streamcore

23a Release notes

Author : Nicolas ROQUES

Table of contents

Copyright

1 Software suite 23a

The Streamcore software suite is a set of software releases for StreamGroomers and the SGM. This document contains the release notes for the Streamcore 23a software suite.

The software suite must be installed on the SGM with the SGMConf application.

The OPE and BOOT elements must be deployed on the StreamGroomers from the SGM with the StreamView application. **Since version 6.3, when an OPE is installed on a StreamGroomer, the SGM automatically deploys the latest versions of the BOOT and ACC modules. The BOOT version will only be active after the StreamGroomer has been restarted (cf. 2.3 Activation of a Boot, ACC and OPE version below)**

This software suite contains the following SGM and StreamGroomers software versions:

Software suite: 23a
Official OPE: 6-4.25
Official OPE: 6-5.18
Official OPE: 6-5.18qhp
Official ACC M4G64 : ACC26
Official ACC M5G : ACC34
Official M4G64 Boot: S56
Official M5G boot: T11

The **6-5.18qhp** version implements the parallelization of the QoS on 2 cores separated from the monitoring core. It has all the functions of the 6-5.18

Version **6-6** (parallelization of QoS on 2 cores and monitoring on all remaining cores) is available on request from support. Functional restrictions apply

2 IMPORTANT RECOMMENDATIONS

Before deploying this version of the software, please read the following recommendations carefully and contact Streamcore support if you have any questions.

2.1 LICENSES

Since version 6- 5.T 06, the Streamcore software suite installs a new license management system that requires an update of the license currently used on the SGM.

If you have already used an SGM in 6- 5.T 06, you do not need to update the license.

2.2 NEW PASSWORD

Starting with version 6- 5.T 06, the default passwords for users sgm and ***sc*** are set to different values.

Please contact Streamcore support at support@streamcore.com to receive these new passwords.

From this version 23a, any modification of the password of the **cli** account implies a modification of the passwords of the **sc** and **sgm** accounts which will be identical to the password of the **cli** account.

Only the password of the **sc** account of StreamGroomer probes remains standard. This account is only accessible when connected to the probe via SSH from an authorized SGM.

2.3 ACTIVATION OF A BOOT, ACC AND OPE VERSION

The activation of a new version of the OPE/ACC requires a restart of the StreamGroomer. During the restart phase, the StreamGroomer is inaccessible. Restarting the StreamGroomer automatically stops the following functions at the corresponding sites:

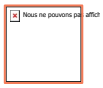
- Monitoring: No measurements (polling) are made during the restart and probably no statistics will be available for the corresponding 1 minute or 10 minute period in the real-time and long-term graphs and reports. The grooming stops working and its status is set to *DOWN,* unless the grooming has been configured to be temporarily managed as a shaping.
- QoS and marking: Traffic will not be prioritized or marked until the StreamGroomer has reloaded and activated its configuration.
- Load balancing: Load balancing is disabled on the site supported by the StreamGroomer.
- WAN optimization: Accelerated TCP sessions will be interrupted.
- Netflow and monitoring: The StreamGroomers will stop sending Netflow tickets and traps/informs until it has reloaded and applied its configuration.

It is strongly recommended to plan and schedule appliance restarts to minimize the impact on network flows and end-user activities.

It is recommended to activate the same versions of Boot, OPE and ACC on the StreamGroomers of a dual and tandem configuration.

If WAN optimization, Grooming, QoS and tagging or Load Balancing features are used, it is strongly recommended to run the same versions of Boot, OPE and ACC software on both ends of a grooming or peering to avoid errors caused by inconsistency between StreamGroomers.

2.4 SOFTWARE VERSIONS FOR M3G NOT AVAILABLE



The boot and OPE packages for M3G appliances are removed from the Streamcore 6-4.12 software suite, as M3G appliances are in EOL.
OPE version 6.1 is also removed from the Streamcore software suite, as this version is also in EOL.

2.5 ACC UPDATE

- The installation of the ACC34 will erase the cache already used on the SG.
- The ACC34 can work with other SGs in ACC26 or higher (for future versions, please see the corresponding release note).

2.6 UPGRADE BOOT M4G64 S49 OR LATER

A critical issue has been identified with boot versions up to S42 on SG360e, SG860e, SG1660e and SG3260e that impacts communication with StreamGroomers and many other operations such as configuration, measurement and statistics collection, WAN optimization.
If the operating time of these StreamGroomers is longer than 200 days, the device may become inaccessible after a software reboot (e.g. when activating an OPE version). The workaround is a hardware reboot (unplug and plug in the power supply). To solve this problem, deploy the Boot S49 on these appliances and apply the new version as soon as possible by restarting the StreamGroomer.
Streamcore strongly recommends that all StreamGroomers be upgraded to an S49 or later boot version as soon as possible.

3 End of support for software suites

Please note the end of support dates for Streamcore software suites and operational software releases (OPEs):

You can refer to the End of Life Policy (EOL POLICY DOC Version 202208_v06) for a comprehensive view of the end of life (EOL) dates for Streamcore equipment and software.

Software suites	End of the assistance
6-4	31 December 2024
6-5	No planned

OPE	End of assistance
6.2 high performance	30/06/2023
6.3	**End of support since 01/04/2019**
6.4	31/12/2024
6.5	No planned

- It is strongly recommended that the SGM, StreamGroomers, and StreamCollectors be updated to the latest versions of the Streamcore software suite, OPE, and Boot.

Please feel free to contact the Streamcore support team (support@streamcore.com) or your sales representative for more details on the upgrade path.

4 New Software Suite 23a features

As with every release now, minor and major changes are incorporated that can be grouped into the following categories:

- New interfaces:
  - SuperView,
  - SCXcenter
- Netflow evolutions
  - Netflow license integrated in the rule count
  - Netflow encryption
  - Automatic activation of Netflow export on Fallback rules
- SGM developments
  - Connexions: new columns
  - Chattiness indicators
  - Top on SNI and TLS
  - Switching to UTF8
  - SGM status: CPU type display
  - Passwords sc account
- SG developments
  - Breakout on Port Wan
  - Port inversion parameter
  - Display of raw statistics
  - Additional parameters SG
  - Passwords sc account
  - Display of max CPU
  - qhp version
- Accelerating developments
  - Default block size
  - DIAS circuit breaker

4.1 NEW INTERFACES

As part of its interface redesign program, 2 new modules appear with version 23a:

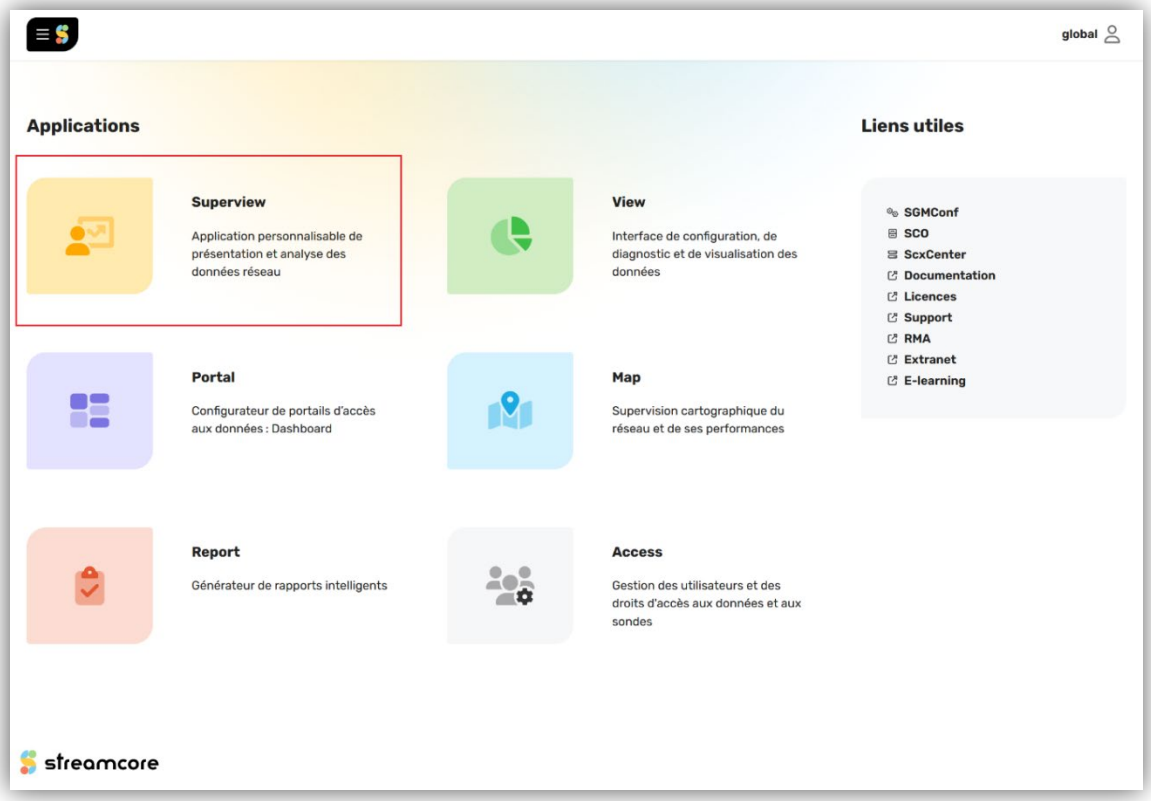
4.1.1 Superview

The 23a software suite introduces a new interface for displaying statistics stored on the SGM.

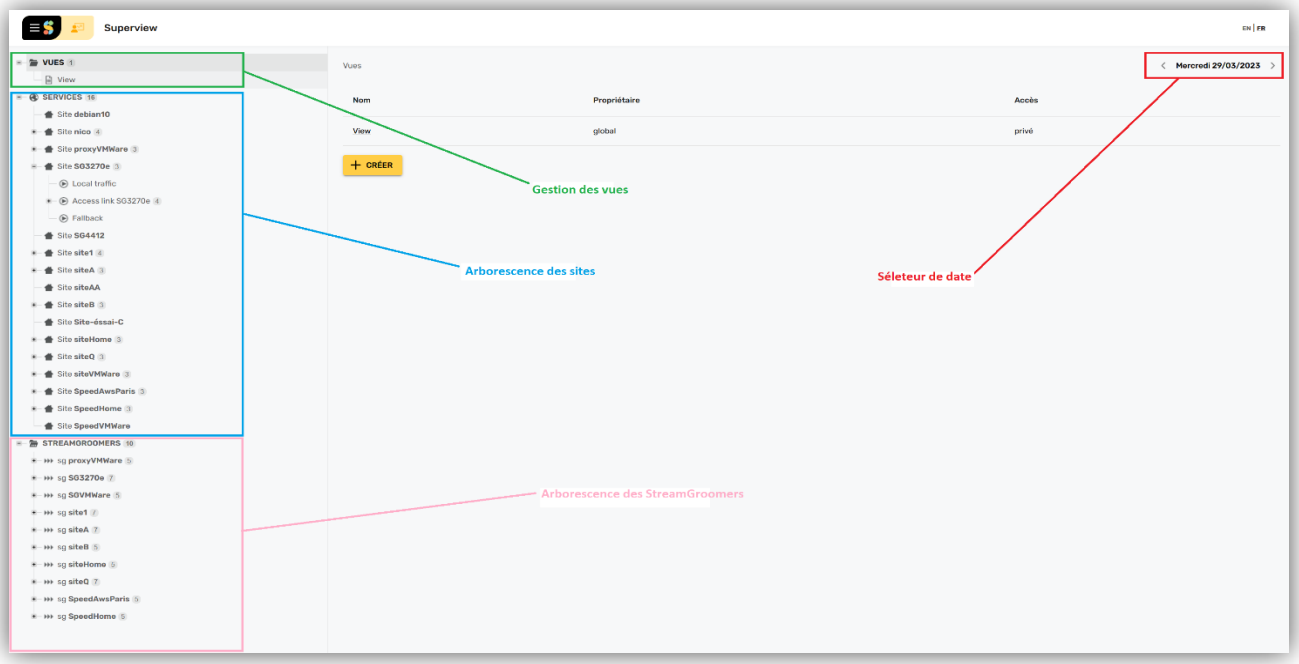
This is the **Superview** interface which is accessible from the home page.

The objective of SuperView is to federate the various tools for presenting long-term data (over 10 minutes) present in the solution with the following characteristics

- Customizable interface
  - The user can choose the items to be displayed and their location on the screen
  - Ability to display data from multiple objects simultaneously
- Publishable interface
  - The user can decide to publish for other users an interface that he has designed
  - Changes to this interface will be updated for "subscriber" users
- Simplified and intuitive ergonomics
  - Responsive interface
  - Interface adapted to touch screens or usable with a mouse
  - Concept of views, sections and widgets to structure pages



Opening this interface displays a new window for the presentation of graphs:



A special technical document presents this interface. Please refer to this document for the use of this interface.
202304_SuperView_v01

4.1.2 SCXCenter

StreamGroomer probes can be configured to provide hosting space for other applications (other VMs) than Streamcore applications.

The probes then become SCXs and are managed locally or remotely from an interactive SCXManager interface. The local interface allows you to configure an SGM in one of the probe's VMs.

The SGM also embeds in its software suite the code of the centralized management of SCX probes: SCXCenter.

The probes and VMs are managed via SCXCenter. If one of the VMs contains a SG, it will be managed as a physical SG via StreamView within the base to which it is paired.

4.1.2.1 PREREQUISITES

- An SGM in SoftwareSuite 23a
- An SCXOne preconfigured by Streamcore
- An SSL (HTTPS) access to the SGM configured

4.1.2.2 GO TO SCXCENTER

- Go to SGM Home, login
- Click on "ScxCenter" in the external links in the right pane
- Login using the password provided in the JSON as a sha256 hash (see below; default: streamcore)

4.1.2.3 CHANGE THE DEFAULT PASSWORD

- Connect as SSH, as root on the SGM
- Do the following command: ***echo -n "streamcore" | sha256sum -z - | head -c 64 | sha256sum*** - taking care to replace *streamcore* by the new password chosen
- Modify the file ***/opt/scx-center-agent/scx-config.json*** and change the parameter ***settings.authorization_token*** with the return of the above command

4.1.2.4 PAIRING A SCXONE

- Once connected, click on "Add", a pop-up will appear
- Fill in :
  - The name of the scxOne (must be identical to its real hostname for a "SG caller mode" pairing)
  - A description
  - SCX-calling mode or not
    it is recommended to leave it activated by default except in specific cases.
- Once validated, a password will be indicated and the pairing will be pending from the scxOne
- Go to console, boot user on the scxOne
- Perform a "classic" pairing by specifying the SGM IP

4.1.2.5 ACCESS TO SCXONE

- Once paired, the scxOne will be listed on the interface
- Click on it to access its services (SG, SGM, virtual machines) and its network configuration
- Once a scxOne and a service are selected, it is possible to access the virtual console of this service
  - Allows the configuration of a virtual SG through its boot menu for example
- Notes:
  - The scxOne can be deleted by returning to the main screen and clicking on the corresponding delete button

- The navigation is done by clicking on the names of the entities. The backtracking is done by the breadcrumb trail below the top bar.

4.2 NETFLOW EVOLUTIONS

The Netflow feature of the Streamcore solution is the ability to historize detailed sessions beyond the real-time mode of the interface.

In real time mode, the Current Connection tab displays the details of the sessions passing through each rule with detailed information (throughput, source and destination IP, response time, etc).

After a few minutes, this detail is deleted and only the consolidated indicators for the rules are kept. It is sometimes interesting to keep for some rules the detail of the sessions in addition to the consolidated indicators. A session logging function has been implemented and is based on the Netflow V10/IPfix protocol for the format and sending of session tickets.

This logging feature has existed for several years at Streamcore and required a dedicated storage server (SCO). Since version T12, it was possible to historize detailed sessions on the SGM by activating a specific license for the historized rules.

4.2.1 Netflow license

To facilitate the management of the session logging option via Netflow, the license management is modified.

The Netflow export is counted against the global number of rules license.

The application of a netflow export on a rule is no longer subject to a specific license request but will count as an additional rule.

A rule with netflow export counts double on the number of rules provided by the license.

This evolution allows for a more granular use of the Netflow feature and allows you to reuse unused rules from your license to log sessions.

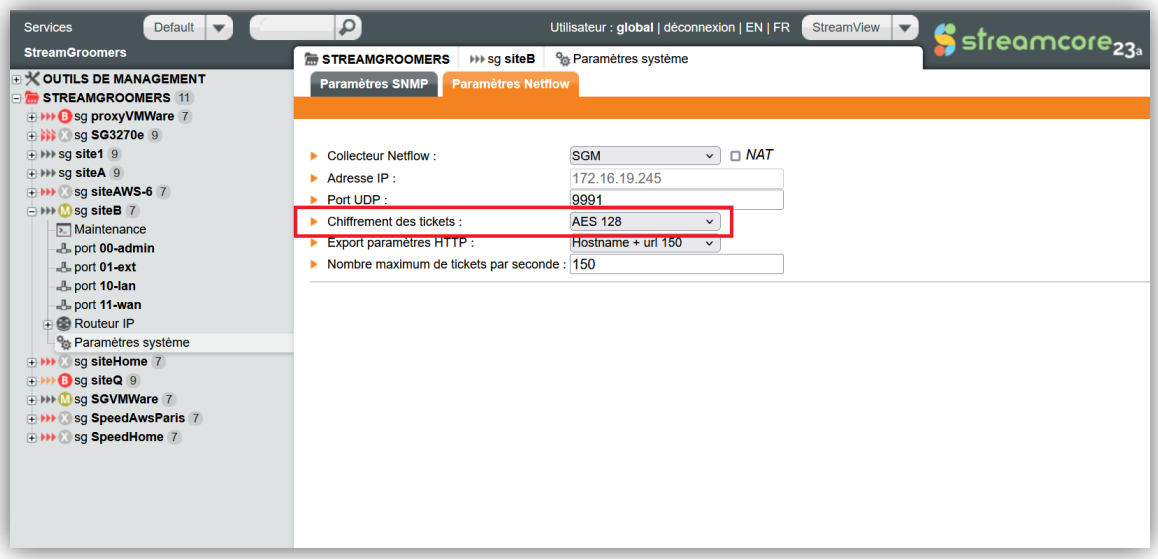
If the number of rules is saturated, it will be necessary to order a pack of additional rules that can be used either to provide application detail as a rule or session logging by activating the Netflow function of a rule.

4.2.2 Netflow payload encryption

Even if Netflow and the standards derived from it did not provide for this, it is now possible to historize Netflow tickets by circulating them with encrypted content. This makes it possible to send tickets between probes deployed on the Internet and an SGM via the Internet without the risk of compromising any of the data referenced therein (IP addresses, hostname, etc).

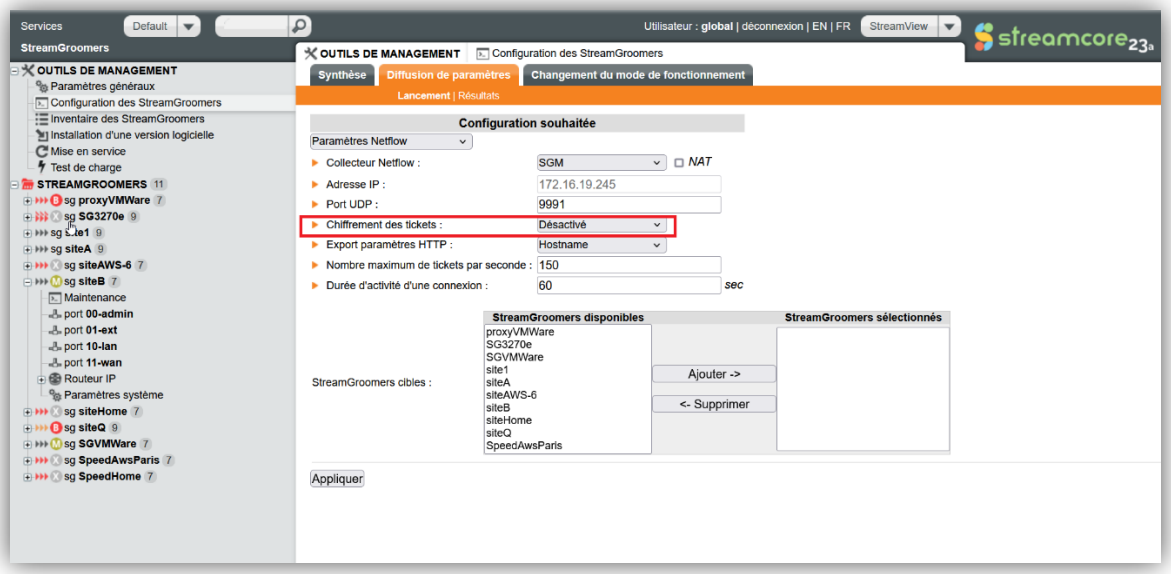
The encryption of the ticket is done in AES and requires that the probes are configured with the encryption key distributed by the SGM. For this, the SG must be at least in OPE version 6-5.18.

And in this case to activate this encryption you have to modify the Netflow configuration on the SG :



By default, the encryption remains disabled.

This configuration change can be globally applied to a batch of SGs in MANAGEMENT TOOLS :



4.2.3 Netflow activation on Fallback rules

Fallback rules are automatically created by the system when an intermediate rule, shaping, grooming or access binding is created.

Their purpose is to capture flows that meet certain criteria that are less precise than those of the terminal rules (which do not have Fallback rules). If Netflow is activated by application, it is useful to be able to configure (or not to forget) the Netflow export on the Fallback rules.

Indeed, in case of a traffic peak on a Fallback rule, it is useful to have the session history with IP addresses and port, source and destination to easily identify what happened.

By default, from version 23a onwards, the Fallback rules will be preset to log session tickets.

However, this setting will only have an effect if the site is Netflow export enabled by application or Total. If Netflow is not activated on the site, no more tickets, including those of the Fallback rules, will be transmitted.

It is also possible to disable this setting for each rule.

Already created Fallback rules are not affected by the new parameter value and will need to be updated.

4.3 SGM DEVELOPMENTS

4.3.1 Connections: new columns

Several new columns can be displayed on the current connections table.

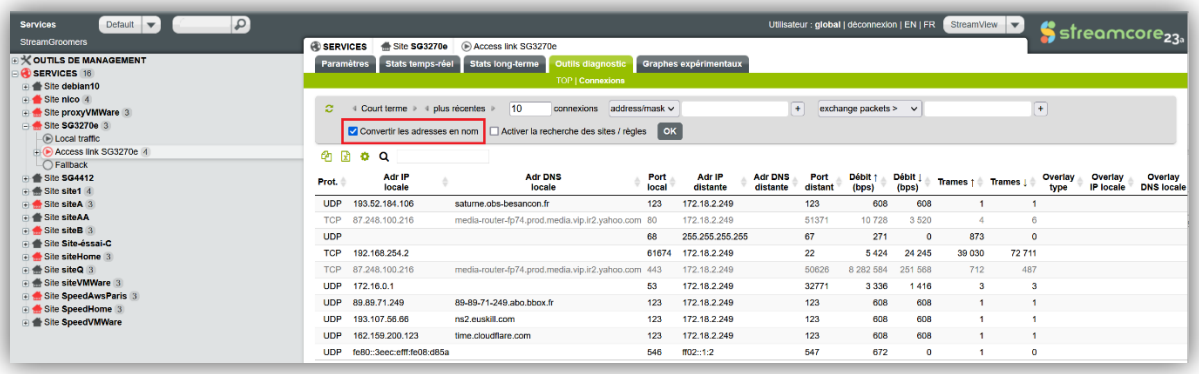
4.3.1.1 DNS NAME

The DNS translation of IP addresses is available in a special column in the current connections display. So now it is possible to read both the IP address and its DNS resolution at the same time.

4.3.1.1.1 PREREQUISITES

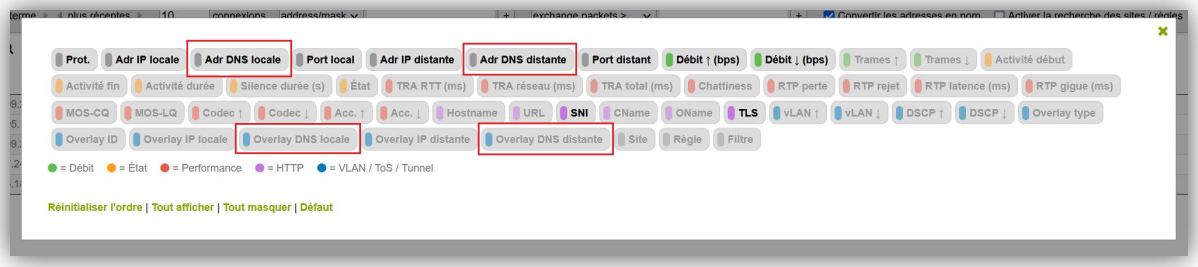
A DNS server must be configured on the SGM (in SGConf).

You have to explicitly ask for the DNS translation of the addresses to obtain this one:

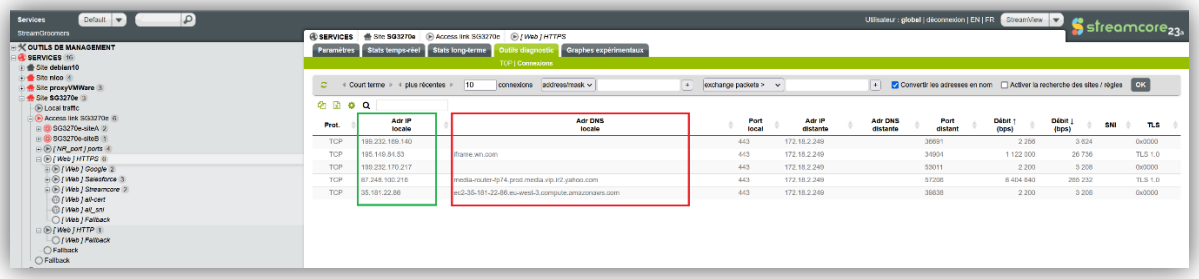


4.3.1.1.2 ADDITIONAL COLUMNS

Four new columns are available to be presented in the current connections table:

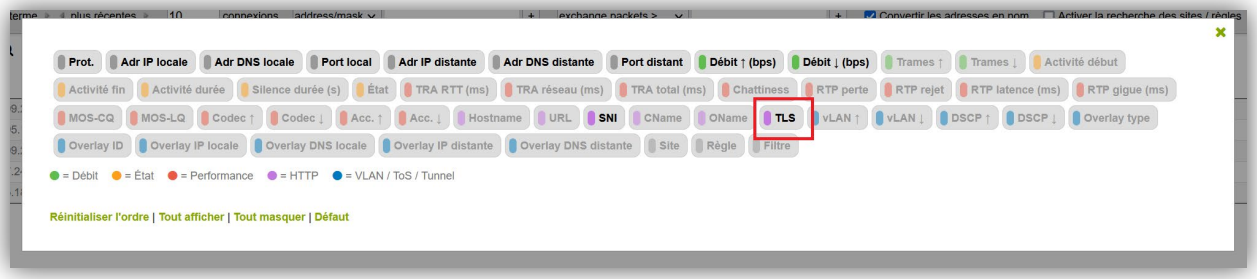


Local DNS address	DNS name of the source. If the connection is encapsulated in a decryptable tunnel, the name is that of the tunnel content.
Remote DNS address	DNS name of the destination. If the connection is encapsulated in a decryptable tunnel, the name is that of the tunnel content.
Local DNS overlay	If the connection is encapsulated in a tunnel (GRE, VxLAN, ...) DNS name of the tunnel for the source
Remote DNS overlay	If the connection is encapsulated in a tunnel (GRE, VxLAN, ...) DNS name of the tunnel for the destination

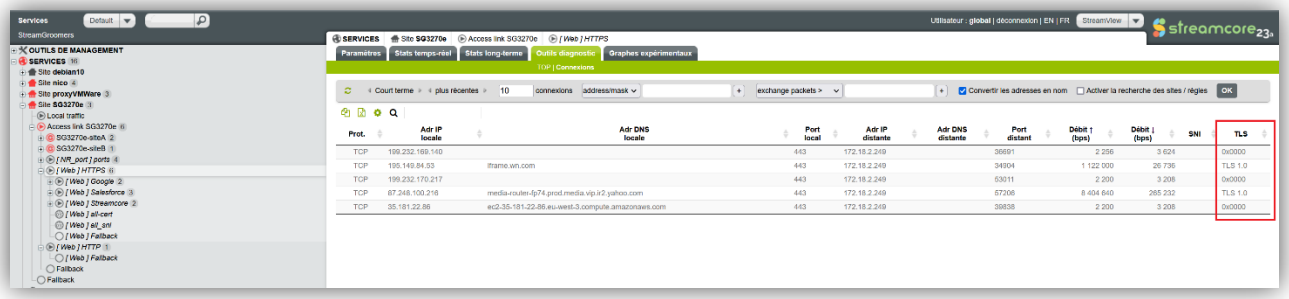


4.3.1.2 TLS VERSION

The TLS version number now has its own column in the display (and is no longer included in the hostname column):



For a display :



Note: The version number 0x0000 indicates an unrecovered version.

4.3.2 Adding a "chattiness" indicator to a rule

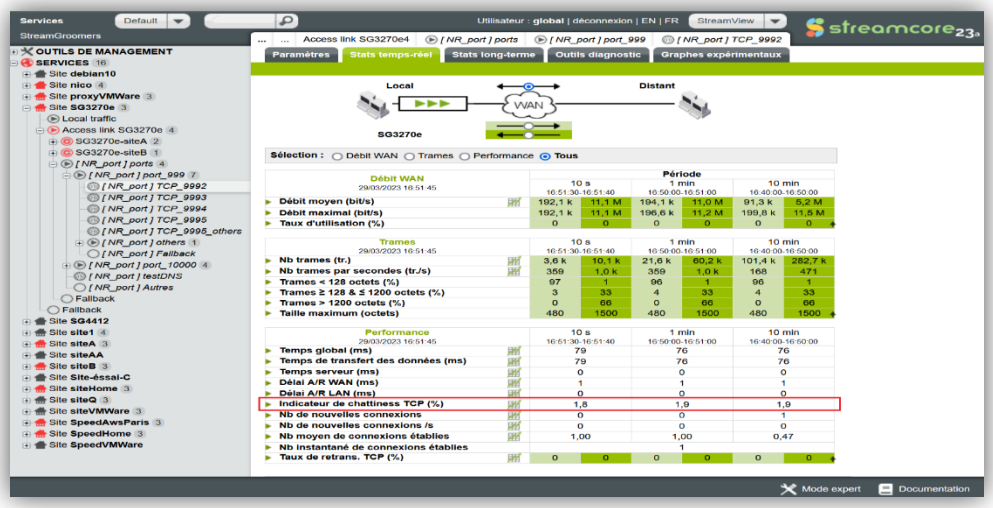
A new indicator on the quality of a session is available on the terminal rules.

The **chattiness** indicator, which indicates the degree of interactivity of an exchange between two interlocutors (two endings in our case). The higher the value of this indicator, the higher the number of requests/responses during the exchange.

4.3.2.1 OPERATION

The value of this index is calculated according to the formula: number of reversals * 100 / (number of total packets/2)
Where a reversal can be considered as a response.
We thus obtain a percentage that could theoretically reach 100% if we have a response packet to each request packet.

Example of a very un-chatty connection (data transfer type):



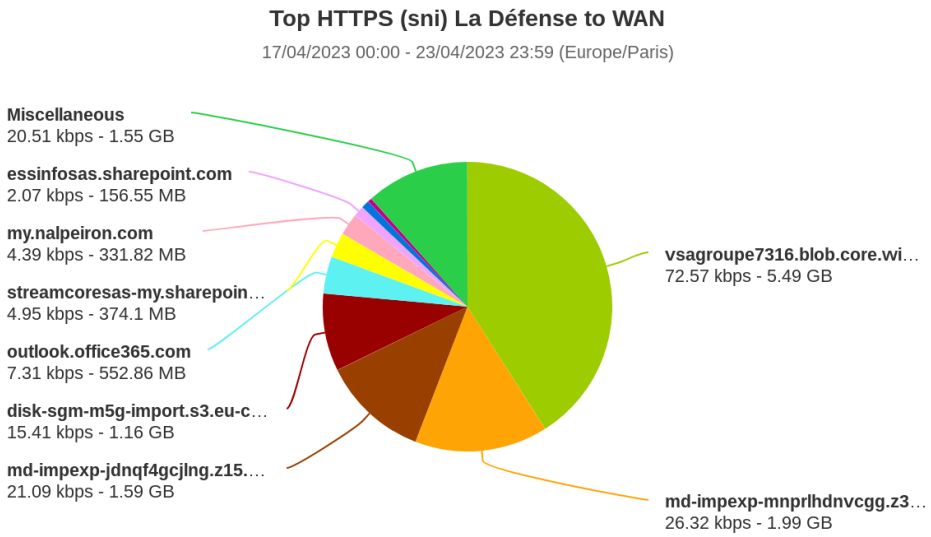
4.3.2.2 PRECAUTIONS

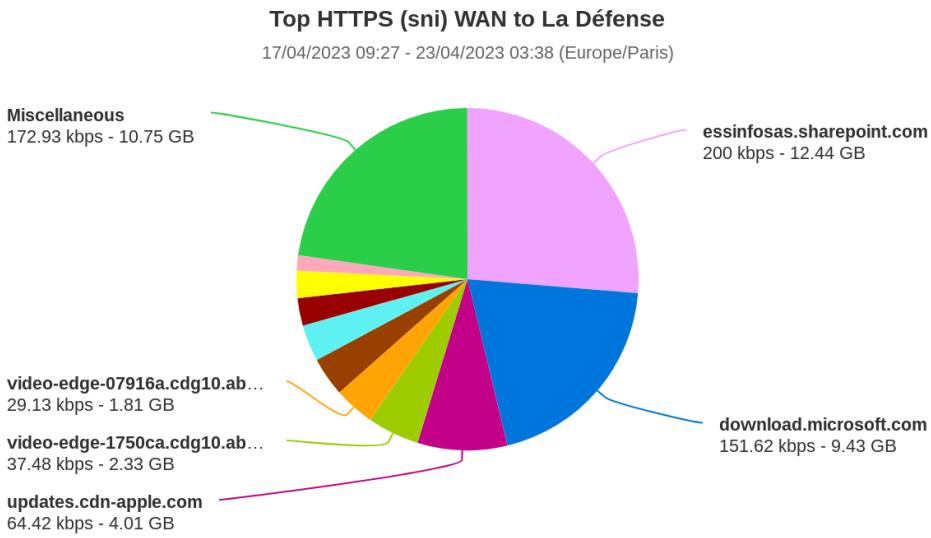
Only TCP traffic will return a non-zero value for the **chattiness** indicator.
All UDP traffic will return a null value.

And the traffic on the rule must be of the same nature to have a meaningful data.

4.3.3 TOP SNI for long term connections

In the long term diagnostic tools it is now possible to request a TOP on the value of the SNI field of HTTPS traffic.





4.3.4 UTF-8

All the components of the software suite use a unique **UTF-8** encoding.

This means that the files imported into the software must also be in UTF-8 format.
This is particularly the case for the import operations of :

- Sites
- Group of rules
- Types of categories and categories

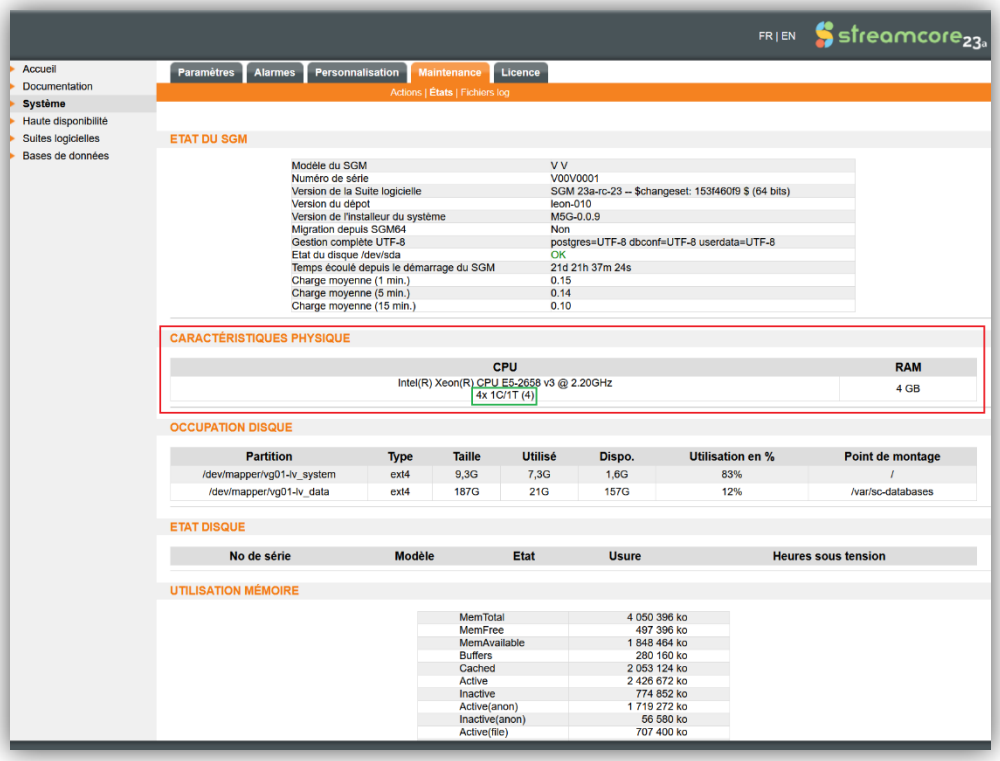
4.3.4.1 SWITCHING TO UTF-8

A transformation to UTF-8 encoding of the StreamView system data is automatically initiated in the following cases:

- Installation of suite 23a
- Migration of an SGM from a lower version to 23a
- Restore a database from a lower version SGM.

4.3.5 SGM status: CPU display

The status of the SGM (in SGMConf > System > Maintenance) now shows the characteristics of its CPU with notably the number of cores (and threads). In the attached illustration we have an SGM with 4 cores on a single thread.



4.3.6 Password for sgm and sc accounts

The passwords for the **sgm** and **sc** technical accounts will be aligned with the SGMConf **cli** account.

Since this version 23a a change of password of the **cli** account will automatically update the password of the **sgm** and **sc** users on the SGM with the same value.

4.4 DEVELOPMENTS ON SG PROBES

4.4.1 Breakout on WAN port

From this version it is possible to use a WAN port of the SG to establish an additional output (breakout) usable for the traffic passing through the SG.

In this architecture only the WAN port will be connected. The associated LAN port is no longer usable.

4.4.1.1 PREREQUISITES

OPE 6-5.18

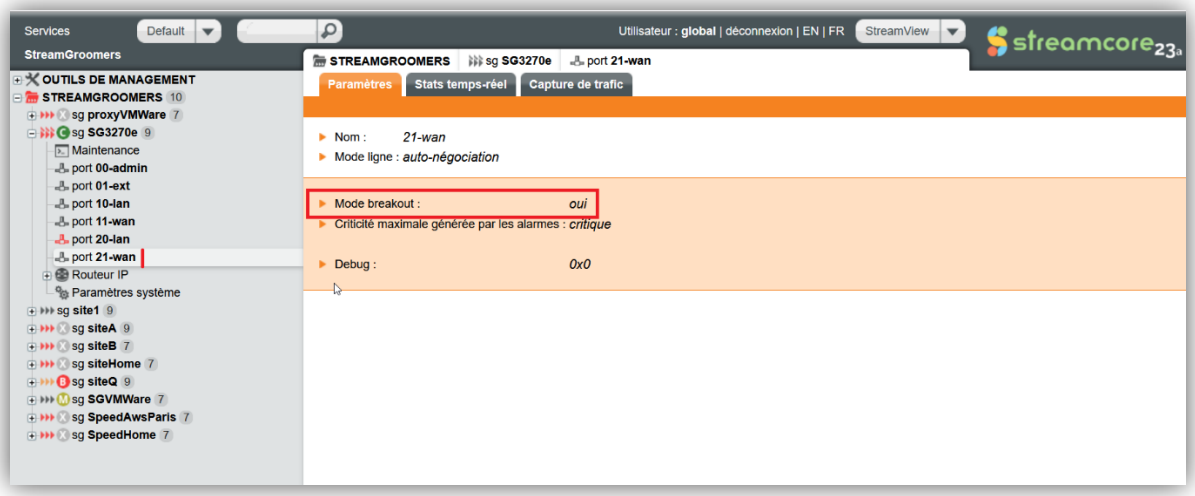
4.4.1.2 USE

As on the EXT port, it is imperative to configure a grooming in tunnel mode to be able to divert the traffic to this port. The traffic thus channeled will be the one filtered by the rule of this grooming.

4.4.1.3 CONFIGURATION

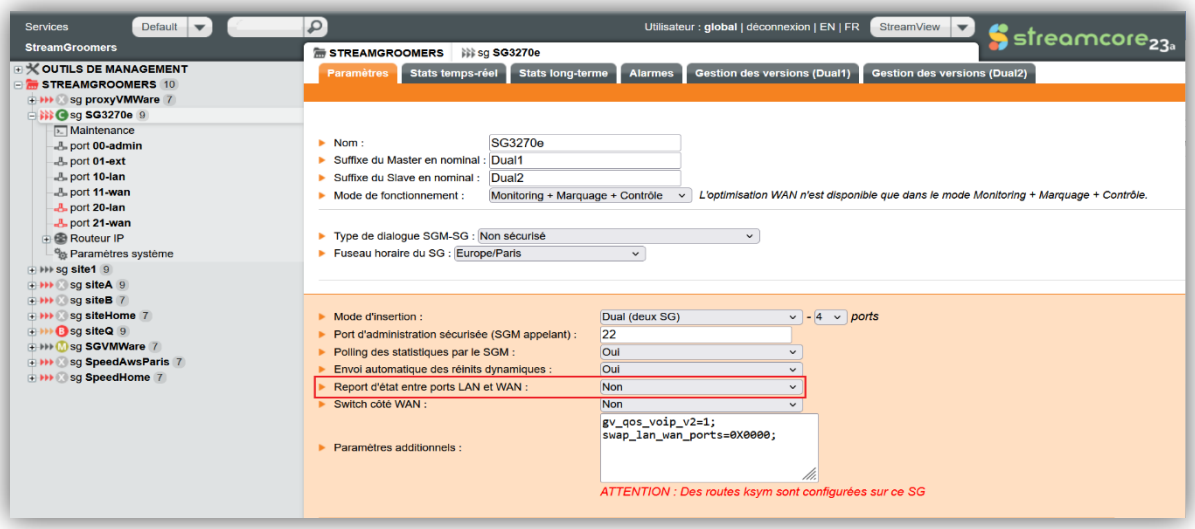
The port must be explicitly declared as a potential exit door.

In expert mode on a port wan switch the breakout mode to yes:

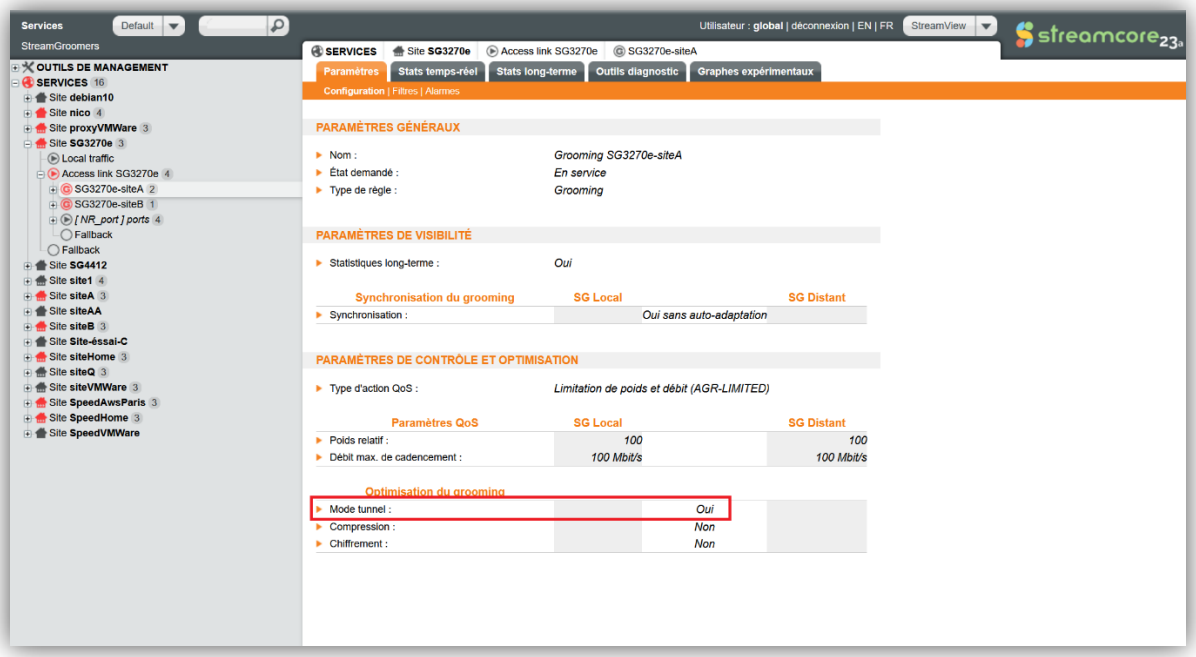


By default this mode is disabled.

As the LAN port is not connected, **it is imperative to deactivate the port status report** on the Streamgroomer (change it to no):



Then you will have to add a grooming in tunnel mode to direct the traffic to this new exit.



4.4.2 New port inversion setting

It is possible to request LAN/WAN port inversion on a SG. And this for any of its pairs.

The inversion will cause the port initially stamped as WAN to act as a port to the LAN.
While the initial LAN will be considered as a WAN exit of the traffic.

4.4.2.1 CONFIGURATION

A special additional parameter must be set (see 4.4.4) to the SG :

Parameter	Values	Defect
swap_lan_wan_ports	0x####	0x0000

The position of the binary '1's in the set value indicates which bypass pair is affected by this inversion.

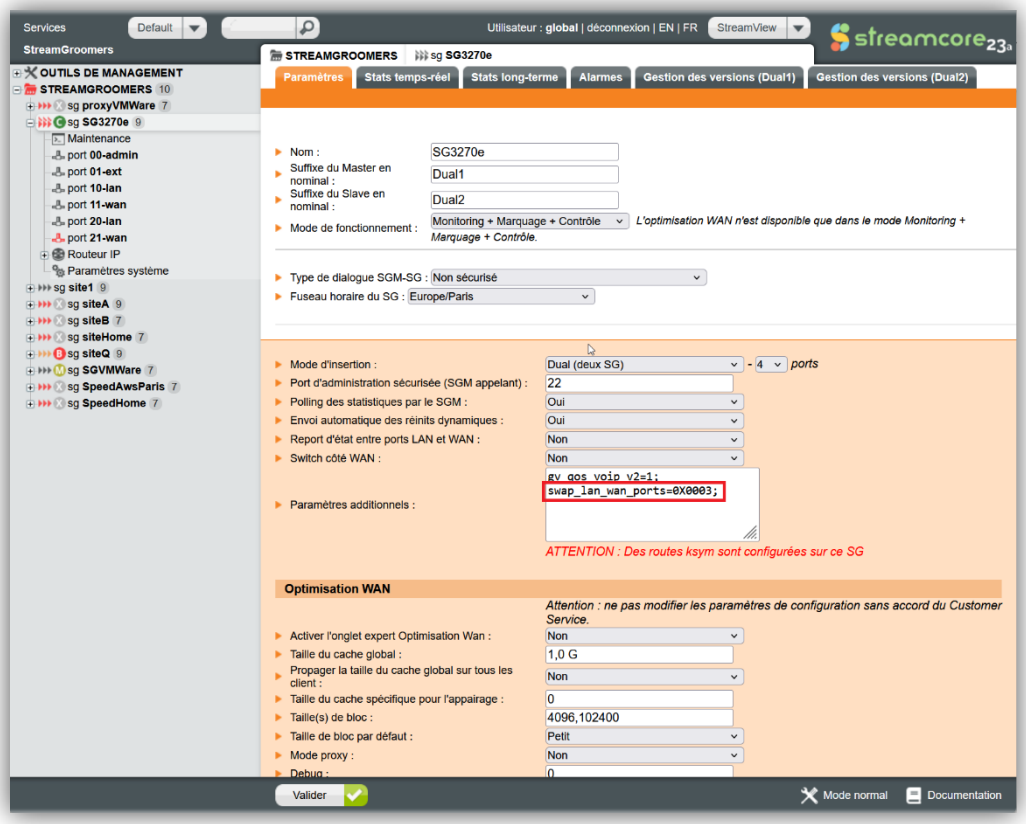
Examples:

0x0000	No inversion
0x0001	10-lan/11-wan torque inversion
0x0002	Reversal of the 20-lan/21-wan torque
0x2081	Inversion of the pairs 10-lan/11-wan, 80-lan-81-wan and e0-lan/e1-wan
0xFFFF	Reverse all ports

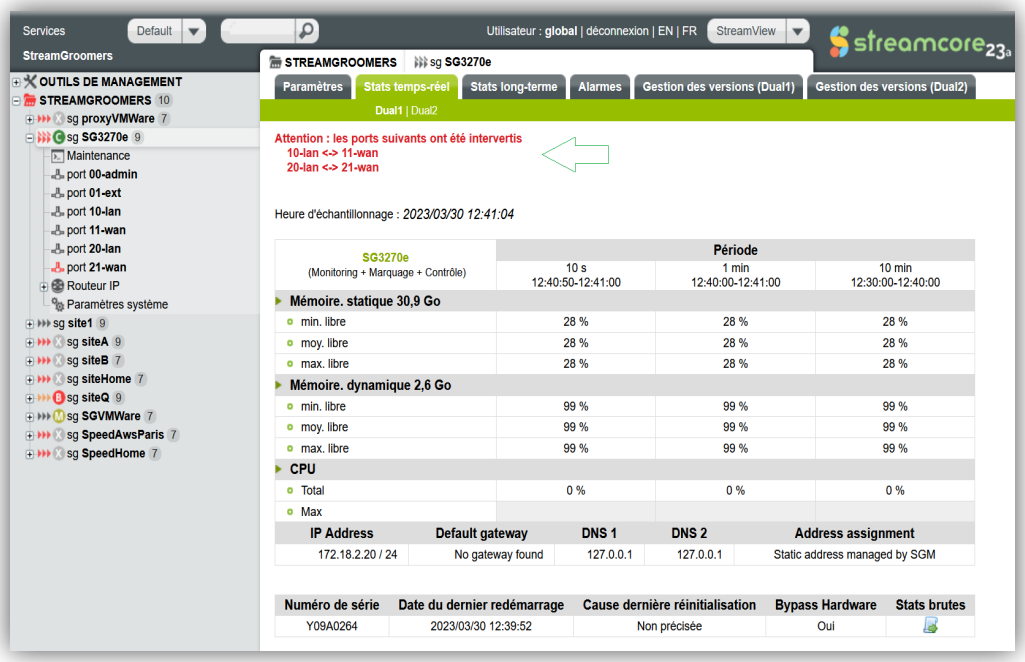
WARNING : a reboot of the SG is necessary to take into account this inversion

Illustration for the inversion of two couples.

Adding the advanced setting:



After rebooting the SG, the port inversion is indicated on the SG real time statistics page:

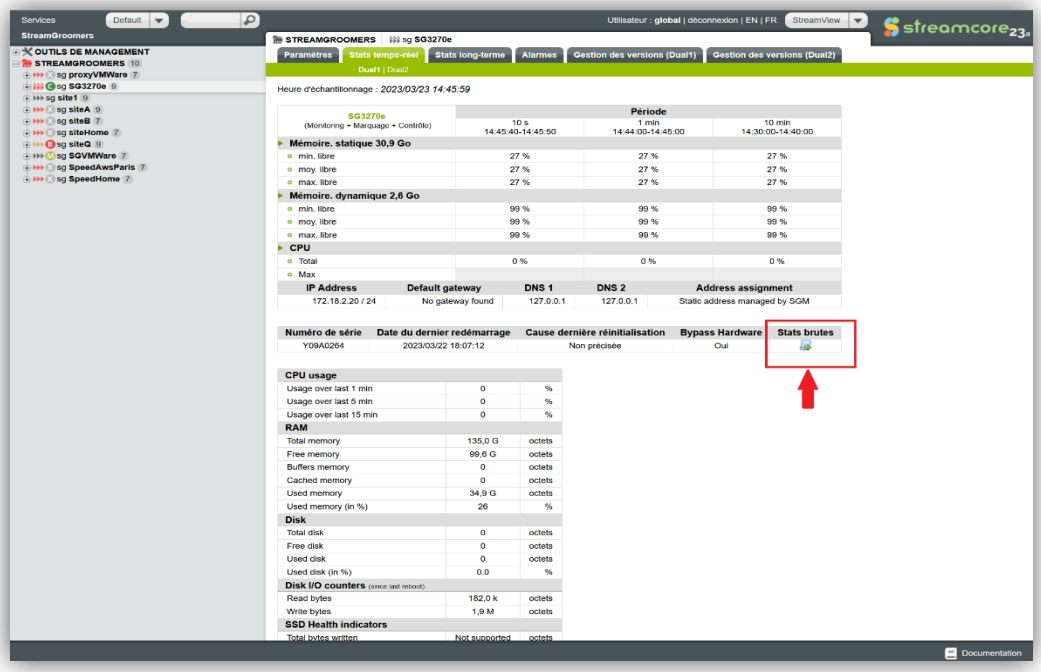


4.4.3 Access to raw statistics on an SG

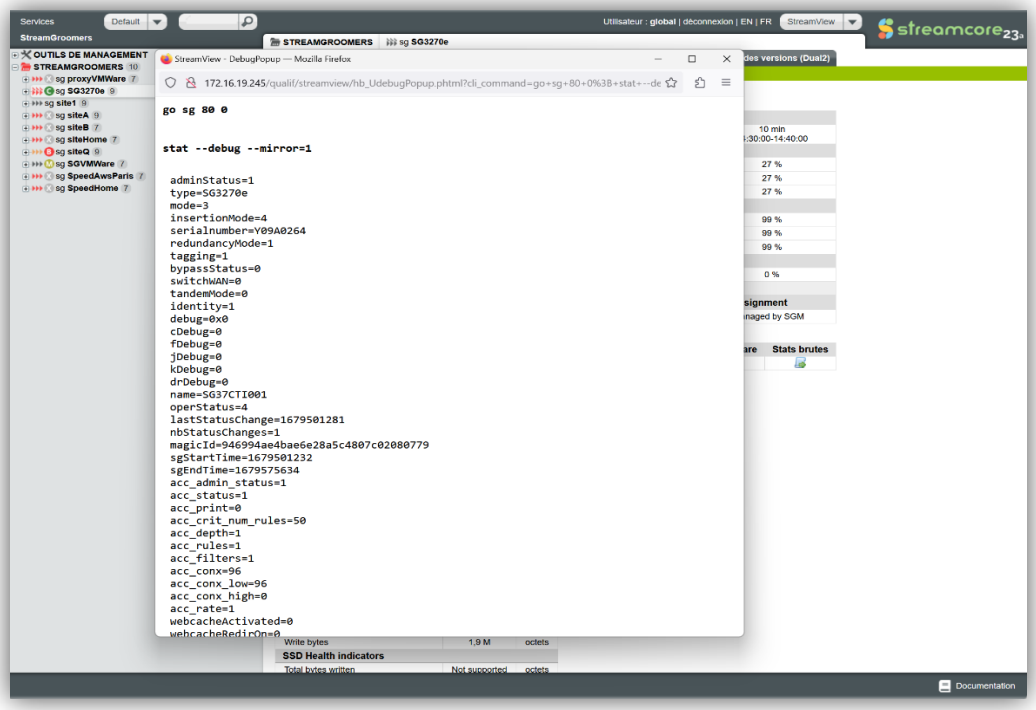
The StreamGroomer probe maintains counters on its activity which are neither displayed in the real time statistics nor historicized in the long term statistics.

Access to these indicators is now possible directly on the probe's real time statistics screen.

Click on :



To display the list of internal (raw) statistics of the SG :

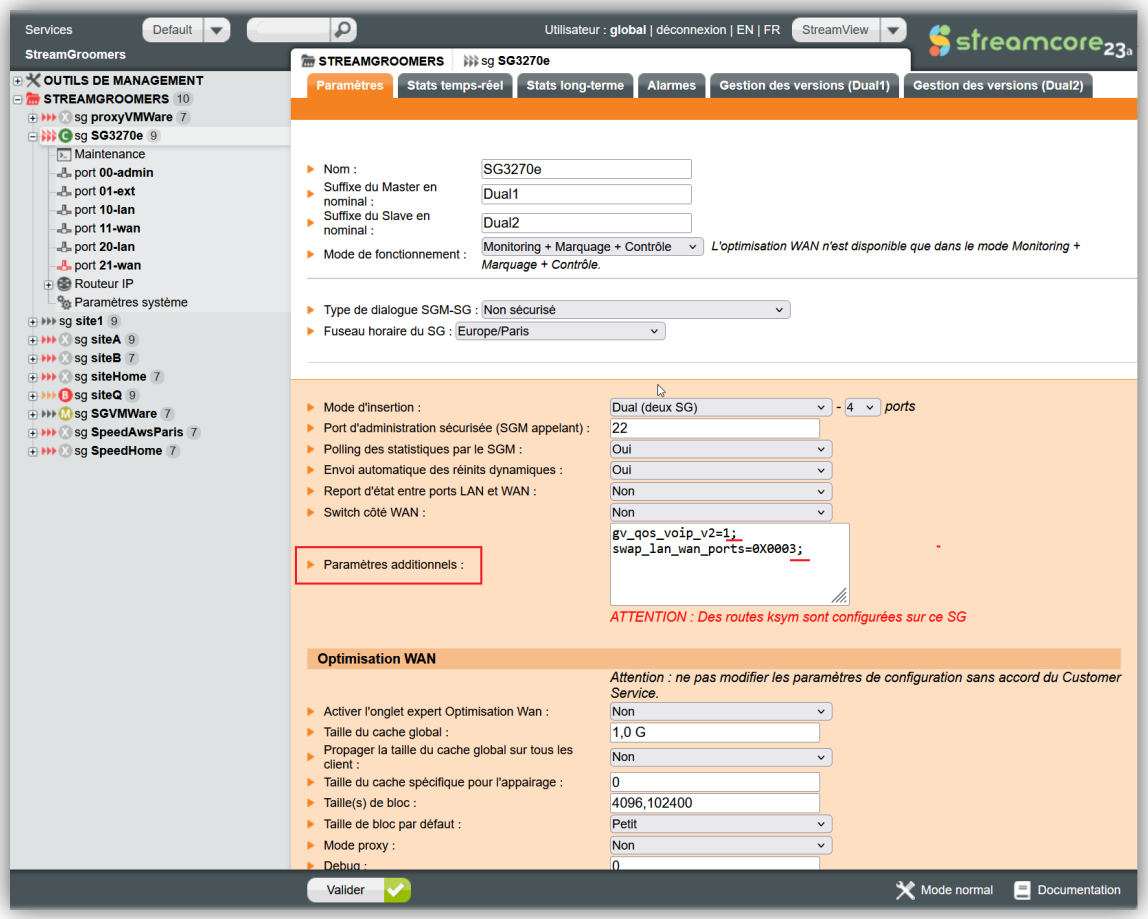


4.4.4 SG Additional parameters

It is possible to modify the behavior of the SG by adding additional parameters.

In this input field it is necessary to write pairs forming the assignment: **<parameter name>=<value> ;**
Always end a simple assignment with a semicolon (;) .

You can enter several assignments in a row.



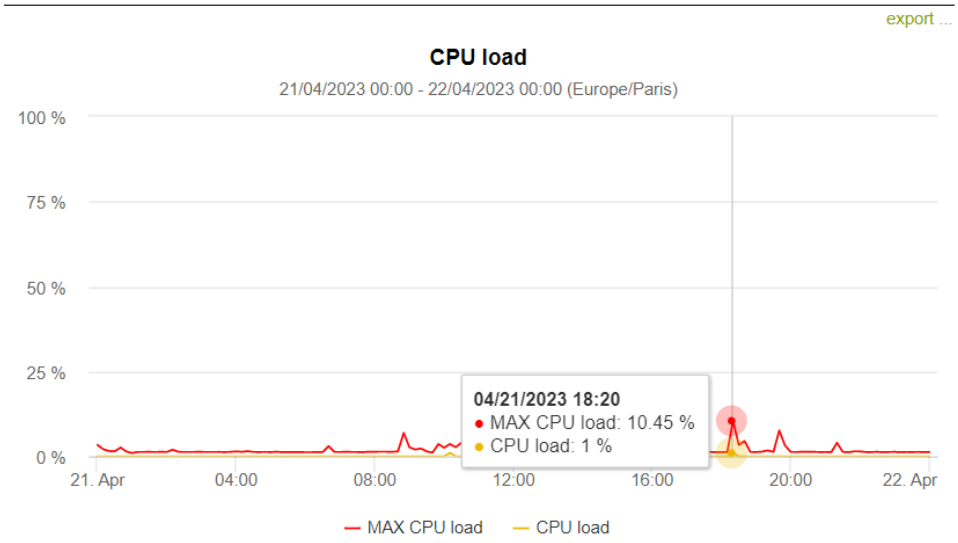
WARNING: deleting a parameter does not delete its assignment. You have to explicitly change its value (to return it to its default value) or delete and then reboot the SG.

These parameters are advanced parameters that should be used with care, contact Streamcore support (support@streamcore.com) for a list of these configurable parameters and their areas of use.

4.4.5 Display of max CPU

The CPU of the probes was displayed over a period of 10 minutes.

As with the other indicators, it is now also displayed with a max calculated over 10 seconds (10 second period of maximum activity during the 10 minute period). The consolidation of this indicator is done by taking the max of the max of the consolidated periods.



4.4.6 qhp version

A parallelized version of the OPE version of the probe has been available on request from support for several months.

This version is now delivered as part of the Software Suite in addition to the standard monothread version.

As a reminder, when moving from the M4G to the M5G generation of software versions, the operation changed from a kernel mode to an application mode above DPDK.

However, even in application mode, all the processing takes place on a single processing core, which is now separated from the OS tasks, which are now handled by the other cores of the machine.

The qhp version integrates a first level of parallelism by separating the flow monitoring part from the QoS part on the flows (the acceleration part is separated from the origin). In this version, the processing is distributed over 3 cores:

- A unique core dedicated to monitoring (classification and calculation of indicators)
- 2 QoS cores (1 per traffic direction)

The performance in terms of QoS is multiplied by 2 compared to the single-core version.

There is no gain in monitoring alone.

This version is recommended for devices that reach a high CPU load in QoS.

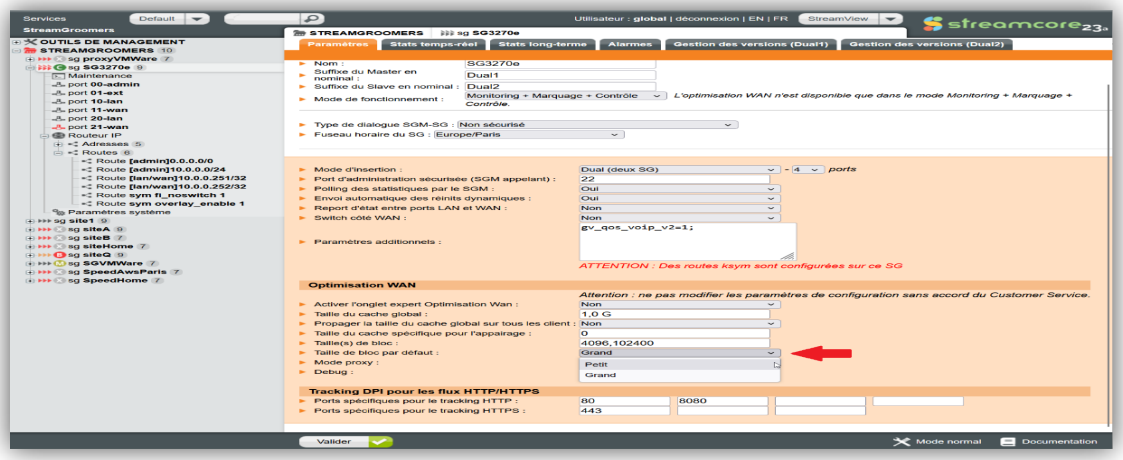
This version is homogeneous with the single-core version and has all its features.

Only the stress and QoS activity rate indicators are not currently available.

4.5 EVOLUTIONS ACCELERATION

4.5.1 Acceleration: choice of default block size, small or large

The acceleration uses a block size of data for caching.
If no blocks can be formed because of insufficient data, no caching will be done.



This block size can be of two dimensions, one of which will be considered large and the other small (obviously). Only one of these sizes is active.

To select this size it is now possible to indicate if you take the small or the big one.
To be configured on the SG in **expert mode**:

4.5.1.1 PREREQUISITES

The associated StreamGroomer must be at least OPE 6-5.18 to be able to take this configuration into account.

4.5.2 Disable application server in error

This version implements DIAS (Disabling Inaccessible Application Servers) on application servers configured for acceleration on a StreamGroomer.

Physical or virtual acceleration probes should be located as close as possible to the applications they are supposed to optimize. However, the architecture and security constraints of data centers mean that the acceleration function can be separated from the applications themselves by intermediate equipment (routers, firewalls, load balancers, etc.). These devices or the routing of flows that must pass through them can fail from time to time, blocking access to the application from the acceleration probe.

In these cases, to prevent access to the application from being interrupted when the flow passes through the acceleration tools, we have developed a circuit breaker mechanism called DIAS.

This DIAS allows you to disable for acceleration any application server that encounters a minimum number of connection problems in a given time. And then reactivate it within a given time.

These three parameters have default values and can be configured by adding "additional parameters" to the StreamGroomer (see chapter on Additional parameters)

These parameters are :

Description	Name	Default value	Limits
Minimum number of occurrences of connection problems on a server before triggering its deactivation	acc_watchdog_errors	5	1 - 60
Maximum time allowed for the successive occurrence of these problems to trigger deactivation. If this time is exceeded, the number of occurrences is reset to zero while waiting for the next incident.	acc_watchdog_period	60s	10s - 600s
Timeout after deactivation to reactivate the server	acc_watchdog_duration	86400s (1d)	60s - 8 days

5 New features OPE 6-5.17

5.1 UTF-8

Switching to UTF-8 encoding of the various StreamGroomer data, including logs.

5.2 DEFAULT BLOCK SIZE

Enables the default block size configuration for acceleration to be taken into account.

To set up this configuration see. 4.5.1

6 New features OPE 6-5.18

6.1 BREAKOUT ON WAN PORT

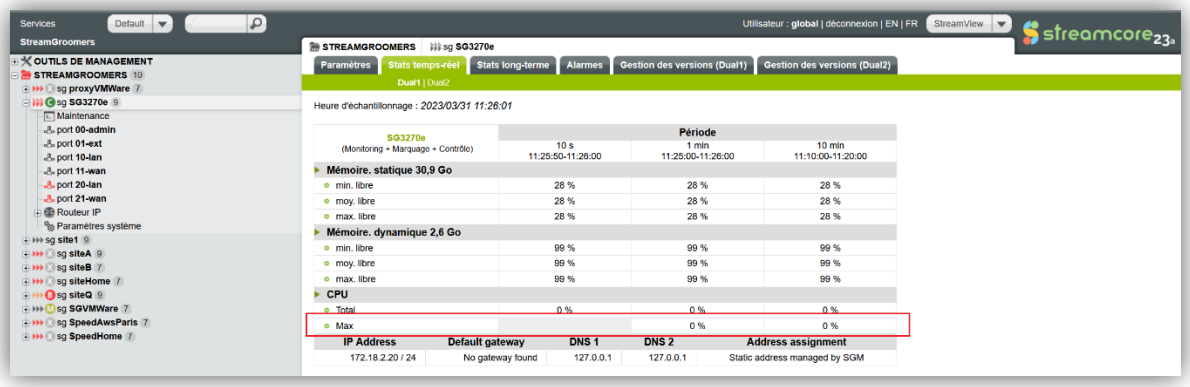
To take into account the detour to a WAN port.

For WAN port configuration see. 4.4.1

6.2 CPU MAXIMUM LOAD

A new information is available in the StreamGroomer real time statistics, the maximum CPU load.

This measurement indicates the maximum load rate reached by the StreamGroomer over the indicated period of time (1mn or 10mn). The CPU load being measured over 10s the maximum is not displayed for this period.



To display this statistic you need an SGM in 23a minimum.

7 New ACC features

7.1 ACC32

7.1.1 Disable Inaccessible Application Server (DIAS)

This version implements DIAS (Disabling Inaccessible Application Servers) on application servers configured for acceleration on a StreamGroomer.

This DIAS allows you to disable for acceleration any application server that encounters a minimum number of connection problems in a given time. And then reactivate it within a given time.

These three parameters have default values and can be configured by adding "additional parameters" to the StreamGroomer (cf. 4.4.4)

These parameters are :

Description	Name	Default value	Limits
Minimum number of occurrences of connection problems on a server before triggering its deactivation	acc_watchdog_errors	5	1 - 60
Maximum time allowed for the successive occurrence of these problems to trigger deactivation. If this time is exceeded, the number of occurrences is reset to zero while waiting for the next incident.	acc_watchdog_period	60s	10s - 600s
Timeout after deactivation to reactivate the server	acc_watchdog_duration	86400s (1d)	60s - 8 days

7.2 ACC34

7.2.1 New acceleration base

The acceleration module has been updated to the new 7.1.0 acceleration system.

This new system brings better performance on the use of the cache.

WARNING : these improvements on the use of the cache required a change of architecture of this one, making inoperative the use of an old cache. Therefore the installation of this new version will erase the cache already built on the SG to be able to start again on a healthier basis.

8 Corrections made by version 23a

All components of the software suite are delivered as updated versions.

Note: In this software suite, the BOOT components are **S56**. and **T11**. The correct version, depending on the type of SG (M4G or M5G), will be installed automatically by the SGM when a BOOT is deployed on the StreamGroomers.

The following tables list the problems that have been fixed in version 23a of the software suite:

Customer ticket	Reference	Description of the problem that was solved (SGM 23a)
SGM 23a		
SCC-00001409	SC-1182	No error message when adding a filter with duplicate name on "inclusion of subrules".
SCC-00001412	SC-1269	On-site long term statistics Applications: unsorted list
SCC-00001414	SC-1270	On the SGM the loadavg of an SG M4G has a value of 6.25
	SC-1286	[Traffic capture] Incorrect colors
	SC-1291	[StreamView] Disconnection of StreamView after a certain time
	SC-1299	[SGMConf] Add a control on some parameters with special characters
	SC-1301	[StreamView] From the Matrix, you can add an empty alarm group
	SC-1314	[SG Configuration] Display a "?" in the category column
	SC-1321	[StreamView] Display of the results of the "Search" field malformed because of the presence of an icon
	SC-1323	[StreamReport] Problem with displaying special characters
	SC-1326	Sending mail from SGM in error (continued)
SCC-00001424	SC-1349	Adding shaping matrix in line: does not respect the choice of location of the rules
	SC-1374	Crash OPE on start-up
SCC-00001426	SC-1387	Grooming : statistics gives synchronization date on 1970
SCC-00001427	SC-1424	StreamAccess : user restricted in read/write rights : no modification

Customer Ticket	Reference	Description of the problem that was solved
OPE 6-5.17		
SCC-00001392	SC-1024	Grooming synchronization loop

Customer Ticket	Reference	Description of the problem that was solved
OPE 6-5.18		
SCC-00001426	SC-1387	Grooming : statistics gives date of synchronization on 1970
SCC-00001437	SC-1535	SG plants on traffic video

Customer Ticket	Reference	Description of the problem that was solved
Boot T11		
	SC-1272	[DHCP] Cannot display the conf if DHCP provides a search domain
	SC-1286	[Traffic capture] Incorrect colors
SCC-00001420	SC-1304	Hole in the curves: "Connection refused" error in polling

Customer Ticket	Reference	Description of the problem that was solved
ACC33		
	SC-1390	[ACC] DIAS - acceleration crash if all appservers are disabled

9 Known issues

The table below lists known problems and provides a workaround if necessary.

Reference	Component	Description of the known problem	Alternative solution
FB46694	StreamView StreamAccess	From software suite 6- 4.S 08 - Authentication with Radius does not work if the password contains the following characters • Double quotation mark " • quotation mark ' • Slash / • Exclamation mark! • Back cut • Hooks [and] • Star *	Change the Radius password avoiding the use of these characters.
FB42810	SG	StreamGroomers can restart in a port mirroring configuration when capturing traffic.	
-	SG	Grooming, dual mode and tandem mode do not work with version 6.6 OPEs	Use for the moment a 6-5qhp version
FB47230	SG	With ACC24 or later and an older OPE (< 6-4.17), each reboot of the SG will clear the acceleration cache.	Upgrade to OPE 6-4.17 or higher
FB49409	SG	On an SG in Dual/Tandem mode and in an SGM HA environment (SGM cluster), changing the communication mode from "calling SG" to "not secured" may cause an error.	Contact Streamcore Support
FB4913	SG	The SG with a T0# boot version could not use any SGM calling the Secure dialog type (weak or strong)	Choose the one that **is not secure** and that already uses an SSH connection. Or a type of SG caller dialog.
SC-1550	SG	Unavailability of QoS and Stress indicators in qhp version	Development of indicators in progress

10 Installation and deployment

Read the following recommendations carefully:

- CAUTION: On the SG250e, status mirroring between LAN and WAN ports does not work.
- After starting the StreamGroomers in operational software, it is strongly recommended to check the LAN and WAN ports statistics (speed and duplex mode, CRC errors, collisions...) in order to avoid any configuration mismatch with the interconnected equipments.
- We recommend to connect to the ADMIN port on the LAN side of the StreamGroomer.
- On the SG350e, when switching from boot software (closed bypass) to operational software in bypass mode, the bypass opens and closes immediately, resulting in two interface state changes. This operation can block traffic for a few seconds.
- Direct connection of peripherals (mouse, keyboard and monitor) to the SGM should only be done for maintenance purposes.

11 Software interoperability rules

11.1 VERSION DOWNGRADE OPERATION

Read the rules carefully:

- SGM: unauthorized operation (risk of data loss)
- SG OPE: operation authorized if the OPE vs Boot/System interoperability rules are respected (see table below).
- SG Boot/System: unauthorized operation (risk of material accident)
- ACC acceleration system: unauthorized operation

11.2 INTEROPERABILITY BETWEEN COMPONENTS

Interoperability is guaranteed for an SGM in the following cases:

- Version SGSS 6.4 with a SG in OPE 6.5, 6.4, 6.3 and 6.2
- Version SGSS 6.5 with a SG in OPE 6.5, 6.4, 6.3 and 6.2
- SGSS 22x version with a SG in OPE 6.5, 6.4 and 6.2-11

Interoperability not guaranteed for an SGM that is older than the OPE version.

The table below indicates when compatibility between SGM and SCO versions is guaranteed:

SCO	SGSS 6.4	SGSS 6.5
Up to 1.2	Not guaranteed	Not guaranteed
Up to 1.3	Yes, for OPE >= 6-2	Yes, for OPE >= 6-2
From 6.5	Yes, for OPE >= 6-2	Yes, for OPE >= 6-2

12 Technical support

Streamcore Technical Support

By e-mail: support@streamcore.com

By phone: +33 (0)1.78.96.53.21
+33 (0)6.45.58.84.68

Customer support

Email: support@streamcore.com

Telephone: +33.1.78.96.53.21