TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING QOS ON SNS FIREWALLS

Product concerned: SNS 4.3.15 and later versions of 4.3 branch, SNS 4.5.3 and higher versions

Document last updated: February 2, 2023

Reference: sns-en-configuring-qos-on-SNS-firewalls-technical_note

Table of contents

Getting started

Quality of Service (QoS) and its components

Quality of service refers to any technology that can manage data transmission while reducing packet loss, latency and jitter for high-priority traffic on the network. The aim of this concept is to monitor and manage network resources by prioritizing certain types of data and network traffic.

There are two ways in which traffic is managed:

- Bandwidth reservation for high-priority traffic or traffic with high technical constraints (e.g., work flows or telephony over IP),
- Bandwidth limitation for lower-priority traffic (e.g., web browsing).

NOTE
Bandwidth reservation or limitation is applied to traffic when it leaves the network interface on which QoS has been enabled. So, these mechanisms do not have any real impact on incoming traffic, such as downloads.

Regulation mechanism: difference in the behavior of TCP and UDP traffic

When TCP traffic exceeds the bandwidth limit set in a QoS queue, the regulation mechanism will reject some of these TCP packets and slow down traffic leaving the interface. The sender of the TCP traffic will then realize that packets were lost along the way and slow down throughput until it meets the firewall's QoS configuration criteria.

As this regulation mechanism does not exist for UDP traffic, incoming throughput on the interface will never adapt to the QoS configuration; it will also not comply with all bandwidth reservations on the incoming interface, and even disrupt them.

QoS queues

For these reservation and limitation operations, the queues that will be assigned to QoS-enabled network interfaces must be defined.

There are three possible types of queues:

- Class-Based Queuing or CBQ: these queues are used for reserving or limiting bandwidth by indicating the maximum or guaranteed bandwidth to apply,
- Priority Queuing or PRIQ: in these queues, packets are prioritized and classified from priority 0 (traffic with the highest priority) to priority 7 (traffic with the lowest priority).
  Packets associated with a filter rule that uses a PRIQ are processed before packets that are not assigned to a PRIQ, or which are attached to a PRIQ with lower priority.

  IMPORTANT
  - To prevent the risk of traffic congestion, such queues must be reserved for throughput-controlled traffic that cannot consume all the bandwidth, and must be reserved for traffic with the highest priority.
  - We strongly recommend having a single PRIQ that can deprive the other queues and assign to it a lower priority than for other queues. For example, do not create a PRIQ for HTTP and another for FTP.
  - You are advised against using more than three or four levels of priority in a configuration.
  - Do not combine PRIQs and CBQs in the same configuration.
    Even though the web administration interface does not prohibit the combination of CBQs and PRIQs, Stormshield does not support such configurations.
- Monitoring Queuing or MONQ: these specific queues do not have any impact on network traffic but make it possible to save and present in graphs (**Monitoring** > **Monitoring** > **QoS** module) information about the bandwidth used by the traffic to which these queues were assigned. This makes it possible to set or refine the configuration of CBQs.

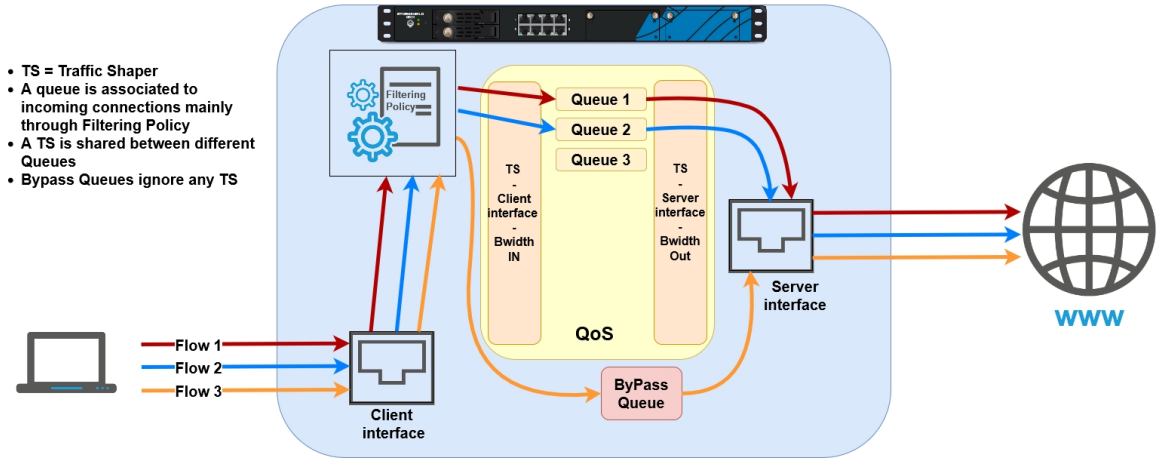
The volume of data exchanged is regulated by a traffic shaper associated with QoS queues. This traffic shaper applies to the outgoing interface of processed packets.

DEFINITION
The aim of traffic shaping is to enforce the Committed Information Rate (CIR) through the regulation of data volume exchanged over the network, by delaying packets that meet the criteria defined in the queues (reservation or limitation). The mechanism runs on an algorithm named TBR (Token Bucket Regulator) which uses a buffer for excess traffic.

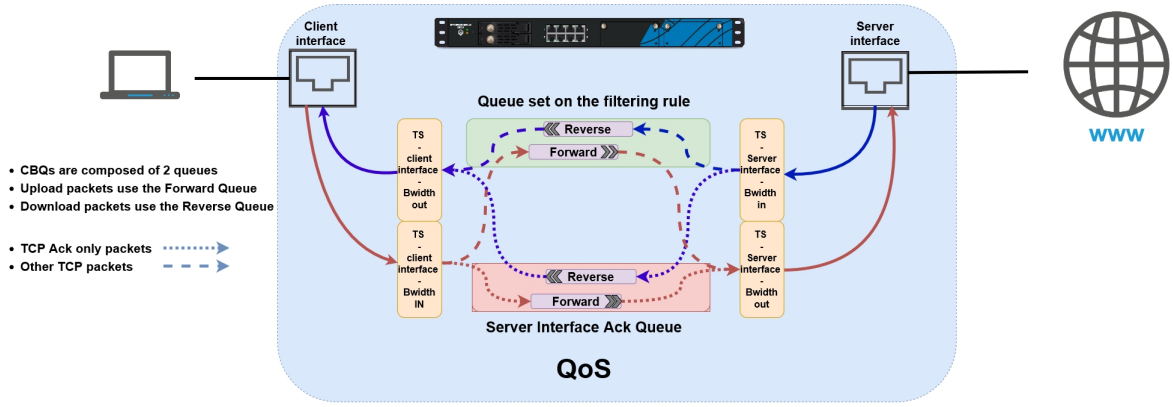
IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

NOTE
In configurations that use IPsec traffic, such traffic will automatically join the default queue for the WAN interface. This is why class-based queuing is applied to this queue.

Illustration: overview of QoS



Application of QoS in LAN/WAN network traffic



Interfaces incompatible with QoS

The following interfaces cannot be selected for the application of QoS:

- GRE interfaces,
- Loopback interfaces,
- SSL VPN interfaces,
- Wi-Fi interfaces,
- LACP link aggregates,
- 4G USB modems,
- PPPoE and PPTP modems.

Using QoS through the SSL proxy

In configurations with HTTPS traffic that goes through the SSL proxy, the corresponding QoS queue must be applied to the decryption rule instead of the proxy filter rule.

Best practices

By observing some best practices, QoS can be optimally implemented:

- Configure a default acknowledgment queue (queue reserved for TCP acknowledgment [ack] packets) for each QoS-enabled network interface. Each acknowledgment queue corresponds to a 5% reservation of bandwidth on the network interface in question.
- Configure default queues for each QoS-enabled network interface. Any traffic for which no specific QoS queue has been specified will join the default queue.
- For traffic that consumes a significant portion of bandwidth, bypass queues must not be used as they have priority over all traffic and cause bandwidth reservation to malfunction. Such traffic will not be taken into account when limitation is detected on the interface and can therefore prevent QoS from activating when bandwidth is saturated on a link.
  Bypass queues are to be used for traffic such as IPsec negotiation or router monitoring.

Implementation precautions

IMPORTANT
Before implementing Quality of Service (QoS) in a production architecture that was initially free of any QoS settings, Stormshield recommends that you first create a configuration based on monitoring queues (MONQ) instead of directly on class-based queues (CBQ).
This step will help you to see the volume of traffic on which no QoS is applied, and to check whether the intended bandwidth reservation or limitation values for CBQs suffice to let QoS-enabled traffic pass through.
Once these values are established, you can then set up your CBQs.

Restrictions and characters allowed in queue names and traffic shaper names

QoS queues

- Names must not exceed 31 characters.
- Prohibited characters:

```
@ [ ] # ! \ " | <space> <tab>
```

- Names must not contain any of the following reserved expressions:

```
internet any any_v4 any_v6 firewall_ network_ broadcast anonymous
none all original
```

Traffic shapers

- Names must not exceed 15 characters,
- Prohibited characters:

```
@ [ ] # ! \ " | <space> <tab>
```

Naming of interfaces in this Technical Note

For a better understanding of the various use cases shown, the firewall's original interfaces have been renamed as follows:

- *in* interface: *LAN*,
- *out* interface, *WAN*,
- *dmz1* interface, *DMZ*,
- *dmz2* interface, *WAN2*.

Lowest configuration required to apply QoS: example of a LAN/WAN architecture

This section describes the lowest configuration required to apply QoS: in an architecture that has a local network (attached to the *LAN* interface in this example) and Internet access (attached to the *WAN* interface in this example). The various steps to follow are:

- Create the default queue and default acknowledgment (ACK) queue for each QoS-enabled interface,
- Specify traffic shapers,
- Assign traffic shapers, default acknowledgment (ACK) queues and default queues for QoS-enabled interfaces.

Creating default queues

Go to **Security policy** > **Quality of service** > **Queues** tab.

Understanding the queue grid

"Guaranteed bandwidth" and "Max bandwidth" columns

The Guaranteed bandwidth and Max bandwidth columns are dedicated to traffic leaving the network interface:

- In the Guaranteed bandwidth column, bandwidth reservation can be set for outgoing traffic,
- In the Max bandwidth column, bandwidth limitation can be set for outgoing traffic.

Guaranteed rev. and Max rev. columns

The Guaranteed rev. (guaranteed reverse bandwidth) and Max rev. (maximum reverse bandwidth) columns are dedicated to a connection's return traffic:

- In the Guaranteed rev. column, bandwidth reservation can be set for return traffic on connections,
- In the Max rev. column, bandwidth limitation can be set for return traffic on connections.

Creating default queues for the *LAN* and *WAN* interfaces

> **NOTE**
> We highly recommend specifying bandwidth reservation (**Guaranteed bandwidth** and **Guaranteed rev.** fields) for default queues.
> This is because when available bandwidth on the link is saturated, if no bandwidth is reserved, the firewall may delete traffic that must join the default queue.
> The value of this reservation depends on the volume and amount of low-priority traffic that is not part of a specific QoS queue.

Creating the default queue for the *LAN* interface

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.

3. Name the queue (*DEF_LAN_Q* in this example).
4. In the **Guaranteed bandwidth** line, indicate the desired value for bandwidth reservation (100 Mbit/s in this example).
5. In the **Max bandwidth** line, leave the value suggested by default (10 Gbit/s).
6. In the **Guaranteed rev.** line, indicate the desired value for bandwidth reservation (100 Mbit/s in this example).
7. In the **Max rev.** line, leave the value suggested by default (10 Gbit/s).
8. Confirm by clicking on **Apply**.

Creating the default queue for the *WAN* interface

Follow the steps explained in the procedure Creating the default queue for the *LAN* interface with the following values:

Queue type	Class Based Queuing
Name	*DEF_WAN_Q*
Guaranteed bandwidth	10 Mbit/s
Max bandwidth	value suggested by default (10 Gbit/s)
Guaranteed rev.	10 Mbit/s
Max rev.	value suggested by default (10 Gbit/s)

NOTE
In configurations that use IPsec traffic, such traffic will automatically join the default queue for the WAN interface. This is why class-based queuing is applied to this queue.
Please note that the application of QoS to IPsec traffic is not covered in this Technical Note.

Creating acknowledgment (ACK) queues for *LAN* and *WAN* interfaces

In this example, the link connected to the LAN interface offers maximum bandwidth of 1 Gbit/s while the link connected to the WAN interface has maximum bandwidth of 100 Mbit/s.

The respective acknowledgment (ACK) queues are therefore 50 Mbit/s for the *LAN* interface and 5 Mbit/s for the *WAN* interface (reservation of 5% of the maximum bandwidth on links).

Creating the acknowledgment (ACK) queue for the *LAN* interface

Follow the steps explained in the procedure Creating the default queue for the *LAN* interface with the following values:

Queue type	Class Based Queuing
Name	*DEF_LAN_ACK_Q*
Guaranteed bandwidth	50 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	50 Mbit/s
Max rev.	unlimited

Creating the acknowledgment (ACK) queue for the *WAN* interface

1. Follow the steps explained in the procedure Creating the default queue for the *LAN* interface with the following values:

Queue type	Class Based Queuing
Name	*DEF_WAN_ACK_Q*
Guaranteed bandwidth	5 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	5 Mbit/s
Max rev.	unlimited

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
⊟ Type: CBQ						
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default LAN Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Creating traffic shapers

A traffic shaper regulates traffic, making it possible to set the maximum usable bandwidth on a QoS-enabled interface.

IMPORTANT

- The value of the traffic shaper must not exceed 90% of the maximum bandwidth on the link attached to the interface in order for QoS to function.
- QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab.

Understanding the traffic shaper grid

Outgoing bandwidth and incoming bandwidth columns

These columns correspond to:

- **Outgoing bandwidth**: maximum usable bandwidth for outgoing traffic (sending files, for example),
- **Incoming bandwidth**: maximum usable bandwidth for incoming traffic (download of files hosted on the WAN by a client located on the LAN, for example).

Creating the traffic shaper for the *LAN* interface

1. Click on **Add**.
2. Name the traffic shaper (*TS_LAN* in this example).
3. In the **Outgoing bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *LAN* in (900 [Mbit/s] in this example).
4. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
5. In the **Incoming bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *LAN* in (900 [Mbit/s] in this example).
6. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
7. Confirm by clicking on **Apply**.

Creating the traffic shaper for the *WAN* interface

Follow the steps explained in the procedure Creating the traffic shaper for the *LAN* interface with the following values:

Name	*TS_WAN*
Outgoing bandwidth	90
Unit	Mbits
Incoming bandwidth	90
Unit	Mbits

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

Enter a filter | + Add | × Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits

Configuring QoS on the *LAN* and *WAN* interfaces

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab, **Interfaces with QoS** grid.

This phase of the configuration involves associating the following with each QoS-enabled interface:

- A traffic shaper,
- A default queue: any traffic that does not have a defined QoS queue in the filter rule that applies to such traffic will join this queue.
- A default acknowledgment queue.

Configuring QoS on the *LAN* interface

1. Click on **Add**.
2. Select the *LAN* interface.

3. Select the **Traffic shaper** for this interface (*TS_LAN* in this example).
4. Select the **Default queue** for this interface (*DEF_LAN_Q* in this example).
5. Select the **Default ACK queue** (*DEF_LAN_ACK_Q* in this example).
6. Confirm by clicking on **Apply**.

Configuring QoS on the *WAN* interface

Follow the steps explained in the section Configuring QoS on the LAN interface, using the following values:

Interface	*WAN*
Traffic shaper	*TS_WAN*
Default queue	*DEF_WAN_Q*
Default ACK queue	*DEF_WAN_ACK_Q*

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:

INTERFACES WITH QOS

Enter a filter | Select all | + Add | × Delete

Interface	Traffic shaper	Default queue	Default ACK queue
in	TS_LAN	DEF_LAN_Q	ACK_Q
out	TS_WAN	DEF_WAN_Q	ACK_Q

VLANs attached to an interface

If one or several VLANs are attached to a physical interface (*LAN* interface in this example), the following must be assigned to each VLAN interface:

- The traffic shaper of the parent interface (*TS_LAN* in this example),
- A default queue: this is a queue specific to the VLAN (if a bandwidth guarantee is ever needed for this VLAN) or queue for the parent interface (*DEF_LAN_Q* in this example),
- The default acknowledgment (ACK) queue of the parent interface (*DEF_LAN_ACK_Q* in this example).

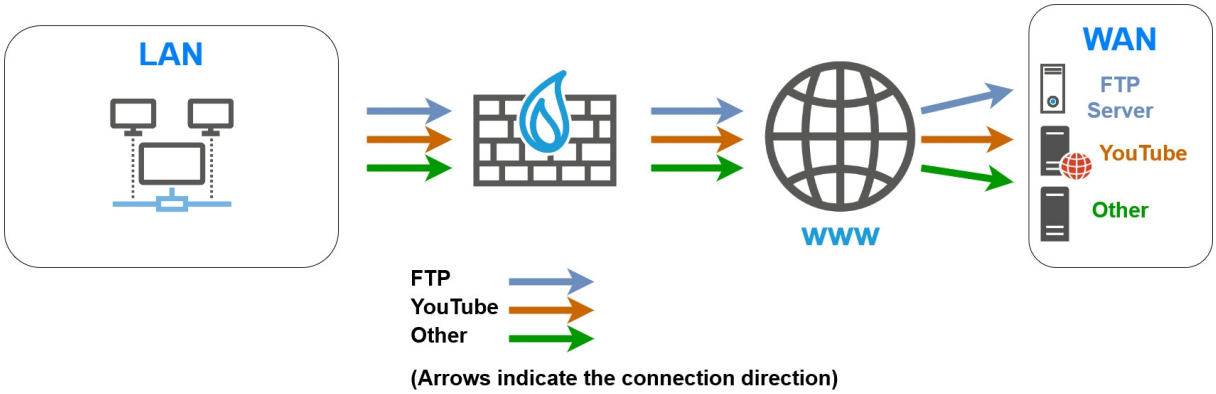
Similarly to physical interfaces, ensure that the total amount of bandwidth reserved for VLANs does not exceed the value of the traffic shaper.

Application: limiting bandwidth in a LAN/WAN architecture

For this section, it is assumed that the user already has the lowest configuration required to apply QoS in a LAN/WAN architecture.

This section also explains how to add the components needed in order to apply bandwidth limitation or reservation to some traffic passing through the links attached to the *LAN* and *WAN* interfaces.

Details of the traffic management policy set up by the administrator are shown below.



Limiting and reserving bandwidth over the WAN link

> **NOTE**
> The sum of all bandwidth reserved for a link must not exceed 85% of the link's total bandwidth. This is because the usable bandwidth for such reservations is equal to the bandwidth assigned to the corresponding traffic shaper (90% of total bandwidth) minus the bandwidth assigned to the acknowledgment queue (5% of total bandwidth).

Transferring work files (FTP)

Set a queue named *FTP_WAN_Q*:

- Limitation to 30 Mbit/s for outgoing traffic,
- Limitation to 40 Mbit/s for return traffic.

Limitation of *YouTube* traffic when the intrusion prevention engine detects a signature

To restrict specific traffic that the intrusion prevention engine detects (*YouTube* in this example), the method used is to apply a specific QoS queue *(YTB_WAN_Q* in this example) to the corresponding detection signature (**Applications and protections** module - "Multimedia: YouTube" signature in this example).

Set a queue named *YTB_WAN_Q*:

- Limitation to 20 Mbit/s for outgoing traffic,
- Limitation to 20 Mbit/s for return traffic.

Creating queues for FTP and YouTube traffic

Go to **Security policy** > **Quality of service** > **Queues** tab.

Creating the queue for FTP traffic

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
3. Name the queue (*FTP_WAN_Q* in this example).
4. In the **Guaranteed bandwidth** line, select **None** in the first field.
5. In the **Max bandwidth** line, specify 30 Mbit/s.
6. In the **Guaranteed rev.** line, select **None** in the first field.
7. In the **Max rev.** line, specify 40 Mbit/s.
8. Confirm by clicking on **Apply**.

Creating the queue for YouTube traffic

1. Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example.

Name	*YTB_WAN_Q*
Guaranteed bandwidth	*None*
Max bandwidth	20 Mbit/s
Guaranteed rev.	*None*
Max rev.	20 Mbit/s

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
⊟ Type: CBQ						
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default LAN Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN Queue
FTP_WAN_Q	CBQ	None	30 Mbits	None	40 Mbits	File transfer Queue
YT_WAN_Q	CBQ	None	20 Mbits	None	20 Mbits	YouTube Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Traffic shapers

For this example, it is assumed that the traffic shapers of the *LAN* and *WAN* interfaces already exist and were created as described in the section Lowest configuration required to apply QoS: example of a LAN/WAN architecture.

IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

Enter a filter | + Add | × Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits

Configuring the interfaces on which QoS has been enabled

For this example, it is assumed that the QoS-enabled interfaces (*LAN* and *WAN* interfaces) have been configured as described in the section Lowest configuration required to apply QoS: example of a LAN/WAN architecture.

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:

INTERFACES WITH QOS

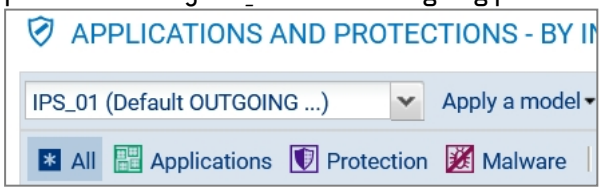
Enter a filter | Select all | + Add | × Delete

Interface	Traffic shaper	Default queue	Default ACK queue
in	TS_LAN	DEF_LAN_Q	ACK_Q
out	TS_WAN	DEF_WAN_Q	ACK_Q

Applying a QoS queue to the YouTube application signature

Go to **Application protection** > **Applications and protections**.

1. In the drop-down list at the top left side of the action bar, select the outgoing inspection profile to modify: *IPS_01* default outgoing profile in this example:



2. In the search field, type a series of characters found in the name of the YouTube application.
3. Select the line in the signature to which you want to apply a QoS queue (signature "Multimedia: YouTube" in this example).
   A **Configure** menu appears in the **Advanced** column.
4. Click on **Configure**.
   A configuration window will open.
5. In the field **QoS applied to traffic**, select the queue reserved for YouTube traffic (*YTB_WAN_Q* in this example).
6. Confirm the change by clicking on **Apply**.
7. Click on **Apply** then on **Save**.

Creating filter rules

> **NOTE**
> This section describes the process of creating filter rules that use specific QoS queues instead of default queues. This technical note will not cover the creation of filter rules for traffic other than from the LAN to the WAN or DMZ.

Go to **Security policy** > **Filter - NAT** > **Filtering** tab.

Creating the filter rule for the FTP protocol

1. In the drop-down list above the filter rule grid, select the security policy that you want to modify.
2. Select the rule above which you want to add a new filter rule.
3. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
4. Double-click on this rule.
   The configuration window of the rule opens.
5. Click on the **General** menu on the left.
6. In the **Status** field, set the value to *On*.
7. Click on the **Action** menu on the left.
8. In the **General** tab, for the **Action** field, select *pass*.
9. In the **Quality of service** tab, for the **Queue** field, select the queue created for FTP traffic to the WAN (*FTP_WAN_Q* in this example).
10. Click on the **Source** menu on the left.
11. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to use the FTP protocol (*LAN_Clients* network in this example).
12. Click on the **Destination** menu on the left.
13. In the **General** tab, for the **Destination hosts** field, click on **Add** and select the FTP server or server group (*WAN_FTP_Server* host in this example).
14. Click on the **Port - Protocol** menu on the left.
15. In the **Port** section, for the **Destination port**, select the *ftp* object.
16. Confirm the creation of the rule by clicking on **OK**.

> **NOTE**
> For protocols that generate child connections (FTP in this example), the queue specified in the filter rule automatically applies to child connections.

Creating the filter rule for YouTube

Follow the steps explained in the procedure Creating the filter rule for the FTP protocol with the following values for this example.#Règle

Status	*on*

Action	*pass*
Queue	Leave the value suggested by default (*Default queue*). When the intrusion prevention engine detects the YouTube application signature, it will assign the appropriate queue (*YTB_WAN_Q* in this example) to traffic affected by this rule.
Source hosts	*LAN_Clients*
Destination hosts	*Internet*
Destination port	*https*

Applying the modified security policy

To confirm changes and apply the new security policy, click on **Apply**, then on **Yes, activate the policy**.

The filter rules that use specific QoS queues will therefore look like this:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	LAN_Clients	WAN_FTP_Server	ftp		IPS
on	pass	LAN_Clients	Internet	https		IPS

Lowest configuration required to apply QoS in a LAN/WAN/DMZ architecture

For this section, it is assumed that the user already has the lowest configuration required to apply QoS in a LAN/WAN architecture. This section also explains how to add the components needed in order to apply QoS to traffic flowing to the DMZ.

Creating queues for the *DMZ* interface

Go to **Security policy** > **Quality of service** > **Queues** tab.

Creating the default queue for the *DMZ* interface

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
3. Name the queue (*DEF_DMZ_Q* in this example).
4. In the **Guaranteed bandwidth** line, indicate the desired value for bandwidth reservation (100 Mbit/s in this example).
5. In the **Max bandwidth** line, leave the value suggested by default (10 Gbit/s).
6. In the **Guaranteed rev.** line, indicate the desired value for bandwidth reservation (100 Mbit/s in this example).
7. In the **Max rev.** line, leave the value suggested by default (10 Gbit/s).
8. Confirm by clicking on **Apply**.

Creating the acknowledgment (ACK) queue for the *DMZ* interface

In this example, the link connected to the *DMZ* interface displays maximum bandwidth of 1 Gbit/s: the acknowledgment (ACK) queue will therefore be 50 Mbit/s (reservation equivalent to 5% of the link's maximum bandwidth).

1. Follow the steps explained in the procedure Creating the default queue for the *DMZ* interface with the following values:

Queue type	Class Based Queuing
Name	*DEF_DMZ_ACK_Q*
Guaranteed bandwidth	50 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	50 Mbit/s
Max rev.	unlimited

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
Type: CBQ						
DEF_DMZ_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default DMZ ACK Queue
DEF_DMZ_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default DMZ Queue
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default LAN Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Creating the traffic shaper for the *DMZ* interface

IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab:

1. Click on **Add**.
2. Name the traffic shaper (*TS_DMZ* in this example).
3. In the **Outgoing bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *DMZ* in (900 [Mbit/s] in this example).
4. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
5. In the **Incoming bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *DMZ* in (900 [Mbit/s] in this example).
6. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
7. Confirm the creation of the traffic shaper by clicking on **Apply**.
8. Confirm by clicking on **Apply**.

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

Enter a filter | + Add | Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits
TS_DMZ	900	Mbits	900	Mbits

Configuring QoS on the *DMZ* interface

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab, **Interfaces with QoS** grid:

1. Click on **Add**.
2. Select the *DMZ* interface.
3. Select the **Traffic shaper** for this interface (*TS_DMZ* in this example).
4. Select the **Default queue** for this interface (*DEF_DMZ_Q* in this example).
5. Select the **Default ACK queue** (*DEF_DMZ_ACK_Q* in this example).

6. Confirm the QoS configuration on the *DMZ* interface by clicking on **Apply**.
7. Confirm by clicking on **Apply**.

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:

INTERFACES WITH QOS

Enter a filter | Select all | + Add | × Delete

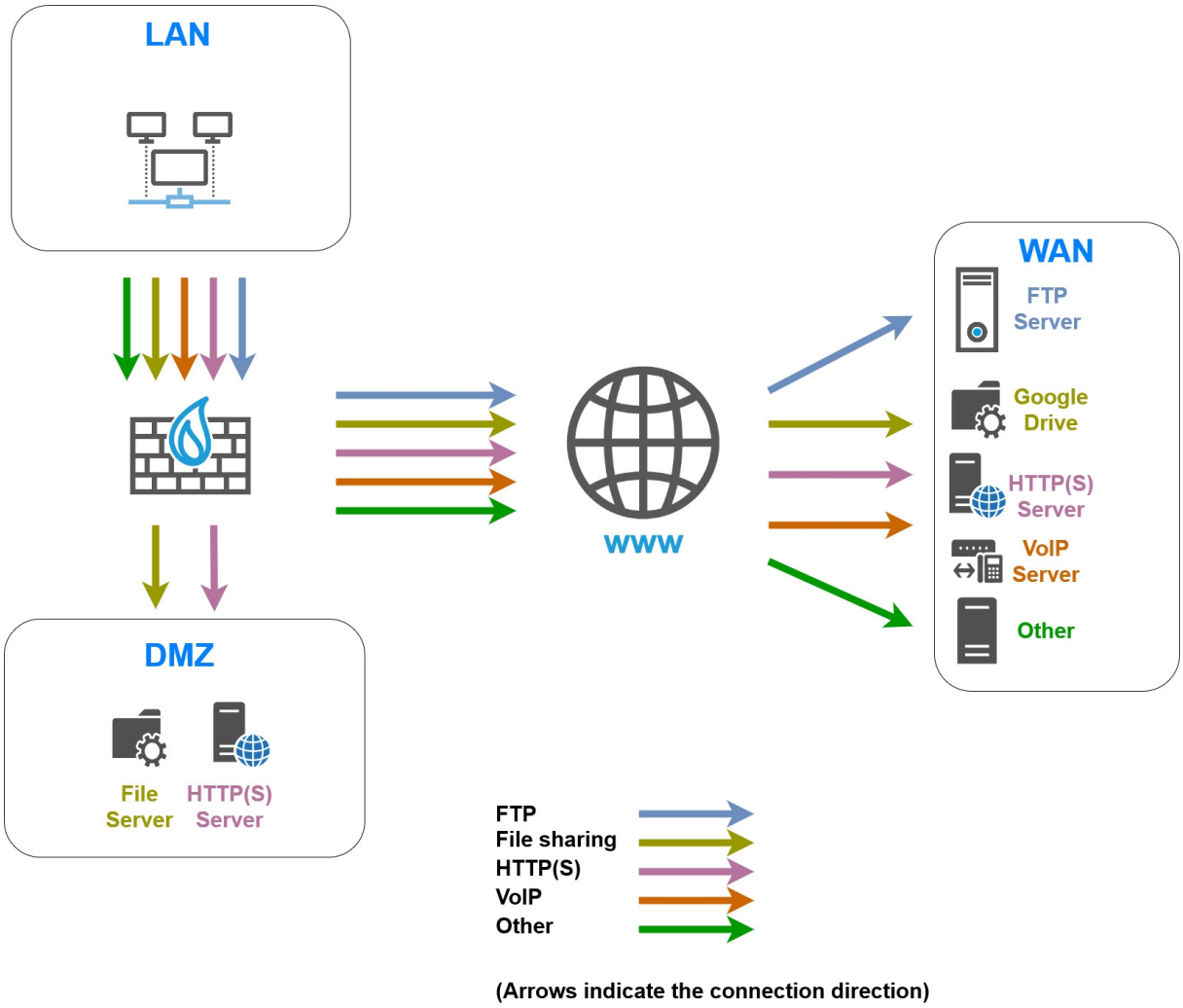
Interface	Traffic shaper	Default queue	Default ACK queue
DMZ	TS_DMZ	DEF_DMZ_Q	DEF_DMZ_ACK_Q
LAN	TS_LAN	DEF_LAN_Q	DEF_LAN_ACK_Q
WAN	TS_WAN	DEF_WAN_Q	DEF_WAN_ACK_Q

Application: limiting and reserving bandwidth in a LAN/WAN/DMZ architecture

For this example, it is assumed that the user already has the **lowest configuration required to apply QoS in a LAN/WAN/DMZ architecture**.

This example also explains how to add the components needed in order to apply bandwidth reservation or limitation to some traffic passing through the links attached to the *LAN*, *WAN and DMZ* interfaces.

Details of the traffic management policy set up by the administrator are shown below.



Limiting and reserving bandwidth over the WAN link

NOTE
The sum of all bandwidth reserved for a link must not exceed 85% of the link's total bandwidth. This is because the usable bandwidth for such reservations is equal to the bandwidth assigned to the corresponding traffic shaper (90% of total bandwidth) minus the bandwidth assigned to the acknowledgment queue (5% of total bandwidth).

Transferring work files (FTP)

Set a queue named *FTP_WAN_Q*:

- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for outgoing traffic,
- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for return traffic.

Hosting and sharing files over external servers (e.g., Google Drive)

A queue named *GD_WAN_Q* will be used in this example:

- Reservation of 10 Mbit/s and no limitation for outgoing traffic,
- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for return traffic.

> **NOTE**
> This queue will be used in a filter rule going to the Google Drive web service.
> This predefined object gathers all the known IP addresses and FQDNs of Google Drive services.
> It is automatically updated via the firewall's Active Update service.

Transferring HTTP/HTTPS files to and from the external work server

Set a queue named *HTTP_WAN_Q*:

- Reservation of 40 Mbit/s and no limitation for outgoing traffic,
- Reservation of 40 Mbit/s and no limitation for outgoing traffic.

VoIP communications (SIP)

Set a queue named *SIP_WAN_Q*:

- Reservation of 15 Mbit/s and no limitation for outgoing traffic,
- Reservation of 15 Mbit/s and no limitation for outgoing traffic.

Reserving bandwidth over the DMZ link

Transferring HTTP/HTTPS files to and from the local work server

Set a queue named *HTTP_DMZ_Q*:

- Reservation of 600 Mbit/s and no limitation for outgoing traffic,
- Reservation of 600 Mbit/s and no limitation for outgoing traffic.

Sharing files over a server

Set a queue named *SMB_DMZ_Q*:

- Reservation of 100 Mbit/s and no limitation for outgoing traffic,
- Reservation of 100 Mbit/s and no limitation for outgoing traffic.

Creating queues

For this example, it is assumed that the default acknowledgment (ACK) queues and default queues for the *LAN*, *WAN* and *DMZ* interfaces already exist and were created as described in the section Lowest configuration required to apply QoS in a LAN/WAN/DMZ architecture.

Go to **Security policy** > **Quality of service** > **Queues** tab.

Creating queues for the *WAN* interface

Creating the queue for FTP traffic

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
3. Name the queue (*FTP_WAN_Q* in this example).
4. In the **Guaranteed bandwidth** line, specify 10 Mbit/s.
5. In the **Max bandwidth** line, specify 20 Mbit/s.
6. In the **Guaranteed rev.** line, specify 10 Mbit/s.
7. In the **Max rev.** line, specify 20 Mbit/s.
8. Confirm by clicking on **Apply**.

Creating the queue for the file share

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example:

Queue type	Class Based Queuing
Name	*GD_WAN_Q*
Guaranteed bandwidth	10 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	10 Mbit/s
Max rev.	20 Mbit/s

Creating the queue for HTTP/HTTPS work traffic

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example:

Queue type	Class Based Queuing
Name	*HTTP_WAN_Q*
Guaranteed bandwidth	40 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	40 Mbit/s
Max rev.	unlimited

Creating the queue for VoIP traffic (SIP)

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example:

Queue type	Class Based Queuing
Name	*SIP_WAN_Q*
Guaranteed bandwidth	15 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	15 Mbit/s
Max rev.	unlimited

Creating queues for the *DMZ* interface

Creating the queue for HTTP/HTTPS work traffic

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example:

Queue type	Class Based Queuing
Name	*HTTP_DMZ_Q*
Guaranteed bandwidth	600 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	600 Mbit/s
Max rev.	unlimited

Creating the queue for the file share

1. Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example:

Queue type	Class Based Queuing
Name	*SMB_DMZ_Q*
Guaranteed bandwidth	100 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	100 Mbit/s
Max rev.	unlimited

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
⊟ Type: CBQ						
DEF_DMZ_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default DMZ ACK Queue
DEF_DMZ_Q	CBQ	100 Mbits	unlimited	100 Mbits	unlimited	Default DMZ Queue
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	None	10 Gbits	None	10 Gbits	Default LAN Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	unlimited	10 Mbits	unlimited	Default WAN Queue
FTP_WAN_Q	CBQ	10 Mbits	20 Mbits	10 Mbits	20 Mbits	File transfer Queue
HTTP_DMZ_Q	CBQ	600 Mbits	unlimited	600 Mbits	unlimited	Local Production Queue
HTTP_WAN_Q	CBQ	40 Mbits	unlimited	40 Mbits	unlimited	Remote Production Queue
MOD_WAN_Q	CBQ	10 Mbits	unlimited	10 Mbits	20 Mbits	Microsoft OneDrive Queue
SIP_WAN_Q	CBQ	15 Mbits	unlimited	15 Mbits	unlimited	VoIP Queue
SMB_DMZ_Q	CBQ	100 Mbits	unlimited	100 Mbits	unlimited	Local File Sharing Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Traffic shapers

For this example, it is assumed that the traffic shapers of the *LAN*, *WAN* and *DMZ* interfaces already exist and were created as described in the section Lowest configuration required to apply QoS in a LAN/WAN/DMZ architecture.

IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

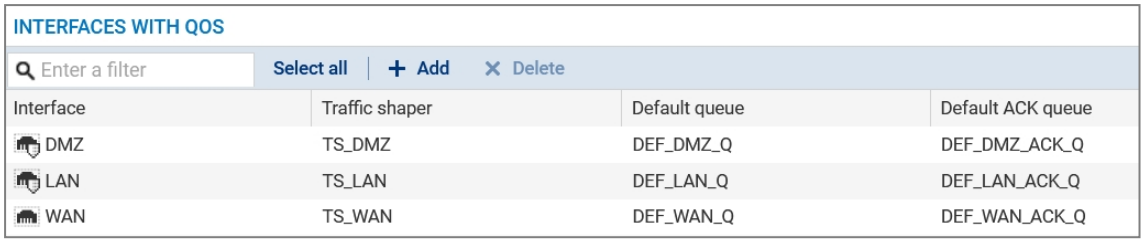
Enter a filter | + Add | Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits
TS_DMZ	900	Mbits	900	Mbits

Configuring QoS on the *LAN*, *WAN* and *DMZ* interfaces

For this example, it is assumed that the interfaces on which QoS has been enabled (*LAN, WAN* and *DMZ* interfaces) were configured as described in the sections Lowest configuration required to apply QoS in a LAN/WAN architecture and Creating the lowest configuration required to apply QoS in a LAN/WAN/DMZ architecture.

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:



Creating filter rules

NOTE
This section describes the process of creating filter rules that use specific QoS queues instead of default queues. This technical note will not cover the creation of filter rules for traffic other than from the LAN to the WAN or DMZ.

NOTE
We advise against specifying acknowledgment (ACK) queues in filter rules.
It is in fact preferable to let ACK traffic automatically join the acknowledgment (ACK) queues set by default on the relevant interfaces for such traffic.

Go to **Security policy** > **Filter - NAT** > **Filtering** tab.

Creating the filter rule to the remote FTP server

1. In the drop-down list above the filter rule grid, select the security policy that you want to modify.
2. Select the rule above which you want to add a new filter rule.
3. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
4. Double-click on this rule.
   The configuration window of the rule opens.
5. Click on the **General** menu on the left.
6. In the **Status** field, set the value to *On*.
7. Click on the **Action** menu on the left.
8. In the **General** tab, for the **Action** field, select *pass*.
9. In the **Quality of service** tab, for the **Queue** field in the **QoS** section: select the queue created for FTP traffic (*FTP_WAN_Q* in this example).
10. Click on the **Source** menu on the left.
11. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to use the FTP protocol (*LAN_Clients* network in this example).
12. Click on the **Destination** menu on the left.
13. In the **General** tab, for the **Destination hosts** field, click on **Add** and select the FTP server or server group (*WAN_FTP_Server* host in this example).
14. Click on the **Port - Protocol** menu on the left.

15. In the **Port** section, select the *ftp* object as the **Destination port**.
16. Confirm the creation of the rule by clicking on **OK**.

> **NOTE**
> For protocols that generate child connections (FTP in this example), the queue specified in the filter rule automatically applies to child connections.

Creating the filter rule for traffic to Google Drive servers

1. Select the rule above which you want to add a new filter rule.
2. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
3. Double-click on this rule.
   The configuration window of the rule opens.
4. Click on the **General** menu on the left.
5. In the **Status** field, set the value to *On*.
6. Click on the **Action** menu on the left.
7. In the **General** tab, for the **Action** field, select *pass*.
8. In the **Quality of service** tab, for the **Queue** field in the **QoS** section, select the queue created for Google Drive traffic (*GD_WAN_Q* in this example).
9. Click on the **Source** menu on the left.
10. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to access Google Drive (*LAN_Clients* network in this example).
11. Click on the **Destination** menu on the left.
12. In the **Web services and reputations** section, under the **Geolocation/Reputation** tab, select the *Google Drive* object.
13. Click on the **Port - Protocol** menu on the left.
14. In the **Port** section, select the *https* object as the **Destination port**.
15. Confirm the creation of the rule by clicking on **OK**.

Creating the filter rule to the remote HTTP/HTTPS server

Follow the steps explained in the procedure Creating the filter rule to the remote FTP server with the following values for this example.#Règle

Status	*on*
Action	*pass*
Queue	*HTTP_WAN_Q*
Source hosts	*LAN_Clients*
Destination hosts	the object corresponding to the remote HTTP/HTTPS server (*WAN_PROD_Server* in this example)
Destination port	the *http* and *https* objects

Creating the filter rule to the remote VoIP server

Follow the steps explained in the procedure Creating the filter rule to the remote FTP server with the following values for this example.#Règle

Status	*on*
Action	*pass*
Queue	*SIP_WAN_Q*
Source hosts	*LAN_VoIP_Clients*
Destination hosts	the object corresponding to the remote SIP server (*WAN_VoIP_Server* in this example)
Destination port	the *sip* object

NOTE
For protocols that generate child connections (SIP in this example), the queue specified in the filter rule automatically applies to child connections.

Creating the filter rule to the HTTP/HTTPS server in the DMZ

Follow the steps explained in the procedure Creating the filter rule to the remote FTP server with the following values.#Règle

Status	*on*
Action	*pass*
Queue	*HTTP_DMZ_Q*
Source hosts	*LAN_Clients*
Destination hosts	the object corresponding to the remote HTTP/HTTPS server (*LOCAL_PROD_Server* in this example)
Destination port	the *http* and *https* objects

Creating the filter rule to the file server in the DMZ

Follow the steps explained in the procedure Creating the filter rule to the remote FTP server with the following values for this example.#Règle

Status	*on*
Action	*pass*
Queue	*SMB_DMZ_Q*
Source hosts	*LAN_Clients*
Destination hosts	the object corresponding to the local file server (*LOCAL_FILE_Server* in this example)
Destination port	the *microsoft-ds* object

Applying the modified security policy

To confirm changes and apply the new security policy, click on **Apply**, then on **Yes, activate the policy**.

The filter rules that use specific QoS queues will therefore look like this:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	LAN_Clients	WAN_FTP_Server	ftp		IPS
on	pass	LAN_Clients	Any Web services and reput Google Drive	https		IPS
on	pass	LAN_Clients	WAN_PROD_Serve	http https		IPS
on	pass	LAN_VoIP_Clients	WAN_VoIP_Server	sip		IPS
on	pass	LAN_Clients	LOCAL_PROD_Ser	http https		IPS
on	pass	LAN_Clients	LOCAL_FILE_Serv	microsoft-ds		IPS

Lowest configuration required to apply QoS in a LAN/WAN/WAN2 architecture

For this section, it is assumed that the user already has the lowest configuration required to apply QoS in a LAN/WAN architecture. This section also explains how to add the components needed in order to apply QoS to traffic flowing to the second WAN2 access link (bandwidth in this example: 100 Mbit/s).

QoS-enabled traffic balanced between two WAN access links is fully compatible with all the following routing methods:

- Static routing,
- Dynamic routing,
- PBR (policy-based routing),
- Use of router objects, with or without load balancing.

Creating queues

Go to **Security policy** > **Quality of service** > **Queues** tab.

Creating the default queue for the *WAN2* interface

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
3. Name the queue (*DEF_WAN2_Q* in this example).
4. In the **Guaranteed bandwidth** line, indicate the desired value for bandwidth reservation (10 Mbit/s in this example).
5. In the **Max bandwidth** line, leave the value suggested by default (10 Gbit/s).
6. In the **Guaranteed rev.** line, indicate the desired value for bandwidth reservation (10 Mbit/s in this example).
7. In the **Max rev.** line, leave the value suggested by default (10 Gbit/s).
8. Confirm by clicking on **Apply**.

NOTE
In configurations that use IPsec traffic, such traffic will automatically join the default queue for the WAN2 interface. This is why class-based queuing is applied to this queue.
Please note that the application of QoS to IPsec traffic is not covered in this Technical Note.

Creating the acknowledgment (ACK) queue for the *WAN2* interface

In this example, the link connected to the *WAN2* interface displays maximum bandwidth of 100 Mbit/s: the acknowledgment (ACK) queue will therefore be 5 Mbit/s (reservation equivalent to 5% of the link's maximum bandwidth).

1. Follow the steps explained in the procedure Creating the default queue for the *WAN2* interface with the following values:

Queue type	Class Based Queuing
Name	*DEF_WAN2_ACK_Q*
Guaranteed bandwidth	5 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	5 Mbit/s
Max rev.	unlimited

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
⊟ Type: CBQ						
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default LAN Queue
DEF_WAN2_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN2 ACK Queue
DEF_WAN2_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN2 Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Creating the traffic shaper for the *WAN2* interface

IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab:

1. Click on **Add**.
2. Name the traffic shaper (*TS_WAN2* in this example).
3. In the **Outgoing bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *DMZ* in (90 [Mbit/s] in this example).
4. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
5. In the **Incoming bandwidth** column, enter the value corresponding to 90% of the bandwidth on the link attached to the *DMZ* in (90 [Mbit/s] in this example).
6. In the **Unit** column, indicate the bandwidth unit (Mbit/s in this example).
7. Confirm the creation of the traffic shaper by clicking on **Apply**.
8. Confirm by clicking on **Apply**.

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

Enter a filter | + Add | × Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits
TS_WAN2	90	Mbits	90	Mbits

Configuring QoS on the *WAN2* interface

Go to **Security policy** > **Quality of service** > **Traffic shaper** tab.

Configuring QoS on the *WAN2* interface

1. Click on **Add**.
2. Select the *WAN2* interface.
3. Select the **Traffic shaper** for this interface (*TS_WAN2* in this example).
4. Select the **Default queue** for this interface (*DEF_WAN2_Q* in this example).
5. Select the **Default ACK queue** (*DEF_WAN2_ACK_Q* in this example).
6. Confirm the QoS configuration on the *WAN2* interface by clicking on **Apply**.
7. Click on **Apply**.

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:

INTERFACES WITH QOS

Enter a filter | Select all | + Add | × Delete

Interface	Traffic shaper	Default queue	Default ACK queue
WAN2	TS_WAN2	DEF_WAN2_Q	DEF_WAN2_ACK_Q
LAN	TS_LAN	DEF_LAN_Q	DEF_LAN_ACK_Q
WAN	TS_WAN	DEF_WAN_Q	DEF_WAN_ACK_Q

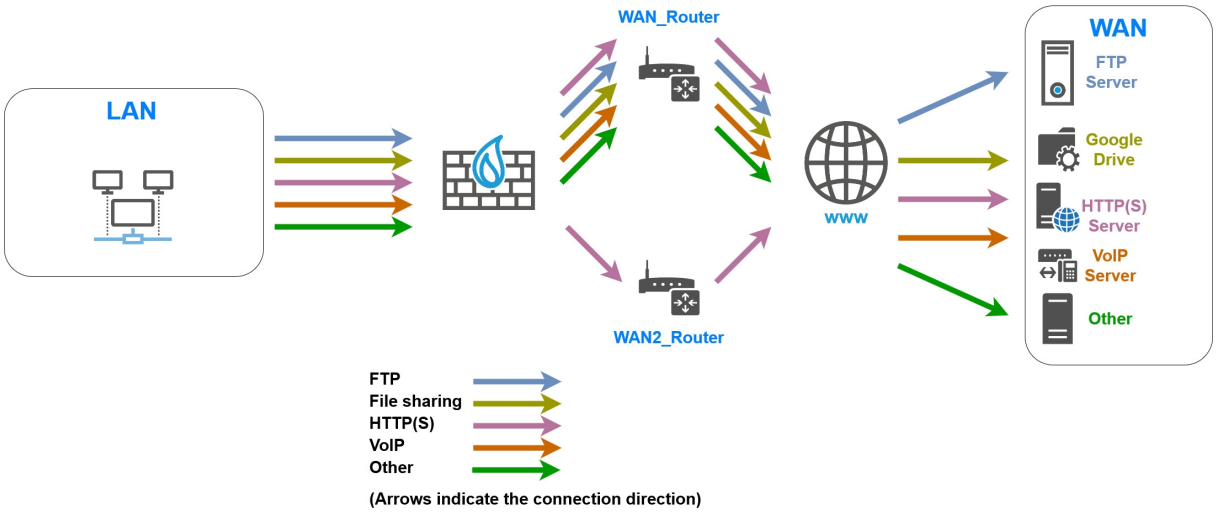
Application: limiting and reserving bandwidth in a LAN/WAN/WAN2 architecture

For this example, it is assumed that the user already has the **lowest configuration required to apply QoS in a LAN/WAN/WAN2 architecture**.

This example also explains how to add the components needed in order to apply bandwidth limitation or reservation to some traffic passing through the links attached to the *LAN*, *WAN and WAN2* interfaces.

In this example, HTTP/HTTPS traffic is balanced between the WAN and WAN2 access links through policy-based routing (PBR) which relies on a router object with load balancing.

Details of the traffic management policy set up by the administrator are shown below.



Limiting and reserving bandwidth over the WAN link

NOTE
The sum of all bandwidth reserved for a link must not exceed 85% of the link's total bandwidth. This is because the usable bandwidth for such reservations is equal to the bandwidth assigned to the corresponding traffic shaper (90% of total bandwidth) minus the bandwidth assigned to the acknowledgment queue (5% of total bandwidth).

Transferring work files (FTP)

Set a queue named *FTP_WAN_Q*:

- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for outgoing traffic,
- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for return traffic.

Sharing files over an external server (e.g., Google Drive)

Set a queue named *GD_WAN_Q*:

- Reservation of 10 Mbit/s and no limitation for outgoing traffic,
- Reservation of 10 Mbit/s and limitation to 20 Mbit/s for return traffic.

VoIP communications and videoconferencing traffic

Set a queue named *SIP_WAN_Q*:

- Reservation of 15 Mbit/s and no limitation for outgoing traffic,
- Reservation of 15 Mbit/s and no limitation for outgoing traffic.

Limiting and reserving bandwidth over the WAN and WAN2 links

Transferring HTTP/HTTPS files to and from the external work server

Set a queue named *HTTP_WAN_Q*:

- Reservation of 40 Mbit/s and no limitation for outgoing traffic,
- Reservation of 40 Mbit/s and no limitation for outgoing traffic.

Creating the router object to use in the HTTP/HTTPS PBR rule

> **NOTE**
> For more information on how to use and configure router objects, refer to the **SNS v4 User Guide** (section Network objects > The various types of objects > Router) and the **Technical Note** SD-WAN - Selecting the best network access.

In this example, WAN and WAN2 links are pinged by using the *ICMP* detection method. These pings are then directed to the server that hosts the service that needs to be reached (*WAN_Prod_Server* in this example).

In **Configuration** > **Objects** > **Network**:

1. Click on **Add**.
   This opens a window to create and edit objects.
2. In the menu on the left, select **Router**.
3. Name the object (e.g., *WAN_WAN2_Router* in this example).

Monitoring

4. For the **Detection method**, select *ICMP*.

> **NOTE**
> If you intend to use a router object for SIP traffic, you are advised to select the **SD-WAN SLA** checkbox and configure the **Latency (ms)**, **Jitter (ms)** and/or the **Packet loss rate (%)** thresholds. For more details, refer to the **Technical note** SD-WAN - Selecting the best the network link.

Gateways

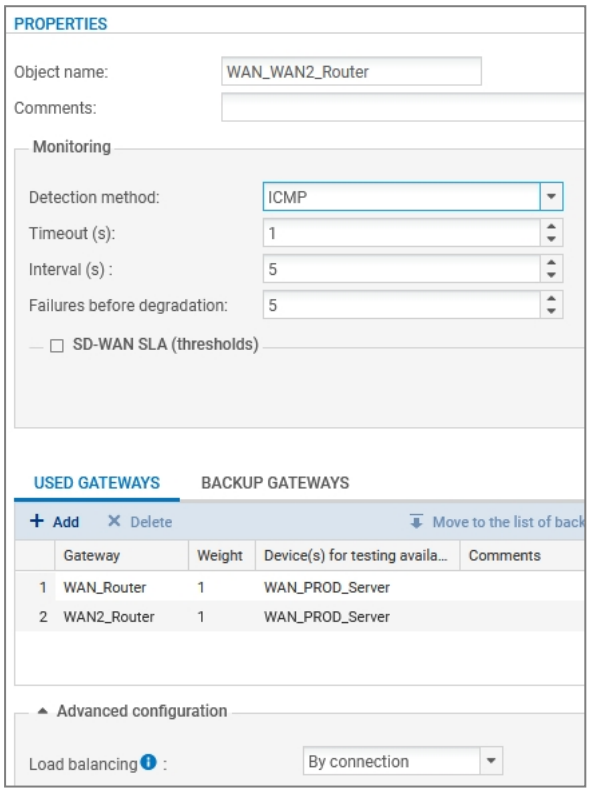
5. In the **Gateways used** tab, click on **Add**.
6. In the **Gateway** column, select the object corresponding to the router of the WAN link (*WAN_Router* in this example).
7. In the **Device(s) for testing availability** column, select the object *WAN_Prod_Server*.
8. Repeat steps 6 to 8 to add the object corresponding to the router of the WAN2 link (*WAN2_Router* in this example).
   The device that will be pinged for this gateway is also the object *WAN_Prod_Server*.

Advanced configuration

To maintain optimal link quality in as many cases as possible, the *WAN_WAN2_Router* router object is configured with load balancing between the links used.

9. In the **Advanced configuration** section, select **Load balancing *By connection*.**
10. Click on **Apply** then **Save**.

The *WAN_WAN2_Router* router object set in this example will therefore look like this:



Creating queues

For this example, it is assumed that the default acknowledgment (ACK) queues and default queues for the *LAN*, *WAN* and *WAN2* interfaces already exist and were created as described in the section Lowest configuration required to apply QoS in a LAN/WAN/WAN2 architecture.

Creating the queue for FTP traffic

Go to **Security policy** > **Quality of service** > **Queues** tab:

1. Click on **Add**.
2. Select **Class Based Queuing (CBQ)**.
3. Name the queue (*FTP_WAN_Q* in this example).
4. In the **Guaranteed bandwidth** line, specify 10 Mbit/s.
5. In the **Max bandwidth** line, specify 20 Mbit/s.
6. In the **Guaranteed rev.** line, specify 10 Mbit/s.
7. In the **Max rev.** line, specify 20 Mbit/s.
8. Confirm by clicking on **Apply**.

Creating the queue for Google Drive

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example.

Queue type	Class Based Queuing
Name	*GD_WAN_Q*
Guaranteed bandwidth	10 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	10 Mbit/s
Max rev.	20 Mbit/s

Creating the queue for HTTP/HTTPS work traffic

Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example.

Queue type	Class Based Queuing
Name	*HTTP_WAN_Q*
Guaranteed bandwidth	40 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	40 Mbit/s
Max rev.	unlimited

Creating the queue for SIP traffic

1. Follow the steps explained in the procedure Creating the queue for FTP traffic with the following values for this example.

Queue type	Class Based Queuing
Name	*SIP_WAN_Q*
Guaranteed bandwidth	15 Mbit/s
Max bandwidth	unlimited
Guaranteed rev.	15 Mbit/s
Max rev.	unlimited

The grid of the QoS queues set in this example will therefore look like this:

QUEUES

Enter a filter | + Add | Delete | Edit selection | Check usage

Name	Type	Guaranteed bandwidth	Max bandwidth	Guaranteed rev.	Max rev.	Comments
⊟ Type: CBQ						
DEF_LAN_ACK_Q	CBQ	50 Mbits	unlimited	50 Mbits	unlimited	Default LAN ACK Queue
DEF_LAN_Q	CBQ	100 Mbits	10 Gbits	100 Mbits	10 Gbits	Default LAN Queue
DEF_WAN2_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN2 ACK Queue
DEF_WAN2_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN2 Queue
DEF_WAN_ACK_Q	CBQ	5 Mbits	unlimited	5 Mbits	unlimited	Default WAN ACK Queue
DEF_WAN_Q	CBQ	10 Mbits	10 Gbits	10 Mbits	10 Gbits	Default WAN Queue
FTP_WAN_Q	CBQ	10 Mbits	20 Mbits	10 Mbits	20 Mbits	File transfer Queue
GD_WAN_Q	CBQ	10 Mbits	unlimited	10 Mbits	20 Mbits	Remote File sharing Queue
HTTP_WAN_Q	CBQ	40 Mbits	unlimited	40 Mbits	unlimited	Remote Production Queue
SIP_WAN_Q	CBQ	15 Mbits	unlimited	15 Mbits	unlimited	VoIP Queue

2. Confirm changes to the QoS configuration by clicking on **Apply**.

Creating traffic shapers

For this example, it is assumed that the traffic shapers of the *LAN*, *WAN* and *WAN2* interfaces already exist and were created as described in the section Creating the lowest configuration required to apply QoS in a LAN/WAN/WAN2 architecture.

IMPORTANT
QoS cannot be implemented on traffic shapers with bandwidth higher than 1 Gbit/s.

The grid of the traffic shapers set in this example will therefore look like this:

TRAFFIC SHAPER

Enter a filter | + Add | Delete

Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits
TS_WAN2	90	Mbits	90	Mbits

Configuring the interfaces on which QoS has been enabled

For this example, it is assumed that the interfaces on which QoS has been enabled (*LAN, WAN* and *WAN2* interfaces) were configured as described in the sections Lowest configuration required to apply QoS in a LAN/WAN architecture and Creating the lowest configuration required to apply QoS in a LAN/WAN/WAN2 architecture.

The grid of the interfaces on which QoS has been enabled in this example will therefore look like this:

INTERFACES WITH QOS

Enter a filter | Select all | + Add | × Delete

Interface	Traffic shaper	Default queue	Default ACK queue
WAN2	TS_WAN2	DEF_WAN2_Q	DEF_WAN2_ACK_Q
LAN	TS_LAN	DEF_LAN_Q	DEF_LAN_ACK_Q
WAN	TS_WAN	DEF_WAN_Q	DEF_WAN_ACK_Q

Creating PBR and filter rules that use QoS queues

NOTE
In this section, only the process of creating PBR and filter rules that use specific QoS queues (instead of default queues) is described. This technical note will not cover the creation of filter rules for traffic on which QoS is not enabled.

NOTE
We advise against specifying acknowledgment (ACK) queues in filter rules.
It is in fact preferable to let ACK traffic automatically join the acknowledgment (ACK) queues set by default on the relevant interfaces for such traffic.

Go to **Security policy** > **Filter - NAT** > **Filtering** tab.

Creating the filter rule to the remote FTP server

1. In the drop-down list above the filter rule grid, select the security policy that you want to modify.
2. Select the rule above which you want to add a new filter rule.
3. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
4. Double-click on this rule.
   The configuration window of the rule opens.
5. Click on the **General** menu on the left.
6. In the **Status** field, set the value to *On*.
7. Click on the **Action** menu on the left.
8. In the **General** tab, for the **Action** field, select *pass*.
9. In the **Quality of service** tab, for the **Queue** field in the **QoS** section, select the queue created for FTP traffic (*FTP_WAN_Q* in this example).
10. Click on the **Source** menu on the left.
11. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to use the FTP protocol (*LAN_Clients* network in this example).
12. Click on the **Destination** menu on the left.
13. In the **General** tab, for the **Destination hosts** field, click on **Add** and select the FTP server or server group (*WAN_FTP_Server* host in this example).
14. Click on the **Port - Protocol** menu on the left.

15. In the **Port** section, select the *ftp* object as the **Destination port**.
16. Confirm the creation of the rule by clicking on **OK**.

> **NOTE**
> For protocols that generate child connections (FTP in this example), the queue specified in the filter rule automatically applies to child connections.

Creating the filter rule to the remote file server

1. Select the rule above which you want to add a new filter rule.
2. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
3. Double-click on this rule.
   The configuration window of the rule opens.
4. Click on the **General** menu on the left.
5. In the **Status** field, set the value to *On*.
6. Click on the **Action** menu on the left.
7. In the **General** tab, for the **Action** field, select *pass*.
8. In the **Quality of service** tab, for the **Queue** field in the **QoS** section, select the queue created for Google Drive traffic (*GD_WAN_Q* in this example).
9. Click on the **Source** menu on the left.
10. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to access Google Drive (*LAN_Clients* network in this example).
11. Click on the **Destination** menu on the left.
12. In the **Web services and reputations** section, under the **Geolocation/Reputation** tab, select the *Google Drive* object.
13. Click on the **Port - Protocol** menu on the left.
14. In the **Port** section, select the *https* object as the **Destination port**.
15. Confirm the creation of the rule by clicking on **OK**.

Creating the PBR rule to the remote HTTP/ HTTP server

1. Select the rule above which you want to add a new filter rule.
2. Click on **New rule** and select **Single rule**.
   A new inactive rule is added to the filter policy.
   You can move this new rule by using the arrows .
3. Double-click on this rule.
   The configuration window of the rule opens.
4. Click on the **General** menu on the left.
5. In the **Status** field, set the value to *On*.
6. Click on the **Action** menu on the left.
   In the **General** tab:
   - In the **General** section, for the **Action** field, select *pass*.
   - In the **Routing** section, for the **Gateway - router** field, select the object *WAN_WAN2_Router*.

7. In the **Quality of service** tab, for the **Queue** field in the **QoS** section, select the queue created for HTTPS/HTTPS traffic (*HTTP_WAN_Q* in this example).
8. Click on the **Source** menu on the left.
9. In the **General** tab, for the **Source hosts** field, select the hosts, host groups or networks allowed to access the remote production server (*LAN_Clients* network in this example).
10. Click on the **Destination** menu on the left.
11. In the **General** tab, for the **Destination hosts** field, click on **Add** and select the object corresponding to the HTTP/HTTPS server (*WAN_PROD_Server* in this example).
12. Click on the **Port - Protocol** menu on the left.
13. In the **Port** section, select the http and *https* objects as the **Destination port**.
14. Confirm the creation of the rule by clicking on **OK**.

Creating the filter rule to the remote VoIP server

Follow the steps explained in the procedure Creating the filter rule to the remote FTP server with the following values for this example.

Status	*on*
Action	*pass*
Queue	*SIP_WAN_Q*
Source hosts	*LAN_VoIP_Clients*
Destination hosts	the object corresponding to the remote VoIP server (*WAN_VoIP_Server* in this example)
Destination port	the *sip* object

NOTE
For protocols that generate child connections (SIP in this example), the queue specified in the filter rule automatically applies to child connections.

Applying the modified security policy

To apply the new security policy, click on **Apply**, then on **Yes, activate the policy**.

The PBR and filter rules that use QoS queues will therefore look like this:

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
on	pass	LAN_Clients	WAN_FTP_Server	ftp		IPS
on	pass	LAN_Clients	Any Web services and reputa Google Drive	https		IPS
on	pass Route: WAN_WAN2	LAN_Clients	WAN_PROD_Server	http https		IPS
on	pass	LAN_VoIP_Clients	WAN_VoIP_Server	sip		IPS

Monitoring QoS

The web administration interface allows the user to view in graphs the amount of bandwidth used by queues defined on your SNS firewall.

Configuring monitoring

Go to **Configuration > Notifications > Monitoring configuration, QoS configuration** tab.

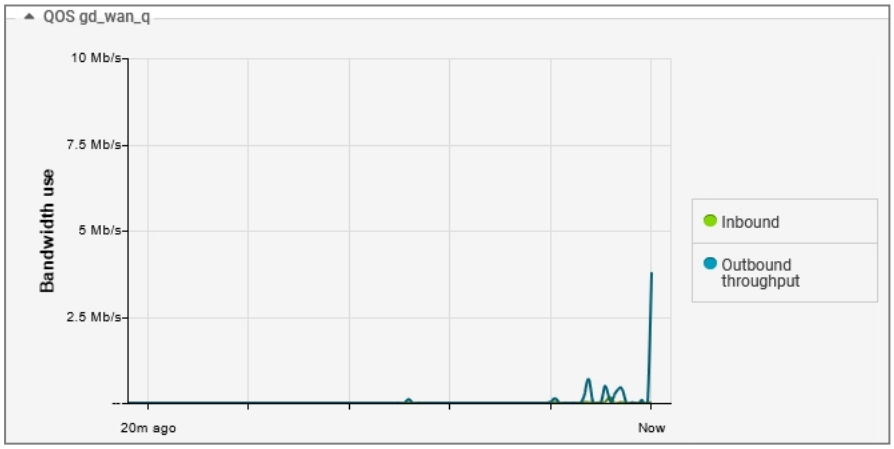
1. Click on **Add**.
2. Select the queue that you wish to monitor.
3. Repeat steps 1 and 2 for all queues that you want to monitor.
4. Click on **Apply**.

Viewing graphs of bandwidth used by QoS queues

Go to **Monitoring** > **Monitoring** > **QoS**.

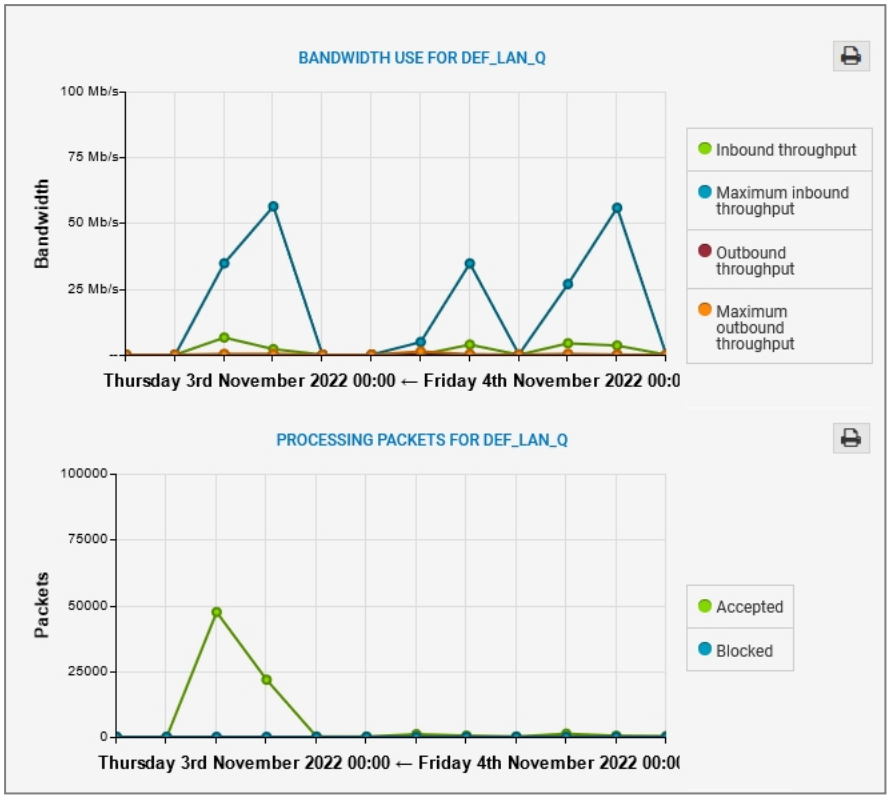
Real time tab

The **Real time** tab displays a graph showing bandwidth use for each monitored QoS queue. These graphs are refreshed in real time:



History tab

The **History** tab displays an aggregate of bandwidth usage data and packet processing data for each monitored QoS queue:



The toolbar can be used to select the period represented:

- Last hour,
- A particular day,
- Last 7 days,
- Last 30 days.

Further reading

Additional information and responses to questions you may have about high availability are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu