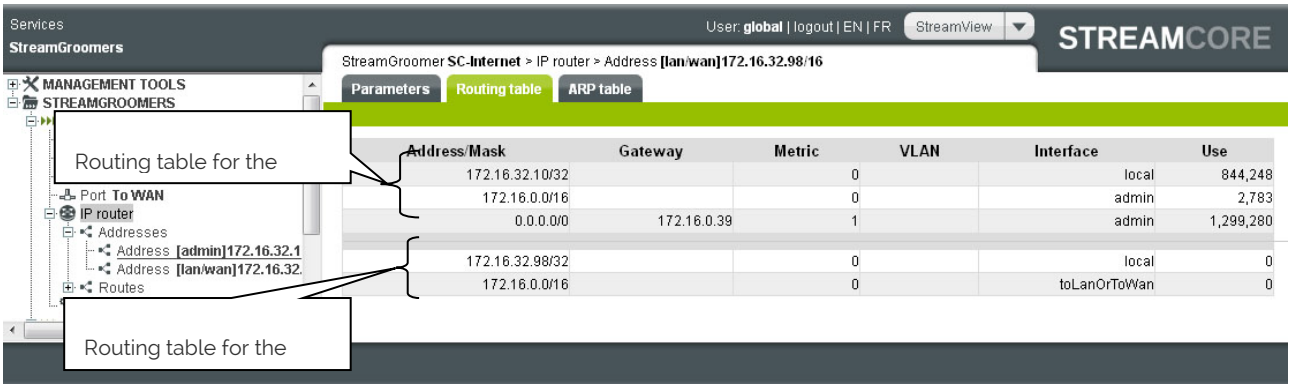


Figure 159 – Routing table for a StreamGroomer

Note: Tunneling in a complex environment such as with 802.1Q trunks or IPSec environments may require further configuration. See chapter 15.2 for more details.

12.1.3 Parameters

189 COMPRESSION

When the tunnel mode is enabled, compression is available. In order to activate compression on a Grooming rule:

1. Click on **SERVICES > ... > site xx > Grooming xx** in the tree menu for the site. Select the *Parameters – Configuration* sub-tab. The tunneling parameter must be set to "Yes" in order to have access to compression parameters.
2. Click on the **Modify** button, change the compression parameter to yes, and then click on the **Submit** button.

Note: The compression throughput can be optimized by deactivating compression in rules with poor compression ratio. To do so, disable the compression expert parameter in these rules.

190 WAN LOAD BALANCING

When different paths are available between two StreamGroomers, it is possible to create two Grooming rules and activate load balancing between these two Grooming rules to route traffic over the 2 paths. This feature is especially useful when an enterprise has branch offices with dual WAN access links, and wants to manage / control bandwidth for both links, with much more granularity than with traditional load balancing capabilities found in routers.

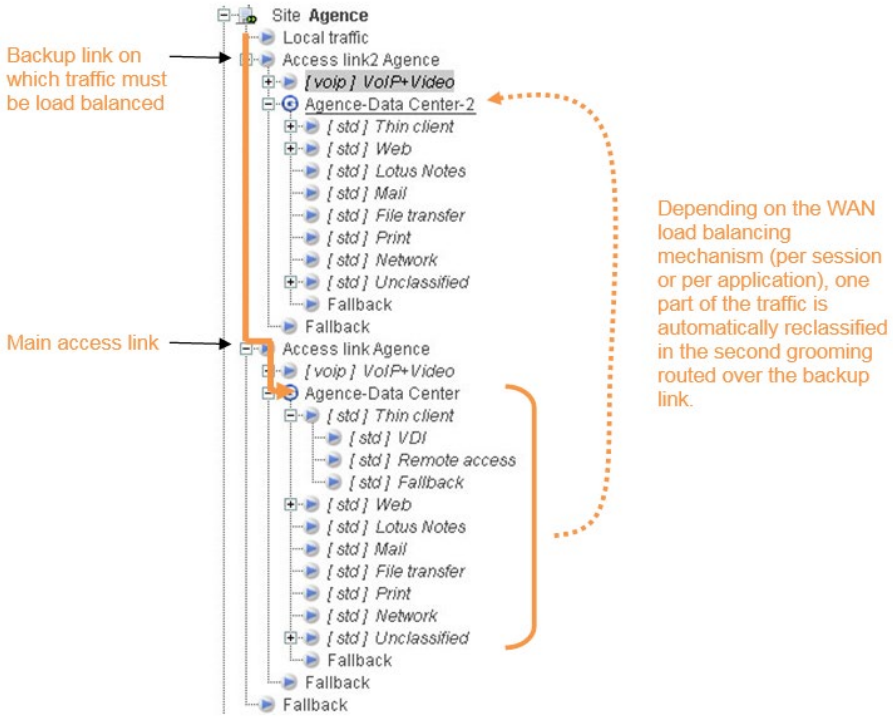
Load balancing principle

The routers should be configured in **failover mode** for the dual WAN access: without StreamGroomers, only the main access link is used, while the backup link is used only in case of failover. When load balancing is enabled on the StreamGroomers, the grooming over the main default access link will balance one part of the traffic to the grooming routed over the backup link.

Two load balancing mode are available:

- **per session:** based on a hash function (source IP, destination IP, source port, destination port, protocol), sessions are balanced equally over the two access links.
- **per application:** based on a load balancing parameter in each application rule, specific applications are offloaded over the backup link. As an example, it is possible to:
  - route bandwidth-hungry traffic on the backup link to offload the main access link

  or
  - route critical business applications on the backup link and leave all default traffic to compete on the main access link.



Access link configuration

The configuration should be the following on a site with dual access links over which Streamcore load balancing is enabled:

Access type	Redundant active/active
Backup management	Yes
Management of the 2 access links	Independent
Second WAN access link	Data throughput, frame format…
WAN access link	Data throughput, frame format…

Both access link's availability should be monitored, either by ping and SNMP polling (see chapter 7.3.5).

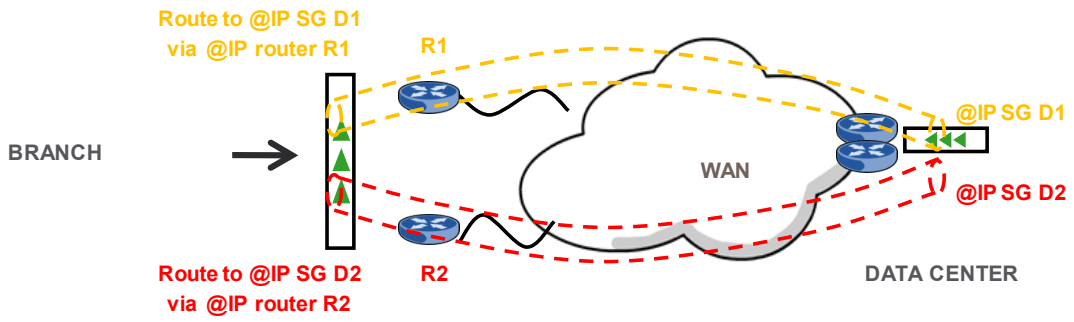
Filter configuration on the access links:

- No filters on the backup access link (load balancing will enforce classification in this rule),
- "All IP" filter on the main access link.

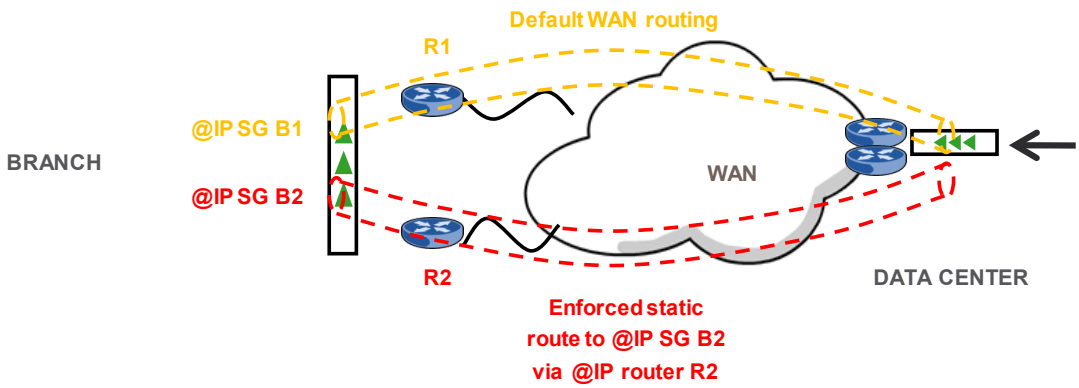
Grooming configuration

In order to enforce grooming traffic routing over each access link, specific configuration is required:

1. Before creating grooming rules, there must be a specific LAN/WAN IP address for each of the 2 grooming: right-click on **STREAMGROOMERS > xx > IP router > addresses**. Select **"Add… → Address**. Fill in the various fields, select the To LAN/To WAN interface, and then click on the **Apply** button.
2. Create the 2 grooming rules and select a different LAN/WAN source IP address for each grooming. The grooming routed over the backup link must be configured in tunnel mode (the grooming over the main access link can be in tunnel mode but it is not mandatory).
3. Enforce **outbound routing** for each grooming: in **STREAMGROOMERS > xx > IP router > routes,** modify the route towards the remote IP address of each grooming, and force the gateway to the main router or backup router individual IP address (do not use the HSRP shared IP address):



4. Enforce **inbound routing** for the grooming over the backup link if the 2 access links are connected to a common IP routing domain (typically the same MPLS network): the WAN service provider may have to define static routes in order to ensure proper routing of the tunnel.



To activate load balancing, the following operations must be performed on the 4 grooming rules:

1. Click on **SERVICES > ... > site xx > Grooming xx** in the tree menu. Select the *Parameters – Configuration* sub-tab.
2. Click on the **Modify** button, and in expert mode:
    a. Set the load balancing parameter to "Enabled".
    b. Select the associated grooming rule
    c. Select the load balancing mode between "per session" or "per application"
3. Click on the **Submit** button.

Application classification tree configuration

We recommend to configure the same rules tree under each access link and grooming. In case one of the access link fails, all traffic will be classified in the tree of the remaining access link: all application and VoIP/video rules must be present.

In case "per application" load balancing is enabled, then an additional step is required. For the applications to be load balanced, perform the following operations:

1. Open the **MANAGEMENT TOOLS** in the tree menu, click on **Rules catalog**. Select the group of rules used in both grooming rules.
2. For each application to be load balanced over the backup link, click on the **Modify** button, and set the "Load balancing with associated grooming rule" parameter to "yes"
3. Click on the **Submit** button.

Note: Backup QoS parameters can be defined in VoIP/Video and application rules, and are automatically applied in case one of the access links fails.

12.2 WEB CACHING

12.2.1 Overview

Transparent Web caching can be activated on branch offices equipped with a StreamGroomer to optimize Web application performance. When a user on a site requests a Web page or object already requested previously, the StreamGroomer automatically retrieves the data in its cache and delivers it locally without having to cross the WAN.

Unlike compression and WAN load balancing, this feature is single-sided and is therefore enabled on a per site basis.

Flexible options are available to select the traffic to optimize:

- Just specific HTTP applications
- All HTTP traffic with some exceptions
- All HTTP traffic

Note: This feature is only available on SG350e and SG850e.

This feature does not require any modifications on the Web browser since the StreamGroomer intercept the Web traffic to optimize and redirect it to the cache.

12.2.2 Parameters

To modify the Webcache parameters of a StreamGroomer, first click on **System parameters** in the StreamGroomer tree menu, and select the *Webcache parameters* tab.

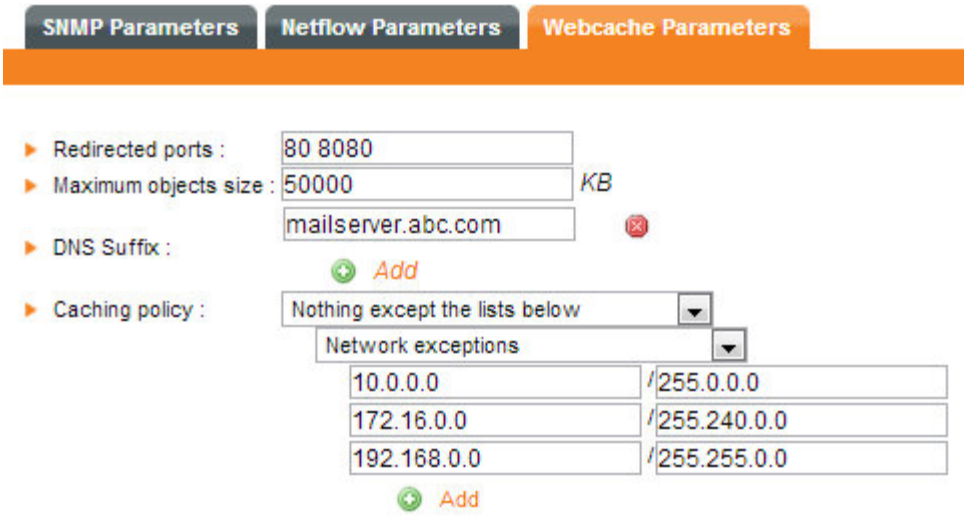


Figure 160 – Webcache parameters

Parameter	Description / Values
Redirected ports	(Default=80, 8080) TCP ports redirected transparently to the Webcache
Maximum object size	(Default= 50 MB) Maximum size of objects stored by the cache
DNS Suffix	Empty by default. Add one or more DNS suffix if required.
Caching policy	(Default=only 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) Set of policies to define what types of traffic should be cached. Two types of policies can be implemented: - Nothing except a list of subnets or FQDN - All except a list of subnets or FQDN

Note: In order to get the best possible optimization for business critical applications, we recommend selecting the policy "Nothing except a list of subnets or FQDN". The administrator can define the subnets or servers hosting the business applications.

To monitor the status of the Webcache engine, first click on the StreamGroomer on the tree menu, and select the *Real-time stats* tab:

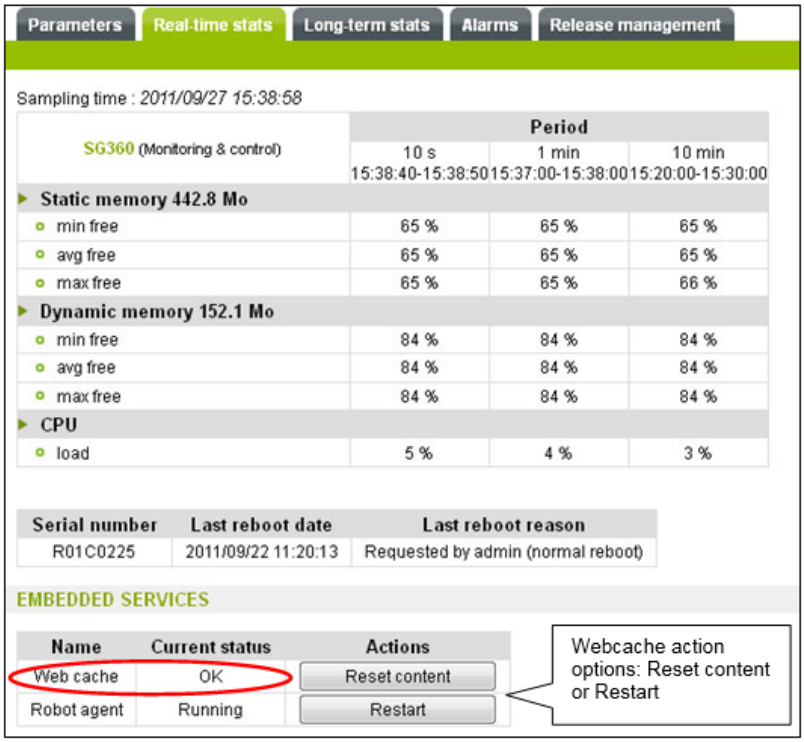


Figure 161 – Webcache service status

12.3 OPTIMIZATION STATISTICS

12.3.1 Site Statistics

191 COMPRESSION AND WEB CACHING

The *Real-time stats - Optimization* and *Long-term stats - Optimization* sub-tabs display a summary of compression and caching statistics:

	Real-time statistics	Long-term statistics
Compression throughput per access link	Compression throughput for all traffic in grooming rules below the access link	
Compression throughput per grooming	List of all grooming rules	Top 10 Grooming rules with the highest compression ratio
Compression throughput per application	N/A	Top 10 applications with the highest compression throughput
	Web caching ratio for HTTP traffic on the site	

Web caching throughput	N/A	HTTP volume sent to LAN (including cached objects)

192 WAN LOAD BALANCING

The *Real-time stats - Network* and *Long-term stats - Network* sub-tabs display data throughput /volume per access link. For long-term stats, the information is displayed in the top traffic by selecting "Up to rules of Level 1".

	Real-time statistic	Long-term statistics
Top traffic	Bandwidth allocation between the 2 access links	

12.3.2 Rule Statistics

193 COMPRESSION

On Grooming rules and application rules in the sub-tree, the *Real-Time stats - Indicators* and *Long-term stats - Indicators* sub-tabs display compression statistics for the traffic classified in the rule:

	Real-time statistic	Long-term statistics
Compression throughput	Compression throughput for all traffic in the grooming rule	
Max. uncompressed throughput	Peak throughput over 10 seconds carried on the network due to compression (observed during the period) Over 1 minute, the max. throughput is the maximum of the six 10-second samples Over 10 minutes, the max. throughput is the maximum of the sixty 10-second samples	Maximum peak throughput carried on the network due to compression, among all 10-second samples taken over the period (10 min., 30 min…).
Compression-throughput distribution	N/A	Top 10 applications with the highest compression throughput (grooming rule)

Note: A compression throughput of P% implies that the network was able to carry 1/(1-P%) additional traffic:

- 50 % - x2
- 66 % - x3
- 75 % - x4
- 80 % - x5

194 WAN LOAD BALANCING

On access link and grooming rules, the *Real-Time stats - Breakdown* and *Long-term stats – Top traffic* sub-tabs display bandwidth usage and allocation for each access link or grooming rule:

	Real-time statistic	Long-term statistics
Top traffic	Bandwidth allocation between the subrules or applications	

13 WAN Optimization Services

13.1 REPORTS VIA WAN OPTIMIZATION TAB

The Accelerator tab is not active by default however it can be activated by going to **STREAMGROOMERS > Site xx >Configuration** >**Expert mode.** Ensure that the checkbox "Activate Accelerator Expert tab" is checked.

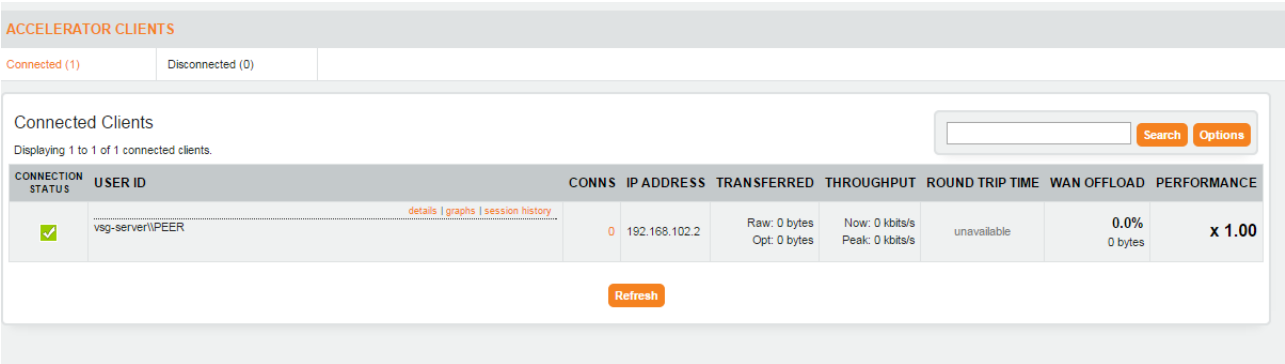
The following reports are available from the Accelerator page:

- Accelerator Clients
- Live Traffic
- Optimized Sessions
- Bandwidth Savings
- CIFS Preferences
- Cache (for viewing purposes only do not adjust cache size in this section of StreamView)

Important: The Accelerator tab should not be used to configure optimization.

13.1.1 Accelerator Clients

Accelerator Clients displays all **Active** (logged in and connected) Accelerator Clients and Peered Streamcore Accelerators. Click the **Hide** link, located at the top of the central display area, to hide all unconnected Accelerator Clients. This becomes a **Show** link; click to display *all*Accelerator Clients. The Accelerator Clients report contains the following data for each Accelerator Client associated with the SA.



13.1.2 Live Traffic

From the Reports section of the main menu, click **Live Traffic** to view the live Raw and Optimized data live. The graphical, animated display shows live traffic over a five-minute period.

The red graph displays the raw data, while the yellow graph shows the Optimized size of the same data.

Click the tabs across the top of the central display area to filter by protocol (All, HTTP, SSL, and CIFS).

There are three settings at the bottom of the screen. The following explains the function of each setting.

Units

The measurement of the amount of data being transferred. Click the Units dropdown arrow to change the units to bytes, kB, MB, kbit or Mbit.

Buffer (for sec)

This is the time interval (in seconds) over which measurements are taken. Click the Buffer dropdown arrow to change the buffer to 2, 4, 6, 8 or 10 seconds.

History (min)

This is the total length of time over which data transfer is plotted. The default is five minutes. Click the History dropdown arrow to change the display to 1, 2, 3, 4, 5, or 10 minute.

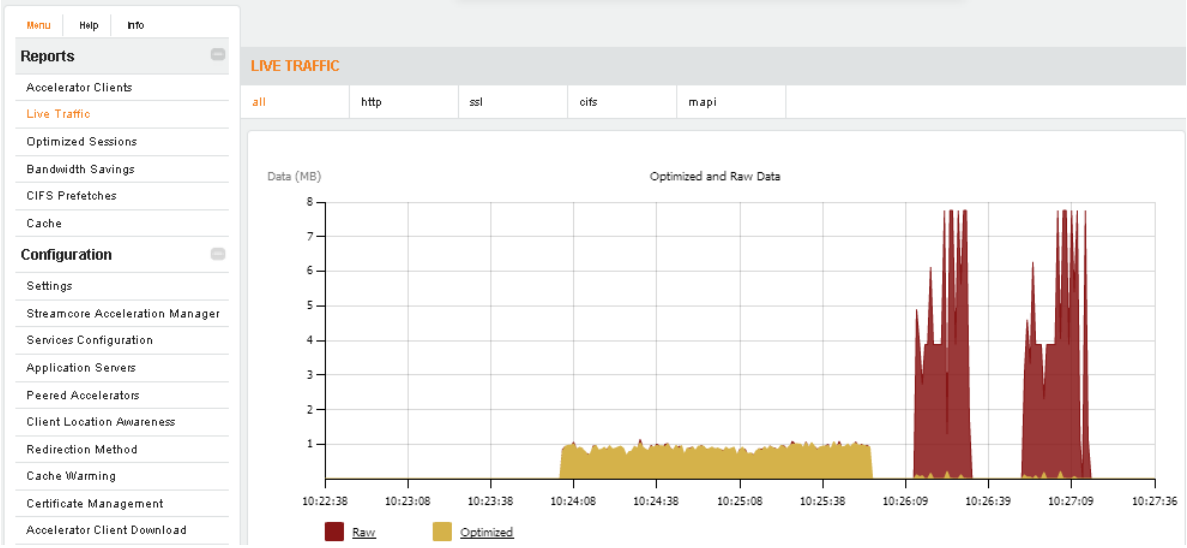


Figure 162 – Example of Live Traffic

13.1.3 Optimized Sessions

Optimized Sessions displays a table listing each Active session and the amount of data optimized.

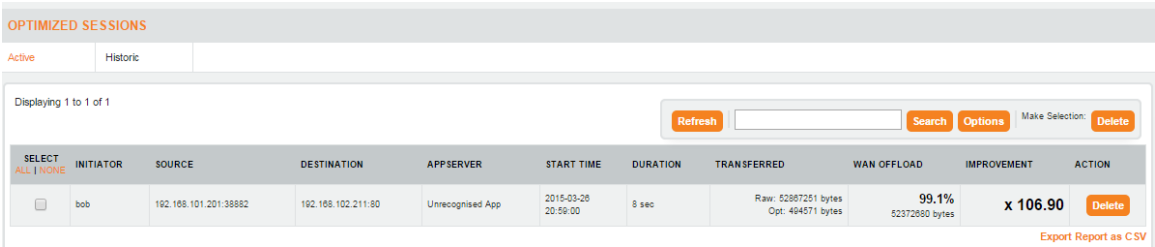


Figure 163 – Active Optimized Sessions

Click the **Historic** tab, located above the central display area, to toggle between **Active** (current) and **Historic** (old) data.

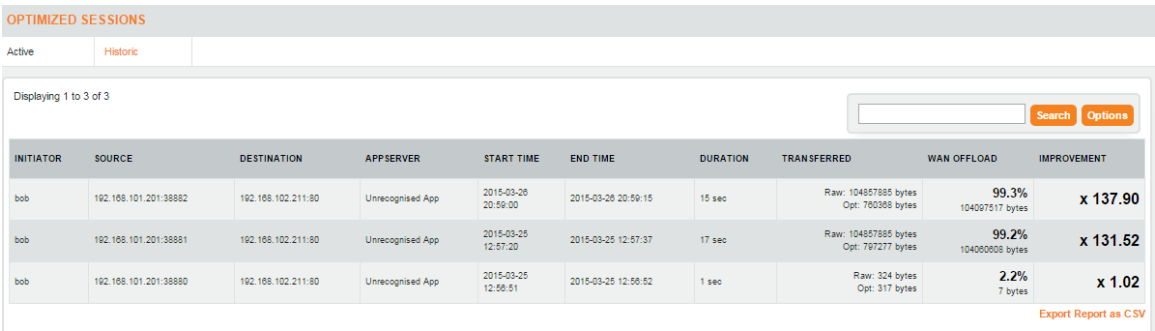


Figure 164 – Historic Optimized Sessions

The following explains the data in each column.

Initiator -This is the name of the computer that initiated the session, separated by \ from the username under which it runs.

Source - This displays the IP address from which the data originates, including its Port Number.

Destination - This displays the IP address of the computer to which the data is going.

App Server - This is the name of the Application Server that the Accelerator Client is attached to.

Start Time - This displays the time the session started.

End Time - This displays the time the session ended. It is displayed only on the Historic tab.

Duration - The length of the session (in hours, minutes or seconds).

Transferred - The amount of raw (Raw) and optimized data (Opt) that has been transferred across the WAN during the session.

WAN Offload -A percentage representing the efficiency of the WAN acceleration during the session, e.g. 78.8%. This is also displayed in size (bytes, or MB and KB).

Improvement - A performance factor statistic representing the efficiency of the WAN acceleration during the session, e.g. 4.71.

13.1.4 Bandwidth Savings

The Bandwidth Savings page displays the overall raw and optimized data for WAN Optimization. Chart representation is by data transferred by protocol (HTTP, HTTPS, and CIFS).

The following data is displayed on the page:

- **Raw Data** (displayed in red) - This is the total amount of data that would have been transferred if WAN Optimization were not activated.
- **Optimized** (displayed in yellow) – This represents the actual amount of data transferred after optimization.
- **WAN Offload** - A percentage representing the efficiency of the WAN Optimization for the SG, e.g. 78.8%.
- **Improvement** - A performance factor statistic representing the efficiency of the WAN Optimization for the SG, e.g. 4.71.

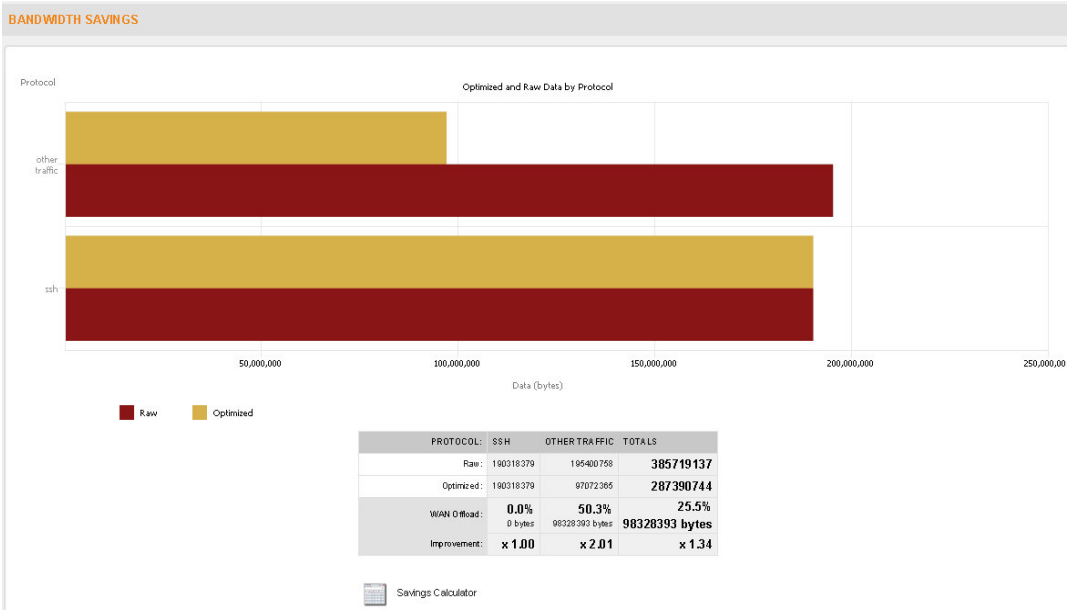


Figure 165 – Bandwidth Savings

13.1.5 CIFS Prefetches

This report shows the gain in response time for the CIFS client only. The time taken to transfer the optimized CIFS data is displayed in a bar chart, along with the time that would have been taken to transfer the non-optimized data.

The total improvement factor is displayed below the bar chart. Underneath that, the following is displayed in a table: client username; file size (in bytes); improvement factor; time taken; and timestamp for each file transferred by CIFS.

If this page displays No CIFS Prefetches have been recorded, this is possibly due to one of the following:

No CIFS traffic - perhaps there is no Windows File sharing happening. Alternatively, it may be the case that none of the configured application servers are Windows File Shares. View the Optimized Sessions and Bandwidth Savings reports to assist in ascertaining the type of traffic which is or has passed through this appliance.

Application Requests

This refers to the number of individual WAN requests the instigating application requires to complete its current task (e.g. file download).

Network Requests

The number of individual WAN requests actually made in order to handle the instigating application's requests. Click on the username to display a separate breakdown of the individual CIFS optimization data transfers for this user. Each transfer is time-stamped along with providing other pertinent information about the Client, the Destination Server, File Size, and Time Taken.

Icons are displayed at the bottom of this window to allow you to download the chart data in .png, .xml, or .csv format. Click an icon to begin downloading the data.

13.1.6 Cache

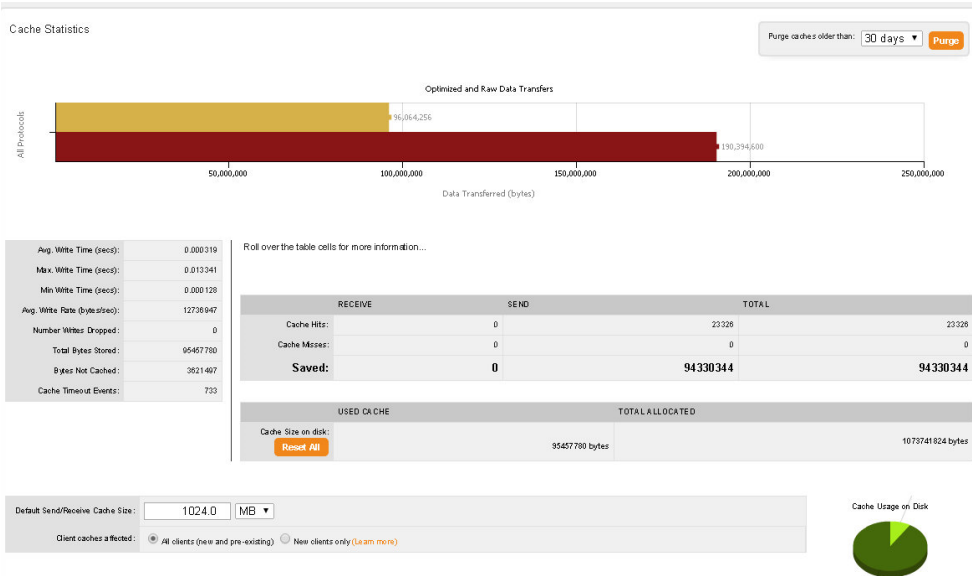


Figure 166 – Cache Summary

Cache Size

The area underneath displays (per client) **Default Initial Cache Size** (256MB). To change the value of the cache simply type a new value in and click save. It is possible to set an individual cache size or apply the change to all clients (bulk cache resize). Ensure that the VA has enough disk space to hold the content of all of the client caches. Changing the cache size while clients are being accelerated can impact the current acceleration while the cache is configured. Click the **Refresh** button, located at the bottom of the window to update the display.

A pie chart to the right displays the **Cache Disk Usage** (used and free).

How Streamcore Accelerator's Cache Technology Works

The Streamcore Accelerator's cache is a bi-directional, network-caching software module. It allows both ends of the WAN to "learn" the patterns of data that travel when it first travels between the Accelerator Client and the accelerated Application Servers.

Subsequent transfers of identical or updated data between Accelerator Clients and Application Server is sent instead as block references. The cached content is retrieved first. If the file has been amended, only the changed portion of the file is sent across the WAN, in addition to the references to the unchanged parts of the file.

Data is "learned" independently of the transmission protocol. For example, a user can download a file via FTP or HTTP, and then send the same file via email. The email will experience the benefits, where the entire file is served from the cache.

Multi-Tiered Cache

When interpreting the report, it is important to remember that each Accelerator Client or Streamcore Accelerator uses a multi-tiered cache.

The first tier is a finite, in-memory RAM Cache that is limited by the available system RAM.

The second tier is a Disk Cache which is often much larger and contains items which have been moved from the RAM cache. It is configurable, and is scaled based on available disk capacity.

The third tier is a Least Recently Used (LRU) algorithm, which rotates objects out of both the RAM Cache and the Disk Cache.

Objects rotated out of the Disk Cache are 'learned' again the next time they accessed. When an object in the Disk Cache is accessed frequently, it is promoted back to the RAM Cache. All objects stored in the RAM Cache are also stored in the Disk Cache.

The following outlines the data that appears in the Cache Report. It is based on calculations made across all Accelerator Clients that use this Streamcore Accelerator cache. The first list displays Cache Statistics.

Cache Label	Description
Avg. Write Time (secs)	The average time in seconds taken to write a cached block to the disk.
Max. Write Time (secs)	The maximum time in seconds taken to write a cached block to the disk.
Min Write Time (secs)	The minimum time in seconds taken to write a cached block to the disk.
Avg. Write throughput (byters/sec)	The average time in bytes per second taken to write a cached block to the disk.
Number Writes Dropped	The number of writes (parts of a data stream) not written to the cache. Normally, this is zero.
Total Bytes Stored	The total amount of disk space used by the cache.
Bytes Not Cached	The number of bytes that have not been cached, for example if the blocks were too small or the data was protocol-related (related data are never cached).
Cache Timeout Events	The number of times the cache times out before it writes a small block of data to the cache. This happens more frequently than Mismatches and Number Writes Dropped, and does not cause problems for Streamcore Accelerator.

14 Services Management Tools

14.1 GENERAL PARAMETERS

14.1.1 Overview

The following parameters are available on the main tab:

Parameter	Description / Values
Routing check	
Routing check	(default=Yes) When creating a grooming rule with tunneling or changing the SG mode to Monitoring + Control, the SGM will check that routing is well configured on StreamGroomers on both sites.
Options of graph display	
Graph display	(default=10) Looking at long-term statistics on sites or categories may launch long statistics consolidation processes. This parameter will deactivate the automatic display of graphs in case there are more than xx shaping/grooming rules to consolidate.
Global parameters for multishaping (see chapter 11.2.4.1)	
Multi-shaping status	(default = Up) To enable/disable the multi-shaping coordinated by the SGM
Dynamic shaping throughput update timer	(default=10 sec.) Dynamic shaping throughput refresh performed by the SGM
Dynamic shaping throughput disabling if SGM unreachable	(default= 30 sec.) Period after which the StreamGroomer will apply the nominal shaping throughput if the SGM has not refreshed it
Minimum throughput (absolute)	(default=20 kbps) Minimum shaping throughput
Minimum throughput (relative)	(default=10%) Minimum shaping throughput in% of the nominal shaping throughput
POP deployments	
Shaping based on VLAN	(default=No) By setting the parameter "Yes", VLAN associated with subnets will also be used by automated filters on Shaping rules. This option is used for StreamGroomers deployed in POP environments.
PoP deployment	By setting the parameter "to "Yes", the terminology in statistics will be adapted to this environment.

14.1.2 Alarm export

Export by email

Email recipients can be defined in the *Alarms export* tab of General parameters (to send all alarms defined on all sites), or on a specific category or site (*Parameters – Alarms sub-tab*). The following operations are available:

- **Updating a recipient:** Click on the recipient in the right-hand operating window; click on the **Modify** button, enter the modifications, and then click on the **Submit** button.
- **Adding a recipient:** Click on **+ Add** in the right-hand operating window; enter the recipient parameters, and then click on the **Submit** button.
- **Deleting a recipient:** Click on the recipient and then on the **Delete** button.

Figure 167 – Add/modify an email recipient

Note: Email sending is effective only if a SMTP gateway has been defined in SGMconf system parameters (see SGMconf user guide for more details).

Export by SNMP trap / Syslog

When selecting the *Alarm export* tab, the following export parameters are available (they are used by alarms defined in Services but also StreamGroomers alarms):

Parameter	Description / Values
Trap SNMP / Inform configuration	
Trap receiver	Add an IP address per line for each SNMP trap receiver
Trap community string	Enter SNMP trap community
Reliable trap (inform)	(default=no)
Administrative status	(default=Up)
Minimum level of alarms to be sent	Select the minimum level of alarms to be exported by SNMP trap
Syslog configuration	
Syslog servers	Add an IP address per line for each Syslog server
Facility	Select the facility to be included in the PRI field of the syslog message
Administrative status	(default=Up)
Minimum level of alarms to be sent	Select the minimum level of alarms to be exported by syslog

Files management

The *Files management* tab is useful when using the LAN inventory tools. All files saved when generating LAN inventories are stored on the SGM. They can be displayed and deleted on this page.

See chapter 9.4.5 for more information.

14.2 CATEGORIES MANAGEMENT

This tool is used to manage the different category types.

See chapter 6.2 for more information.

14.3 SITES MANAGEMENT

This tool is used to manage all sites.

See chapter 6.3.4 for more information.

14.4 MATRIX

Network rules matrix

This tool is used to manage grooming and shaping rules through and easy-to-use matrix.

See chapter 7.4.5 for more information.

Application/VoIP/Video rules matrix

This tool is used to manage groups of rules through and easy-to-use matrix.

See chapter 7.6.4 for more information.

Network alarms and SLM matrix

This tool is used to manage network groups of alarms and Network SLM through and easy-to-use matrix.

See chapter 9.2.2.5 for more information.

14.5 TIME CATALOG

QoS time-exceptions

This tool is used to manage QoS time-exceptions.

See chapter 11.5.1.2 for more information.

Reporting business hours

This tool is used to manage Reporting business hours (only for StreamReport). When generating a PDF report, the "Business hours" template can be applied to filter statistics to be considered in the report:

- When applying "Business hours", only the statistics within the defined days and time are computed.
- When applying "NON business hours", only the statistics out of the defined days and time are computed.

See "StreamReport User Guide" for more information.

To create a reference Business hours template, open the **MANAGEMENT TOOLS,** right-click on **Reporting business hours**, and then select **Add...** → **Business hours**. Enter the parameters, and click on the **Submit** button.

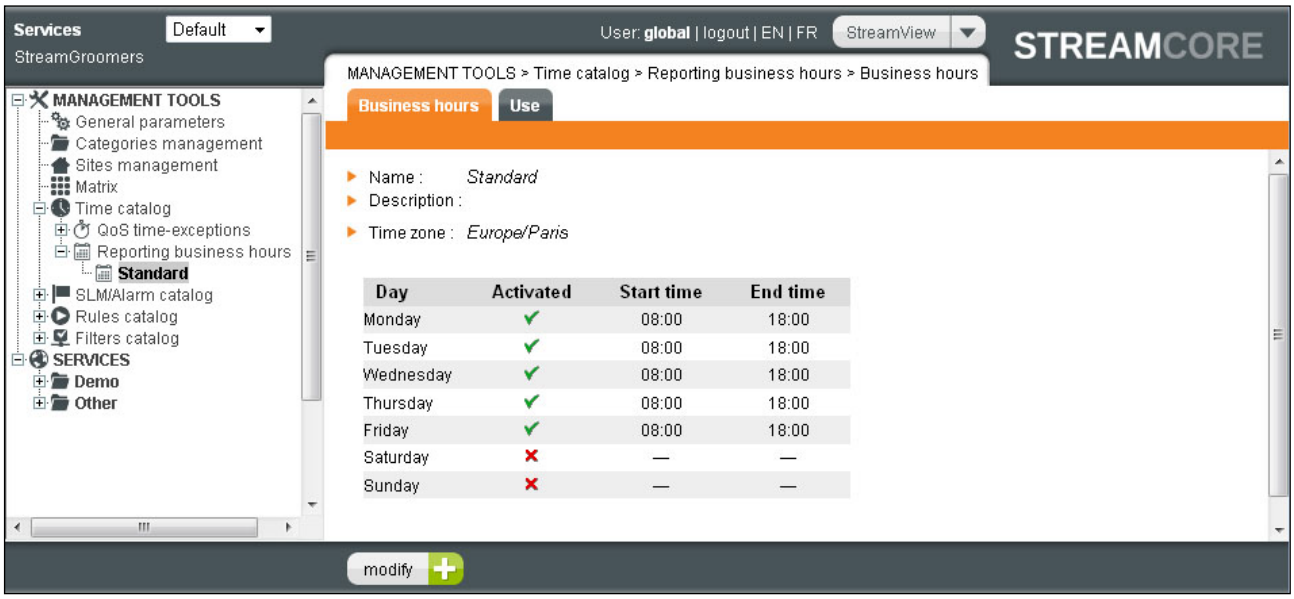


Figure 168 – Business hours template parameters

Parameter	Description / Values
Name	Name of the business hours template
Description	(optional)

Time zone	Select the timezone for reporting purpose
Days and time	Select the day and time during which StreamReport will compute or not compute statistics

To modify the name, click on it and then on the **Modify** button, enter the modifications, and then click on the **Submit** button.

To delete a business hours template, click on it and then on the **Delete** button (displayed only if the group is not used anywhere). Validate the confirmation message.

Note: The timezone for time-based QoS is different from the timezone for business hours reporting. The timezone for time-based QoS is defined on the StreamGroomer. See chapter 4.2.4.

14.6 SLM/ALARMS CATALOG

This tool is used to distribute a coherent set of alarms (network, application, VoIP/Video) on several sites.

See chapter 9.2.2.5 for more information.

14.7 RULES CATALOG

This tool is used to distribute a coherent set of application of VoIP/Video group of rules on several sites.

See chapter 7.6 for more information.

14.8 FILTERS CATALOG

This tool is used to create filter template manually or automatically from the Troubleshooting tools.

See chapter 7.5.3.3 for more information.

14.9 WAN OPTIMIZATION

This tool is used to help accelerated and optimize applications over a WAN. This tool comes with a default WAN Optimization profile but also offers the possibility of customizing protocols.

15 Appendix

15.1 CHANGING SGM-SG COMMUNICATION TO SSH

The SGM-SG communication can use two different protocols:

- RSH (default)
- SSH for secured communications (blowfish 128 bit-mode CBC encryption)

In order to change the administration protocol from RSH to SSH, 2048 bits RSA public keys must be exchanged between the SGM and the SG in order to ensure bidirectional authentication. Two methods are available:

- In-band key exchange for "SSH communication with weak authentication"
- Out-of-band key exchange for "SSH communication with strong authentication"

SSH with weak authentication

When a StreamGroomer has been deployed and can be accessed by the SGM with the default RSH administration protocol, it is possible to exchange RSA public keys through the network.

The process is entirely automated: click on **STREAMGROOMERS > xx** in the tree menu, on the *Parameters-Configuration* sub-tab, then on the **Modify** button. Select the "SSH – secured with weak authentication" mode, and then click on the **Submit** button.

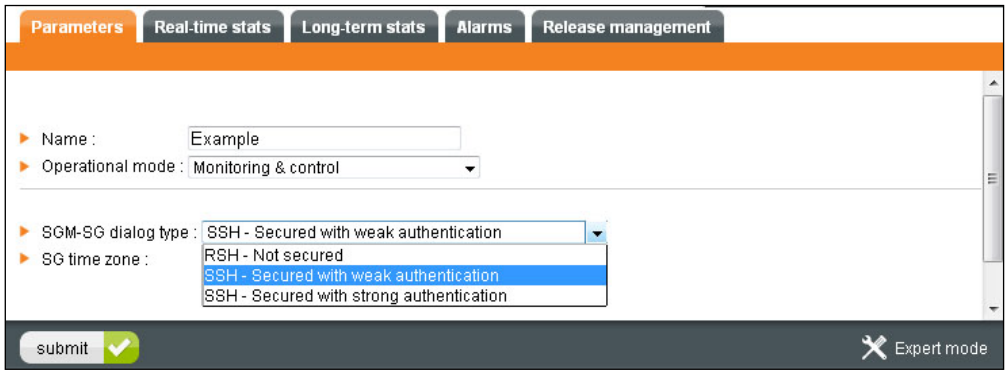


Figure 169 – Changing SGM-SG administration protocol

Click on *Real-time stats* tab to check that the operation has been successful:

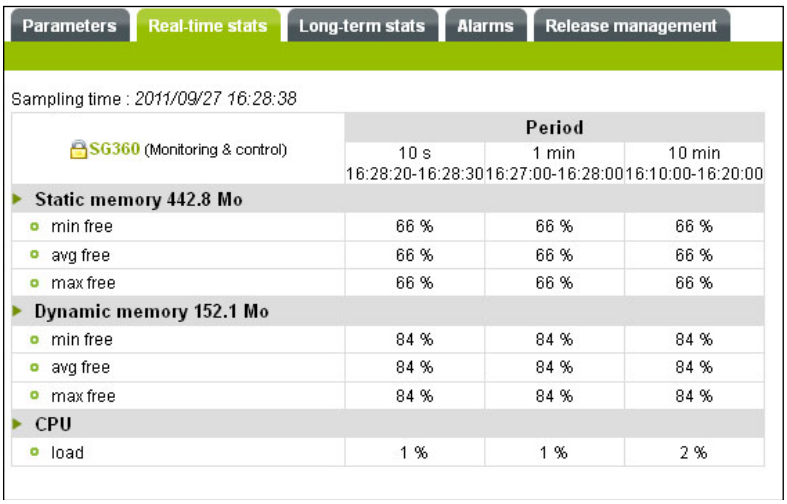
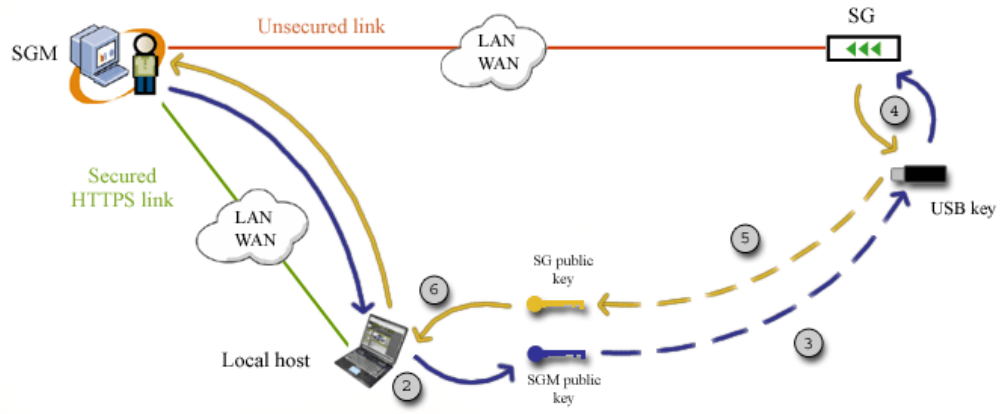


Figure 170 – Checking SSH administration

SSH with strong authentication

In order to ensure the strongest possible authentication, RSA public keys can be exchanged out-of-band. This process can be performed on a deployed StreamGroomer or on a to-be-deployed StreamGroomer when configuring its boot IP parameters:



1. Click on **STREAMGROOMERS > xx** in the tree menu, on the *Parameters-Configuration* sub-tab, then on the **Modify** button. Select the "SSH – secured with strong authentication" mode, and then click on the **Submit** button.
2. Download the boot file.
3. Transfer the boot file on an USB-key.
4. Plug the USB key on the SG and reboot the SG. The SG will transfer a "status" file on a USB key at the end of its reboot, containing its public key.
5. Transfer the SG status file from the USB key to the local host.
6. Click on **STREAMGROOMERS > xx** in the tree menu, on the *Parameters-Configuration* sub-tab, then on the **Import** button. Browse to select the StreamGroomer status file and click on the **Submit** button.

Note: Changing the SGM-SG administration from SSH to RSH on the SGM will delete the stored StreamGroomer public key on the SGM. In order to change the communication to RSH on the StreamGroomer, it is necessary to install the new boot file with a USB key

15.2 GROOMING TUNNELING IN COMPLEX ENVIRONMENTS

802.1Q trunk

When a StreamGroomer is deployed over a 802.1Q VLAN trunk and tunneling is used in grooming rules, a per-VLAN Routing parameter, which is accessible by clicking on **STREAMGROOMERS > xx > IP router**, makes it possible to tell whether the StreamGroomer LAN / WAN interface routing table handles VLANs:

If VLAN routing is deactivated (the default value), **routing occurs globally**. When the StreamGroomer de-encapsulates a tunneled frame sent from the WAN, it can use all of the routes in the routing table (that are associated with the LAN / WAN interface).

Note: Deactivation of VLAN routing is recommended when inter-VLAN communication is authorized at the site. Example: StreamGroomer is positioned in front of an agency router that is performing inter-VLAN routing.

In order for a remote site, whose traffic is managed under Grooming with a tunnel, to be able to reach all of the VLANs, one single Grooming rule is sufficient. However, a LAN / WAN address must be defined in each VLAN ("Expert mode" when an IP address is added), so that all of the directly connected subnetworks will be accessible.

- If VLAN routing is activated, **routing occurs within a VLAN** (there is one "VRF" per VLAN). When the StreamGroomer de-encapsulates a tunneled frame received from the WAN, it can use only the routes in

the routing table that are in the same VLAN as the tunnel that the frame came from (e.g. the VLAN of the IP address of the tunnel extremity). Thus, the VLAN parameter — accessible under "Expert mode" when an IP address or a route is added — allows a unique routing table to be defined for each VLAN.

Note: Activation of VLAN routing is recommended when inter-VLAN communication is prohibited at the site. Example: Environment in which a different default route must be defined for each VLAN

In order for a remote site, whose traffic is managed under Grooming with a tunnel, to be able to reach all of the VLANs, one Grooming rule is necessary for each VLAN. To classify the traffic sent towards the WAN in the correct grooming rules, VLANs can be used as filter criteria ("Expert mode" for a filter), in particular when identical destination subnetworks can be reached from each VLAN.

IPSec VPNs

When tunnel is activated, traffic is encapsulated between the two StreamGroomers and IP routing is implemented in the StreamGroomer. Therefore, various precautions must be taken to ensure full transparency, especially when the MTU is not standard.

StreamGroomers are able to auto-discover the end-to-end MTU by detecting fragmented packets (for instance for a Grooming over a GRE tunnel, over PPoE or over IPinIP). The auto-discovered MTU can be checked in the Expert mode of a grooming rule "Real-time stats":

Figure 171 – Auto-discovered MTU

The StreamGroomers use the auto-discovered MTU value to apply an automated fragmentation / re-assembly mechanism in order to ensure full transparency to traffic exchanged between the two StreamGroomers.

Note: In some IPSec environment, traffic is fragmented and reassembled between the StreamGroomers: they are therefore not able to detect that fragmentation occurred in that case. Therefore, when the "IPSEC encapsulation performed by WAN router" is set to yes on a site, then the MTU parameter is forced to a maximum of 1300 bytes. This value can be changed in the "Expert mode" of a Grooming rule's parameters.

15.3 LIST OF PREDEFINED SERVICES IN FILTERS

Note: the list of application automatically discovered by the troubleshooting tools (Traffic discovery, TopN, Live sessions) is much more detailed (around 300 applications).

	Protocol
IP	-
TCP	6
UDP	17
UDP+TCP	6, 17
ICMP	1 (IPv4) 58 (IPv6)
IGMP	2

IPSec	50, 51
IPcomp	108
IPv6 tunnel	41
EIGRP	88
OSPF	89
PIM	103
GRE	47
SCTP	132
RSVP	46
Other protocol over IP	-

	TCP port	UDP port	With pattern matching
AOL-ICQ	5190-5193	5190-5193	
ADOBE-FLASH-RTMP	1935	1935	
APPLE-FP	548		
APPLE-ICHAT	5298	5297, 5298, 5353,5678, 16384-16403	
BGP	179		
BIFF		512	
CC-MAIL	3264	3264	
CDP	4224		
CHARGEN	19	19	
CITRIX-BROWING-ICA	1604	1604	
CITRIX-ICA	1494		
CITRIX-ICA-CGP	2598		
CITRIX-IMA	2512		
CUSEEME	7640, 7642, 7648, 7649	7640, 7642, 7648, 7649	
DAYTIME	13	13	
DHCP/BOOTP		67, 68	
DLSRPN	2065		
DLSWPN	2067		
DNS	53	53	
ECHO	7	7	
FINGER	79		
FTP	20,21		X
FTP-CTRL	21		X
FTP-DATA	20		
GROOMING-LMP		49152	
H323	1718, 1719, 1720, 1731	1718, 1719,1720, 1731	

HSRP	1985	1985	
HTTP	80		X
HTTP-PROXY	8080		X
HTTPS	443		
IDENT	113		
IBM-DB2	523		
IMAP	143		
IMAP-S	993		
INFORMIX-SERVER	3800		
IPP	631		
IPSec NAT-T		4500	
IRC	194, 6665, 6667	194, 6665, 6667	
IRC-S	994	994	
ISAKMP		500	
JABBER	5220, 5222, 5223, 5269		
KERBEROS	88	88	
KERBEROS-SERVICES	543, 544, 1109, 2105	543, 544, 1109, 2105	
L2TP	1701	1701	
LDAP	389, 3268, 3269	389	
LDAP-SSL	636		
LOTUS-NOTES	1352	1352	
LOTUS-SAMETIME	1516, 1533		
MGCP	2427, 2727, 2428	2427, 2727, 2428	
MS-CIFS	445		
MS-NETBIOS	137, 138, 139	137, 138, 139	
MS-PSOM	8057		
MS-RPC	135		
MS-SQL-SERVER	1433	1434	
MS-STREAMING	1755	1755	
MS-RDP	3389		
MSN-MESSENGER	1863, 6891-6901	6901	
MS-MQ	1801, 2101, 2103		
MYSQL	3306		
NFS	2049	2049	
NNTP	119		
NNTP-S	563		
NOVELL-GROUPWISE-POA	1677, 7101, 7181	1677	
NOVELL-GROUPWISE-MTA	7100, 7180		
NOVELL-GROUPWISE-GWIA	7102, 9850		
NOVELL-GROUPWISE-WEBACCESS	7205, 7211		

NOVELL-NCP	524		
NTP	123	123	
ORACLE	1521, 1526, 1575, 1630, 1748, 1754, 1808, 1809, 1810, 1830, 1831, 1850, 2481, 2482	1521, 1526, 1575, 1630, 1748, 1754, 1808, 1809, 1810, 1830, 1831, 1850, 2481, 2482	
PC-ANYWHERE	5631, 65301	5632	
PDL-DATASTREAM	9100	9100	
PGSQL	5432	5432	
POP3	110		
POP3-S	995	995	
PPTP	1723	1723	
PRINTER	515		
RADIUS		1812, 1813	
RIP		520	
RADMIN	4899		
RLOGIN	513		
RSH	514		
RSYNC	873		
RTP+RTCP			X
RTSP	554	554, 5004, 5005	
SAP-COMMUNICATIONS	3200, 3300, 3600		
SAP-ROUTER	3299		
SCCP	2000, 2443	2000	
SIEBEL	2320, 2321, 8448		
SIP	5060	5060	
SIP-TLS	5061		
SLP	427	427	
SMTP	25		
SMTP-S	465		
SNMP	161, 162	161, 162	
SOAP	7627	7627	
SOCKS	1080		
SSH	22	22	
SSL-SHELL	614		
SUN-RPC	111	111	
SYBASE	1498, 2439, 2638, 3968	1498, 2439, 2638, 3968	
SYSLOG		514	
T120	1503		
TACACS	49, 65	49	
TELNET	23		

TELNET-S	992		
TFTP		69	
TIMBUKTU	407, 1417-1420		
TRACEROUTE		33434	
VMWARE-PCOIP	4172	4172	
VNC	5800-5809, 5900-5909		
WHOIS	43		
WINS	42, 1512	42, 1512	
XOT	1998		
X-WINDOW	6000		
YAHOO-MESSENGER	1614, 5001, 5050, 5100,5150	5001	

15.4 TRAFFIC CAPTURE OPTIONS AND FILTERS

The following information relates to the "options" and "filter" feature for Traffic Capture.

15.4.1 Options

Option	Description
-e	Print the link-level header on each dump line.
-S	Print absolute, rather than relative, TCP sequence numbers.
-T	Force packets selected by "expression" to be interpreted the specified type. Currently known types are: • **aodv** (Ad-hoc On-demand Distance Vector protocol) • **cnfp** (Cisco NetFlow protocol) • **rpc** (Remote Procedure Call) • **rtp** (Real-Time Applications protocol) • **rtcp** (Real-Time Applications control protocol) • **snmp** (Simple Network Management Protocol) • **tftp** (Trivial File Transfer Protocol) • **vat** (Visual Audio Tool) • **wb** (distributed White Board)
-ttt	Print a delta (in micro-seconds) between current and previous line on each dump line.
-v	(Slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.
-vv	Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded.
-vvv	Even more verbose output. For example, telnet **SB ... SE** options are printed in full. With **-X** telnet options are printed in hex as well.
-X	When printing hex, print ascii too. Thus if **-x** is also set, the packet is printed in hex/ascii. This is very handy for analyzing new protocols. Even if **-x** is not also set, some parts of some packets may be printed in hex/ascii.

15.4.2 Filters

Selects which packets will be dumped. If no expression is given, all packets on the net will be dumped. Otherwise, only packets for which expression is `true' will be dumped. The expression consists of one or more primitives. Primitives usually consist of an id (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

Qualifier	Description
type	These qualifiers specify what kind of entity the id name or number refers to. Possible types are host, net and port. E.g., "host foo", "net 128.3", "port 20". If there is no type qualifier, host is assumed.
dir	These qualifiers specify a particular transfer direction to and/or from id. Possible directions are src, dst, src or dst and src and dst. E.g., "src foo", "dst net 128.3", "src or dst port ftp-data". If there is no dir qualifier, src or dst is assumed. For "null" link layers (i.e. point to point protocols such as slip) the inbound and outbound qualifiers can be used to specify a desired direction.
proto	These qualifiers restrict the match to a particular protocol. Possible protos are: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp and udp. For example, "ether src foo",

	"arp net 128.3", "tcp port 21". If there is no proto qualifier, all protocols consistent with the type are assumed. For example, "src foo" means "(ip or arp or rarp) src foo" (except the latter is not legal syntax), "net bar" means "(ip or arp or rarp) net bar" and "port 53" means "(tcp or udp) port 53". "fddi" is actually an alias for "ether"; the parser treats them identically as meaning "the data link level used on the specified network interface." FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression. Similarly, "tr" is an alias for "ether"; the previous paragraph's statements about FDDI headers also apply to Token Ring headers.

15.5 WAN OPTIMIZATION – USER ACTIONS, EFFECTS ON THE TRAFFIC AND USER EXPERIENCE

The following tables outline some common scenarios with reference to user actions and the effects that they might cause on traffic and user experience.

15.5.1 Scenario 1:

Two sites are WAN optimized. Initial state:

- WAN optimization is configured and running between 2 equipped sites (peering).
- Both SG are in **Monitoring + Tagging + Control** mode.
- Some TCP Sessions are currently being accelerated when the action is executed by the user.

User action	Impact on traffic	user experience
Change the WAN optimization settings: application servers, WAN optimization profiles, valid SSL certificates added/removed to/from the SGM	- TCP Sessions opened and accelerated before the transition occurs are maintained and keep being optimized until they end up. Keep in mind that TCP sessions can last several days! - New TCP sessions are optimized according to the new configuration.	User experience will be improved or affected according to the new WAN optimization settings
Delete the existing peering between the 2 sites	- TCP Sessions opened and accelerated before the transition occurs are maintained and keep being optimized until they end up. Keep in mind that TCP sessions can last several days! - New TCP sessions are not optimized. It is recommended to plan a maintenance window to set the SG in bypass mode and warn end-users.	User experience will be affected for all the end-users accessing application servers on both sites.
Change SG mode from Monitoring + Tagging + Control → Monitoring + Tagging Change SG mode from Monitoring + Tagging + Control → Monitoring	- TCP Sessions already opened and accelerated before the transition occurs are maintained and keep being optimized until they end up. Keep in mind that TCP sessions can last several days! - New TCP sessions opened after the transition are not accelerated. - QoS is deactivated no matter TCP sessions are accelerated or not.	User experience can be affected for all the end-users (since both QoS and WAN optimization services are disabled).
Change the SG mode from Monitoring + Tagging + Control → Bypass	- All accelerated TCP sessions are interrupted. It is recommended to plan a maintenance window to set the SG in bypass mode and warn end-users.	User experience can be affected for all the end-users.
Install an OPE on one of the SG	- No impact on the traffic between both sites	User experience is not affected by this action.
Reboot one of the SG or both SG (OPE or Boot)	- All accelerated TCP sessions are interrupted. It is recommended to plan a maintenance window to reboot the SG and warn end-users.	User experience can be affected for all the end-users.

15.5.2 Scenario 2:

Two sites are WAN optimized. Initial state:

- WAN optimization is not active: no peering between the sites.
- SG mode is **Monitoring + Tagging + Control**.

User action	Impact on traffic and user experience	
Change the WAN optimization settings: application servers, WAN optimization profiles, valid SSL certificates added/removed to/from the SGM	- No impact on the traffic	User experience is not affected by this action.
Create the peering between the 2 sites	- New TCP sessions that match the WAN optimization settings are optimized. - TCP Sessions already opened before the transition occurs are maintained and not optimized until they end up.	User experience will be improved for end-users accessing application servers on both sites according to the new WAN optimization settings.

15.5.3 Scenario 3:

Two sites are optimized. Initial state:

- SG mode is **Monitoring + Tagging + Control** for both sites.
- A peering has been created between the sites.

User action	Impact on traffic	user experience
Change the WAN optimization settings : application servers, WAN optimization profiles, valid SSL certificates added/removed to/from the SGM		User experience can be improved or affected by this action according to the new WAN optimization settings.
Create a peering between one of the 2 sites and a 3rd site	- No impact on the traffic between initial sites	User experience is not affected by this action for both initial sites. The user experience on the 3rd site will be improved when accessing application servers according to the new WAN optimization settings.