



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER LA QOS SUR LES FIREWALLS SNS

Produits concernés : SNS 4.3.15 et versions supérieures de la branche 4.3, SNS 4.5.3 et versions supérieures

Dernière mise à jour du document : 2 février 2023

Référence : [sns-fr-configurer-la-qos-sur-les-firewalls-SNS-note_technique](#)



Table des matières

Avant de commencer	5
La Qualité de service (QoS, Quality of service) et ses composants	5
Mécanisme de régulation : différence de comportement entre flux TCP et flux UDP	5
Les files d'attente de QoS	6
Illustration du principe général de la QoS	7
Application de QoS à un trafic réseau LAN / WAN	7
Interfaces incompatibles avec la QoS	7
Utilisation au travers du proxy SSL	8
Bonnes pratiques	8
Précautions de mise en œuvre	8
Limites et caractères autorisés dans les noms des files d'attente et des Traffic shapers	9
Files d'attente de QoS	9
Traffic shapers	9
Nommage des interfaces dans cette Note Technique	9
 Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN	 10
Créer les files d'attente par défaut	10
Comprendre la grille des files d'attente	10
Créer les files d'attente par défaut pour les interfaces LAN et WAN	10
Créer les files d'attente d'acquiescement (ACK) pour les interfaces LAN et WAN	11
Créer les Traffic shapers	12
Comprendre la grille des Traffic shapers	13
Créer le Traffic shaper pour l'interface LAN	13
Créer le Traffic shaper pour l'interface WAN	13
Configurer la QoS sur les interfaces LAN et WAN	13
Configurer la QoS sur l'interface LAN	14
Configurer la QoS sur l'interface WAN	14
Cas de VLAN rattachés à une interface	14
 Application : limitation de bande passante dans une architecture de type LAN / WAN ..	 15
Limitation et réservation de bande passante sur le lien WAN	15
Transferts de fichiers métier (FTP)	15
Limitation des flux YouTube sur détection de signature par le moteur de prévention d'intrusion ...	15
Créer les files d'attente pour les flux FTP et YouTube	16
Créer la file d'attente pour les flux FTP	16
Créer la file d'attente pour les flux YouTube	16
Traffic shapers	17
Configurer les interfaces concernées par la QoS	17
Appliquer une file d'attente de QoS à la signature de l'application YouTube	17
Créer les règles de filtrage	18
Créer la règle de filtrage pour le protocole FTP	18
Créer la règle de filtrage pour l'application YouTube	19
Appliquer la politique de sécurité modifiée	19
 Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ	 20
Créer les files d'attente de l'interface DMZ	20
Créer la file d'attente par défaut de l'interface DMZ	20
Créer la file d'attente d'acquiescement (ACK) de l'interface DMZ	20



Créer le Traffic shaper de l'interface DMZ	21
Configurer la QoS sur l'interface DMZ	21
Application : limitation et réservation de bande passante dans une architecture de type LAN / WAN / DMZ	23
Limitation et réservation de bande passante sur le lien WAN	23
Transferts de fichiers métier (FTP)	23
Hébergement et partage de fichiers sur des serveurs externes (exemple : Google Drive)	24
Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier externe	24
Communications en VoIP (SIP)	24
Réservation de bande passante sur le lien DMZ	24
Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier local	24
Partage de fichiers sur un serveur	24
Créer les files d'attente	24
Créer les files d'attente pour l'interface WAN	25
Créer les files d'attente pour l'interface DMZ	26
Traffic shapers	27
Configurer la QoS sur les interfaces LAN, WAN et DMZ	27
Créer les règles de filtrage	28
Créer la règle de filtrage vers le serveur FTP distant	28
Créer la règle de filtrage pour les flux vers les serveurs Google Drive	29
Créer la règle de filtrage vers le serveur HTTP / HTTPS distant	29
Créer la règle de filtrage vers le serveur VoIP distant	30
Créer la règle de filtrage vers le serveur HTTP / HTTPS en DMZ	30
Créer la règle de filtrage vers le serveur de fichiers en DMZ	30
Appliquer la politique de sécurité modifiée	31
Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2	32
Créer les files d'attente	32
Créer la file d'attente par défaut pour l'interface WAN2	32
Créer la file d'attente d'acquittement (ACK) de l'interface WAN2	32
Créer le Traffic shaper pour l'interface WAN2	33
Configurer la QoS sur l'interface WAN2	34
Configurer la QoS sur l'interface WAN2	34
Application : limitation et réservation de bande passante dans une architecture de type LAN / WAN / WAN2	35
Limitation et réservation de bande passante sur le lien WAN	35
Transferts de fichiers métier (FTP)	35
Partage de fichiers sur un serveur externe (exemple : Google Drive)	36
Communications en VoIP et flux de visioconférence	36
Limitation et réservation de bande passante sur les liens WAN et WAN2	36
Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier externe	36
Créer l'objet routeur à utiliser dans la règle de PBR HTTP / HTTPS	36
Créer les files d'attente	37
Créer la file d'attente pour les flux FTP	37
Créer la file d'attente pour le partage de fichiers Google Drive	38
Créer la file d'attente pour les flux métier HTTP / HTTPS	38
Créer la file d'attente pour les flux SIP	38
Créer les Traffic shapers	39
Configurer les interfaces concernées par la QoS	39
Créer les règles de PBR et de filtrage utilisant des files d'attente de QoS	40



Créer la règle de filtrage vers le serveur FTP distant	40
Créer la règle de filtrage vers le serveur de fichiers distant	41
Créer la règle de PBR vers le serveur HTTP / HTTPS distant	41
Créer la règle de filtrage vers le serveur VoIP distant	42
Appliquer la politique de sécurité modifiée	42
Superviser la QoS	44
Configurer la supervision	44
Visualiser les graphes de bande passante utilisée par les files de QoS	44
Onglet Temps réel	44
Onglet Historique	44
Pour aller plus loin	46



Avant de commencer

La Qualité de service (QoS, *Quality of service*) et ses composants

La qualité de service désigne toute technologie capable de gérer la transmission des données, tout en réduisant la perte de paquets, la latence et la gigue pour les flux prioritaires du réseau. Ce concept a pour but de contrôler et de gérer les ressources réseau, en hiérarchisant certains types de données et flux réseau.

Cette gestion des flux peut prendre deux formes :

- La réservation de bande passante pour des flux prioritaires ou à forte contrainte technique (exemple : flux métier, téléphonie sur IP...),
- La limitation de bande passante pour des flux moins prioritaires (exemple : consultation de site Web).

i NOTE

La réservation ou la limitation de bande passante sont appliquées aux flux lorsqu'ils quittent l'interface réseau sur laquelle est appliquée la QoS. Ces mécanismes n'ont donc pas de réel impact sur les flux entrants (cas du téléchargement).

Mécanisme de régulation : différence de comportement entre flux TCP et flux UDP

Quand un flux TCP dépasse la limitation de bande passante définie dans une file d'attente de QoS, le mécanisme de régulation rejette certains de ces paquets TCP et ralentit le flux en sortie de l'interface. L'émetteur du flux TCP perçoit alors que des paquets sont perdus sur le chemin et ralentit le débit jusqu'à atteindre les critères de configuration de QoS du firewall.

Ce mécanisme de régulation n'existant pas pour le trafic UDP, le débit entrant sur l'interface ne s'adaptera jamais à la configuration de QoS et toutes les réservations de bande passante sur l'interface entrante seront perturbées et non-respectées.



Les files d'attente de QoS

Pour réaliser ces opérations de réservation ou de limitation, il est nécessaire de définir des files d'attente qui seront affectées aux interfaces réseau soumises à la QoS.

Les files d'attente possibles sont de 3 types :

- Files d'attente par classe d'application ou d'affectation (CBQ, *Class-Based Queing*) : ces files sont utilisées pour la réservation ou la limitation de bande passante en indiquant les bandes passantes garanties ou maximales à appliquer,
- Files d'attente par priorité (PRIQ, *Priority Queing*) : elles induisent une priorisation des paquets et sont classées de la priorité 0 (flux les plus prioritaires) à la priorité 7 (flux les moins prioritaires).

Les paquets associés à une règle de filtrage utilisant une file PRIQ sont traités avant les paquets qui ne sont pas affectés à une file PRIQ ou qui sont attachés à une file PRIQ moins prioritaire.

! IMPORTANT

- Pour éviter des risques de congestion de trafic, il faut réserver ce type de files d'attente à des flux maîtrisés en termes de débit qui ne peuvent pas consommer toute la bande passante et doivent être réservées aux flux les plus prioritaires.
- Il est fortement recommandé d'avoir une seule file de type PRIQ pouvant affamer les autres files d'attente et de lui affecter une priorité plus basse que les autres files d'attente. Par exemple, ne pas créer une file de type PRIQ pour le HTTP et une autre pour le FTP par exemple.
- Il est fortement recommandé de ne pas utiliser plus de 3 ou 4 niveaux de priorité dans une configuration.
- Il ne faut pas combiner des files de type PRIQ et des files de type CBQ dans une même configuration.
Bien que l'interface Web d'administration n'interdise pas la combinaison de files CBQ et PRIQ, cette configuration n'est pas supportée par Stormshield.

- Files d'attente de supervision (MONQ *Monitoring Queing*) : ces files spécifiques n'influent pas sur le trafic réseau mais permettent d'enregistrer, et de présenter sous forme de graphes (module **Monitoring > Supervision > QoS**), les informations de bande passante utilisées par les flux auxquels elles sont affectées. Ceci permet de mieux définir ou d'affiner le paramétrage des files de type CBQ.

Le contrôle de volume des échanges de données est effectué par un Traffic shaper (régulateur de flux) associé aux files d'attente de QoS. Celui-ci s'applique à l'interface de sortie des paquets traités.

💡 DÉFINITION

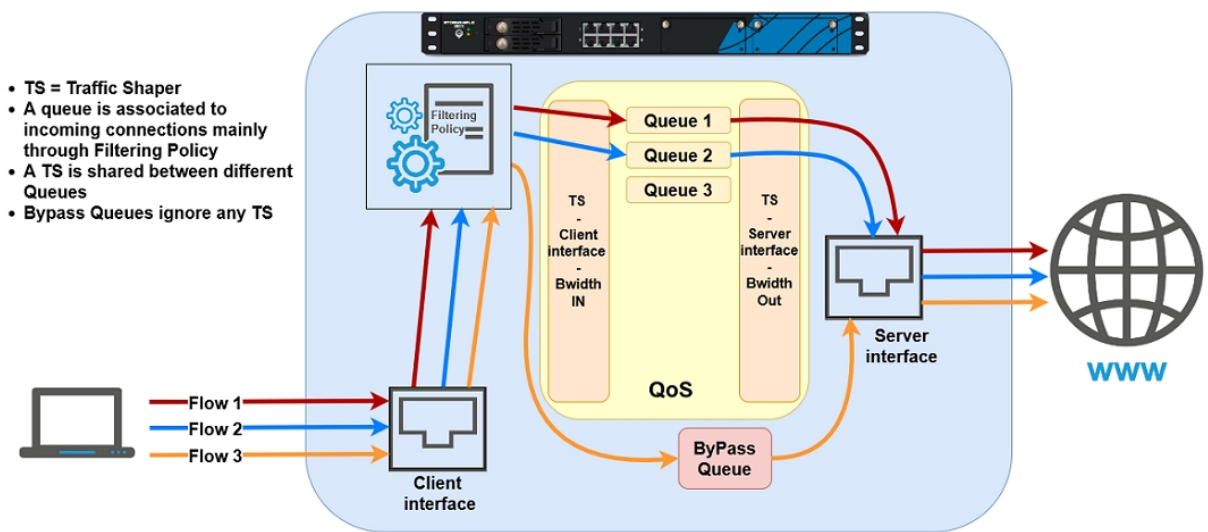
L'objectif du *Traffic shaping* (régulation de flux) est de faire respecter le débit d'informations garanties (CIR - *Committed Information Rate*) par le contrôle du volume des échanges sur le réseau, en retardant les paquets qui correspondent aux critères définis dans les files d'attente (réservation ou limitation). Il fonctionne grâce à un algorithme nommé TBR (*Token Bucket Regulator*) utilisant un espace tampon pour le trafic excédentaire.



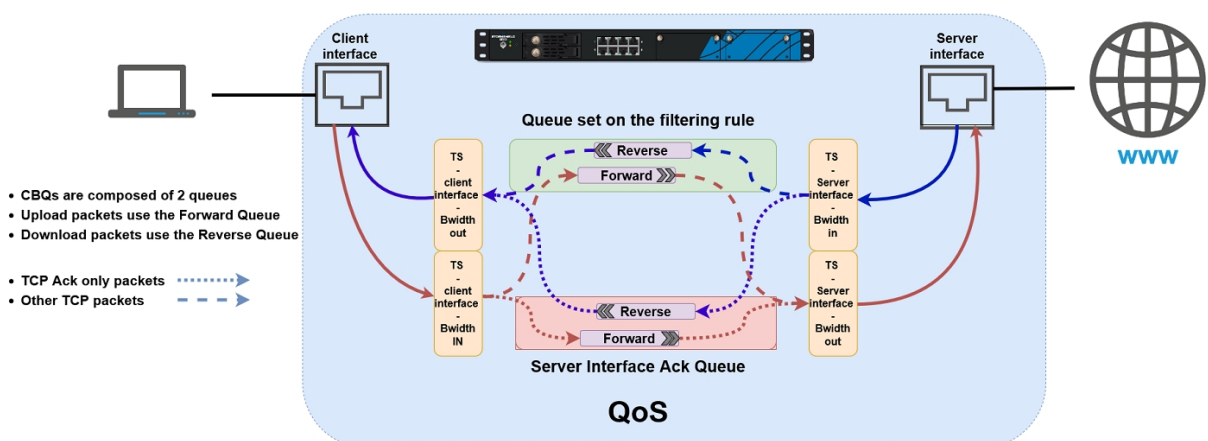
! IMPORTANT
La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

i NOTE
Dans une configuration utilisant des flux IPsec, ces flux emprunteront automatiquement la file d'attente par défaut pour l'interface WAN. C'est la raison pour laquelle une réservation de bande passante est appliquée à cette file d'attente.

Illustration du principe général de la QoS



Application de QoS à un trafic réseau LAN / WAN



Interfaces incompatibles avec la QoS

Certains types d'interfaces ne peuvent pas être sélectionnés pour y appliquer de la QoS. Il s'agit des types d'interfaces suivants :



- Interfaces GRE,
- Interfaces Loopback,
- Interfaces VPN SSL,
- Interfaces Wi-Fi,
- Agrégats de liens LACP,
- Modems USB 4G,
- Modems PPPoE et PPTP.

Utilisation au travers du proxy SSL

Dans une configuration avec des flux HTTPS passant par le proxy SSL, la file d'attente de QoS correspondante doit être appliquée au niveau de la règle de déchiffrement et non au niveau de la règle de filtrage via le proxy.

Bonnes pratiques

Le respect de certaines bonnes pratiques permet une implémentation optimale de la QoS :

- Configurer une file d'attente d'acquittement par défaut (file d'attente réservée aux paquets TCP d'acquittement [ack]) pour chaque interface réseau soumise à la QoS. Chaque file d'attente d'acquittement correspond à une réservation de 5% de la bande passante de l'interface réseau concernée.
- Configurer des files d'attente par défaut pour chacune des interfaces réseau soumises à la QoS. La file d'attente par défaut est empruntée par tout flux pour lequel aucune file d'attente spécifique de QoS n'est précisée.
- Pour les flux consommant une partie non négligeable de la bande passante, il ne faut pas utiliser de files d'attente de type bypass qui sont prioritaires sur l'ensemble des flux et entraînent un dysfonctionnement des réservations de bande passante. En effet, ces flux ne sont pas pris en compte dans la détection de contention sur l'interface et peuvent donc empêcher la QoS d'intervenir lorsque la bande passante d'un lien est saturée. Les files d'attente de type bypass sont à utiliser pour des flux comme la négociation IPsec ou la supervision des routeurs.

Précautions de mise en œuvre

! IMPORTANT

Avant de mettre en œuvre la Qualité de service (QoS) dans une architecture de production initialement vierge de toute notion de QoS, Stormshield vous recommande de réaliser tout d'abord une configuration basée sur des files d'attente de supervision (MONQ) et non directement sur des files d'attente par classe d'application ou d'affectation (CBQ). Cette étape vous permet en effet de visualiser le volume de flux sur lesquels aucune QoS n'est appliquée et de vérifier si les valeurs de réservation ou de limitation de bande passante envisagées pour les files de type CBQ suffisent à laisser passer les flux soumis à la QoS. Une fois ces valeurs établies, vous pouvez alors mettre en places vos files d'attente CBQ.



Limites et caractères autorisés dans les noms des files d'attente et des Traffic shapers

Files d'attente de QoS

- Le nom est limité à 31 caractères.
- Les caractères interdits sont :

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

- Le nom ne doit pas contenir les expressions réservées suivantes :

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

Traffic shapers

- Le nom est limité à 15 caractères,
- Les caractères interdits sont :

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

Nommage des interfaces dans cette Note Technique

Pour une meilleure compréhension des différents cas d'usage présentés, les interfaces d'origine du firewall ont été renommées comme suit :

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



Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN

Cette section présente la configuration minimale permettant d'appliquer de la QoS dans une architecture disposant d'un réseau local (rattaché à l'interface *LAN* dans cet exemple) et d'un accès Internet (rattaché à l'interface *WAN* dans cet exemple). Les différentes étapes nécessaires sont les suivantes :

- Créer la file d'attente par défaut et la file d'attente d'acquittement (ACK) par défaut pour chaque interface soumise à la QoS,
- Définir les Traffic shapers,
- Attribuer les Traffic shapers, files d'attente d'acquittement (ACK) et files d'attente par défaut aux interfaces soumises à la QoS.

Créer les files d'attente par défaut

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente**.

Comprendre la grille des files d'attente

Colonnes BP garantie et BP max

Les colonnes BP garantie (Bande passante garantie) et BP max (Bande passante maximale) sont dédiées au trafic sortant de l'interface réseau :

- La colonne BP garantie permet de définir une réservation de bande passante pour un flux sortant,
- La colonne BP max permet de définir une limitation de bande passante pour un flux sortant.

Colonnes BP inv. garantie et BP inv. max

Les colonnes BP inv. garantie (Bande passante inverse garantie) et BP inv. max (Bande passante inverse maximale) sont dédiées au trafic de retour d'une connexion :

- La colonne BP inv. garantie permet de définir une réservation de bande passante pour le trafic de retour des connexions,
- La colonne BP inv. max permet de définir une limitation de bande passante pour le trafic de retour des connexions.

Créer les files d'attente par défaut pour les interfaces *LAN* et *WAN*

i NOTE

Il est fortement recommandé de préciser une réservation de bande passante (champs **Bp garantie** et **Bp inv. garantie**) pour les files d'attente par défaut.

En effet, en cas de saturation de la bande passante disponible sur le lien, et sans réservation de bande passante, le trafic devant emprunter la file d'attente par défaut pourrait être supprimé par le firewall.



La valeur de cette réservation dépend du volume et du nombre de flux moins prioritaires et donc non soumis à une file d'attente de QoS spécifique.

Créer la file d'attente par défaut pour l'interface LAN

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*DEF_LAN_Q* dans cet exemple).
4. Sur la ligne **Bp garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (100 Mbit/s dans cet exemple).
5. Sur la ligne **Bp max**, laissez la valeur proposée par défaut (10 Gbit/s).
6. Sur la ligne **Bp inv. garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (100 Mbit/s dans cet exemple).
7. Sur la ligne **Bp inv. max**, laissez la valeur proposée par défaut (10 Gbit/s).
8. Validez en cliquant sur **Appliquer**.

Créer la file d'attente par défaut pour l'interface WAN

Suivez la procédure détaillée dans [Créer la file d'attente par défaut pour l'interface LAN](#) avec les valeurs suivantes :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	DEF_WAN_Q
Bp garantie	10 Mbit/s
Bp max	valeur proposée par défaut (10 Gbit/s)
Bp inv. garantie	10 Mbit/s
Bp inv. max	valeur proposée par défaut (10 Gbit/s)

i NOTE

Dans une configuration utilisant des flux IPsec, ces flux emprunteront automatiquement la file d'attente par défaut pour l'interface WAN. C'est la raison pour laquelle une réservation de bande passante est appliquée à cette file d'attente.

Notez que l'application de QoS aux flux IPsec n'est pas traitée dans cette Note Technique.

Créer les files d'attente d'acquittement (ACK) pour les interfaces LAN et WAN

Dans cet exemple, le lien connecté à l'interface LAN offre une bande passante maximale de 1 Gbit/s et celui connecté à l'interface WAN une bande passante maximale de 100 Mbit/s.

Les files d'attente d'acquittement (ACK) respectives sont donc de 50 Mbit/s pour l'interface LAN et 5 Mbit/s pour l'interface WAN (réservation de 5% de la bande passante maximale des liens).

Créer la file d'attente d'acquittement (ACK) pour l'interface LAN

Suivez la procédure détaillée dans [Créer la file d'attente par défaut pour l'interface LAN](#) avec les valeurs suivantes :



Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	DEF_LAN_ACK_Q
Bp garantie	50 Mbit/s
Bp max	illimité
Bp inv. garantie	50 Mbit/s
Bp inv. max	illimité

Créer la file d'attente d'acquittement (ACK) pour l'interface WAN

1. Suivez la procédure détaillée dans [Créer la file d'attente par défaut pour l'interface LAN](#) avec les valeurs suivantes :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	DEF_WAN_ACK_Q
Bp garantie	5 Mbit/s
Bp max	illimité
Bp inv. garantie	5 Mbit/s
Bp inv. max	illimité

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :

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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.

Créer les Traffic shapers

Un Traffic shaper est un régulateur de flux : il permet de définir la bande passante maximale utilisable sur une interface soumise à la QoS.

! IMPORTANT

- La valeur du Traffic shaper ne doit pas dépasser 90% de la bande passante maximale du lien rattaché à l'interface pour que la QoS soit fonctionnelle.
- La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper**.



Comprendre la grille des Traffic shapers

Colonnes Bande passante sortante et Bande passante entrante

Ces colonnes correspondent à :

- **Bande passante sortante** : bande passante maximale utilisable pour le trafic sortant (envoi de fichiers par exemple),
- **Bande passante entrante** : bande passante maximale utilisable pour le trafic entrant (téléchargement de fichiers hébergés sur le WAN par un client situé sur le LAN par exemple).

Créer le Traffic shaper pour l'interface LAN

1. Cliquez sur **Ajouter**.
2. Nommez le Traffic shaper (*TS_LAN* dans cet exemple).
3. Dans la colonne **Bande passante sortante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *LAN* (900 [Mbit/s] dans cet exemple).
4. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
5. Dans la colonne **Bande passante entrante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *LAN* (900 [Mbit/s] dans cet exemple).
6. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
7. Validez en cliquant sur **Appliquer**.

Créer le Traffic shaper pour l'interface WAN

Suivez la procédure détaillée dans [Créer le Traffic shaper pour l'interface LAN](#) avec les valeurs suivantes :

Nom	<i>TS_WAN</i>
Bande passante sortante	90
Unité	Mbit/s
Bande passante entrante	90
Unité	Mbit/s

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :

TRAFFIC SHAPER				
Q Enter a filter	+ Add		X Delete	
Name	Outgoing bandwidth	Unit	Incoming bandwidth	Unit
TS_LAN	900	Mbits	900	Mbits
TS_WAN	90	Mbits	90	Mbits

Configurer la QoS sur les interfaces LAN et WAN

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper** > grille **Interfaces avec QoS**.



Cette phase de la configuration consiste à associer à chaque interface concernée par la QoS :

- Un Traffic shaper,
- Une file d'attente par défaut : cette file d'attente sera empruntée par tout flux pour lequel aucune file d'attente de QoS n'est précisée dans la règle de filtrage du flux considéré.
- Une file d'attente d'acquittement par défaut.

Configurer la QoS sur l'interface LAN

1. Cliquez sur **Ajouter**.
2. Sélectionnez l'interface *LAN*.
3. Sélectionnez le **Traffic shaper** pour cette interface (*TS_LAN* dans cet exemple).
4. Sélectionnez la **File d'attente par défaut** pour cette interface (*DEF_LAN_Q* dans cet exemple).
5. Sélectionnez la **File d'attente d'acquittement (ACK) par défaut** (*DEF_LAN_ACK_Q* dans cet exemple).
6. Validez en cliquant sur **Appliquer**.

Configurer la QoS sur l'interface WAN

Suivez la procédure détaillée dans la section précédente (**Configurer la QoS sur l'interface LAN**) avec les valeurs suivantes :

Interface	<i>WAN</i>
Traffic shaper	<i>TS_WAN</i>
File d'attente par défaut	<i>DEF_WAN_Q</i>
File d'attente d'acquittement (ACK) par défaut	<i>DEF_WAN_ACK_Q</i>

La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :

INTERFACES WITH QOS			
Enter a filter			
Select all + Add X Delete			
Interface	Traffic shaper	Default queue	Default ACK queue
LAN	TS_LAN	DEF_LAN_Q	DEF_LAN_ACK_Q
WAN	TS_WAN	DEF_WAN_Q	DEF_WAN_ACK_Q

Cas de VLAN rattachés à une interface

Si un ou plusieurs VLAN sont rattachés à une interface physique (interface *LAN* dans cet exemple), il est nécessaire d'attribuer à chaque interface VLAN :

- Le Traffic shaper de l'interface parente (*TS_LAN* dans cet exemple),
- Une file d'attente par défaut : file d'attente spécifique au VLAN (en cas de besoin de garantie de bande passante pour ce VLAN) ou file d'attente de l'interface parente (*DEF_LAN_Q* dans cet exemple),
- La file d'attente d'acquittement (ACK) par défaut de l'interface parente (*DEF_LAN_ACK_Q* dans cet exemple).

Comme pour les interfaces physiques, veillez à ce que la somme des réservations de bande passante des VLAN n'excède pas la valeur du Traffic shaper.

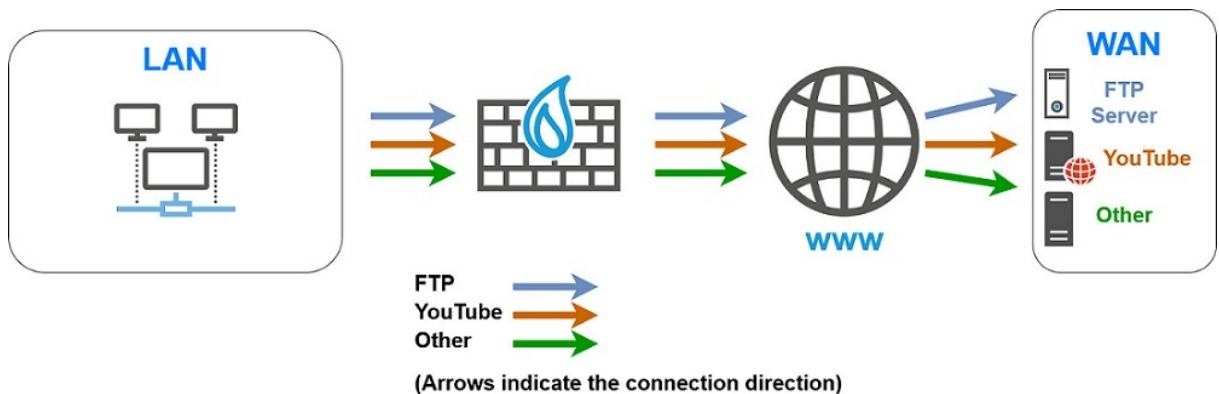


Application : limitation de bande passante dans une architecture de type LAN / WAN

Cette section suppose que la [configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN](#) est existante.

Elle décrit l'ajout des composants nécessaires à l'application de limitation et réservation de bande passante pour certains flux transitant par les liens attachés aux interfaces LAN et WAN.

Le détail de la politique de gestion de trafic mise en place par l'administrateur est décrit ci-dessous.



Limitation et réservation de bande passante sur le lien WAN

i NOTE

La somme des réservations de bande passante pour un lien doit être au maximum égale à 85% de la bande passante totale de ce lien. En effet, la bande passante utilisable pour ces réservations est égale à la bande passante affectée au Traffic shaper correspondant (90% de la bande passante totale) moins la bande passante affectée à la file d'attente d'acquittement (5% de la bande passante totale).

Transferts de fichiers métier (FTP)

On définit une file d'attente nommée *FTP_WAN_Q* :

- Limitation à 30 Mbit/s pour les flux sortants,
- Limitation à 40 Mbit/s pour les flux retour.

Limitation des flux *YouTube* sur détection de signature par le moteur de prévention d'intrusion

La méthode utilisée pour limiter un flux spécifique détecté par le moteur de prévention d'intrusion (*YouTube* dans cet exemple) est d'appliquer une file d'attente de QoS spécifique (*YTB_WAN_Q* dans cet exemple) à la signature de détection correspondante (module **Applications et protections** - signature "Multimédia : YouTube" dans cet exemple).

On définit ici une file d'attente nommée *YTB_WAN_Q* :



- Limitation à 20 Mbit/s pour les flux sortants,
- Limitation à 20 Mbit/s pour les flux retour.

Créer les files d'attente pour les flux FTP et YouTube

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente**.

Créer la file d'attente pour les flux FTP

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*FTP_WAN_Q* dans cet exemple).
4. Sur la ligne **Bp garantie**, sélectionnez **Aucun** dans le premier champ.
5. Sur la ligne **Bp max**, spécifiez 30 Mbit/s.
6. Sur la ligne **Bp inv. garantie**, sélectionnez **Aucun** dans le premier champ.
7. Sur la ligne **Bp inv. max**, spécifiez 40 Mbit/s.
8. Validez en cliquant sur **Appliquer**.

Créer la file d'attente pour les flux YouTube

1. Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Nom	YTB_WAN_Q
Bp garantie	Aucun
Bp max	20 Mbit/s
Bp inv. garantie	Aucun
Bp inv. max	20 Mbit/s

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :

QUEUES						
<input type="text" value="Enter a filter"/> + Add X 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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.



Traffic shapers

Dans cet exemple, on considère que les Traffic shapers des interfaces *LAN* et *WAN* sont existants et ont été créés comme décrit dans la section [Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN](#).

! IMPORTANT

La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :

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

Configurer les interfaces concernées par la QoS

Dans cet exemple, on considère que les interfaces soumises à la QoS (interfaces *LAN* et *WAN*) ont été configurées comme décrit dans la section [Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN](#).

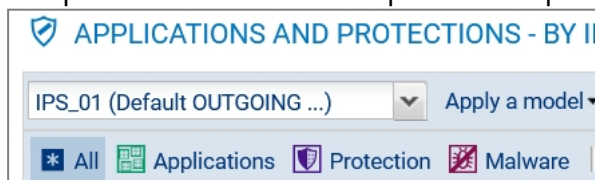
La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :

INTERFACES WITH QOS			
🔍 Enter a filter			
Select all + Add ✕ Delete			
Interface	Traffic shaper	Default queue	Default ACK queue
🏠 LAN	TS_LAN	DEF_LAN_Q	DEF_LAN_ACK_Q
🏠 WAN	TS_WAN	DEF_WAN_Q	DEF_WAN_ACK_Q

Appliquer une file d'attente de QoS à la signature de l'application *YouTube*

Placez-vous dans le module **Protection applicative** > **Applications et protections**.

1. Dans la fenêtre située en haut à gauche de la barre d'action, sélectionnez le profil d'inspection sortant à modifier : profil sortant par défaut *IPS_01* dans cet exemple :



2. Dans le champ de recherche, tapez une suite de caractères contenue dans le nom de l'application *YouTube*.
3. Sélectionnez la ligne de la signature à laquelle vous souhaitez appliquer une file d'attente de QoS [signature "Multimédia : YouTube" dans cet exemple]. Un menu **Options avancées** s'affiche dans la colonne **Avancé**.
4. Cliquez sur **Options avancées**. Une fenêtre de configuration s'ouvre.



5. Dans le champ **QoS appliquée au flux**, sélectionnez la file d'attente réservée aux flux *YouTube* (*YTB_WAN_Q* dans cet exemple).
6. Validez cette modification en cliquant sur **Appliquer**.
7. Cliquez sur **Appliquer** puis sur **Sauvegarder**.


Créer les règles de filtrage

i NOTE

Cette section décrit la création des règles de filtrage utilisant des files d'attente de QoS spécifiques, autres que les files d'attente par défaut. La création des règles de filtrage pour les autres flux depuis le LAN vers le WAN ou la DMZ n'est pas abordée.

Placez-vous dans le module **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.

Créer la règle de filtrage pour le protocole FTP

1. Dans la liste déroulante située au-dessus de la grille de filtrage, sélectionnez la politique de sécurité à modifier.
2. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches .
4. Effectuez un double clic sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
5. Cliquez sur le menu de gauche **Général**.
6. Dans le champ **État**, sélectionnez la valeur *On*.
7. Cliquez sur le menu de gauche **Action**.
8. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
9. Dans l'onglet **Qualité de service**, pour le champ **File d'attente**, sélectionnez la file d'attente créée pour les flux FTP vers le WAN (*FTP_WAN_Q* dans cet exemple).
10. Cliquez sur le menu de gauche **Source**.
11. Dans l'onglet **Général**, pour le champ **Machines sources** sélectionnez les machines, les groupes de machines ou les réseaux autorisés à utiliser le protocole FTP (réseau *LAN_Clients* dans cet exemple).
12. Cliquez sur le menu de gauche **Destination**.
13. Dans l'onglet **Général**, pour le champ **Machines destinations**, cliquez sur **Ajouter** et sélectionnez le serveur ou le groupe de serveurs FTP (machine *WAN_FTP_Server* dans cet exemple).
14. Cliquez sur le menu de gauche **Port / Protocole**.
15. Dans le cadre **Port**, pour le **Port destination**, sélectionnez l'objet *ftp*.
16. Validez la création de la règle en cliquant sur **OK**.

**i NOTE**

Dans le cas d'un protocole générant des connexions filles (FTP dans cet exemple), la file d'attente précisée dans la règle de filtrage s'applique automatiquement aux connexions filles.

Créer la règle de filtrage pour l'application YouTube

Suivez la procédure détaillée dans [Créer la règle de filtrage pour le protocole FTP](#) avec les valeurs suivantes pour cet exemple :

État	<i>on</i>
Action	<i>passer</i>
File d'attente	Laissez la valeur proposée par défaut (<i>File d'attente par défaut</i>). En effet, c'est la détection de la signature de l'application YouTube par le moteur de prévention d'intrusion qui affectera la file d'attente adéquate (<i>YTB_WAN_Q</i> dans cet exemple) aux flux empruntant cette règle.
Machines sources	<i>LAN_Clients</i>
Machines destinations	L'objet <i>Internet</i>
Port destination	L'objet <i>https</i>

Appliquer la politique de sécurité modifiée

Pour valider les modifications et appliquer la nouvelle politique de sécurité, cliquez sur **Appliquer** puis sur **Oui, Activer la politique**.

Les règles de filtrage utilisant des files d'attente de QoS spécifiques prennent donc la forme suivante :

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



Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ

Cette section suppose que la [configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN](#) est existante et décrit l'ajout des composants nécessaires à l'application de QoS aux flux vers la DMZ.

Créer les files d'attente de l'interface DMZ

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente**.

Créer la file d'attente par défaut de l'interface DMZ

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*DEF_DMZ_Q* dans cet exemple).
4. Sur la ligne **Bp garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (100 Mbit/s dans cet exemple).
5. Sur la ligne **Bp max**, laissez la valeur proposée par défaut (10 Gbit/s).
6. Sur la ligne **Bp inv. garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (100 Mbit/s dans cet exemple).
7. Sur la ligne **Bp inv. max**, laissez la valeur proposée par défaut (10 Gbit/s).
8. Validez en cliquant sur **Appliquer**.

Créer la file d'attente d'acquiescement (ACK) de l'interface DMZ

Dans cet exemple, le lien connecté à l'interface *DMZ* présente une bande passante maximale de 1 Gbit/s : la file d'attente d'acquiescement (ACK) sera donc de 50 Mbit/s (réservation égale à 5% de la bande passante maximale du lien).

1. Suivez la procédure détaillée dans [Créer la file d'attente par défaut pour l'interface DMZ](#) avec les valeurs suivantes :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>DEF_DMZ_ACK_Q</i>
Bp garantie	50 Mbit/s
Bp max	illimité
Bp inv. garantie	50 Mbit/s
Bp inv. max	illimité

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :



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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.

Créer le Traffic shaper de l'interface DMZ

! IMPORTANT

La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper** :

1. Cliquez sur **Ajouter**.
2. Nommez le Traffic shaper (*TS_DMZ* dans cet exemple).
3. Dans la colonne **Bande passante sortante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *DMZ* (900 [Mbit/s] dans cet exemple).
4. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
5. Dans la colonne **Bande passante entrante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *DMZ* (900 [Mbit/s] dans cet exemple).
6. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
7. Validez la création du Traffic shaper en cliquant sur **Appliquer**.
8. Validez en cliquant sur **Appliquer**.

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :

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

Configurer la QoS sur l'interface DMZ

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper** > grille **Interfaces avec QoS** :

1. Cliquez sur **Ajouter**.
2. Sélectionnez l'interface *DMZ*.
3. Sélectionnez le **Traffic shaper** de cette interface (*TS_DMZ* dans cet exemple).



4. Sélectionnez la **File d'attente par défaut** de cette interface (*DEF_DMZ_Q* dans cet exemple).
5. Sélectionnez la **File d'attente d'acquittement (ACK) par défaut** (*DEF_DMZ_ACK_Q* dans cet exemple).
6. Validez la configuration de la QoS sur l'interface *DMZ* en cliquant sur **Appliquer**.
7. Validez en cliquant sur **Appliquer**.

La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :

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

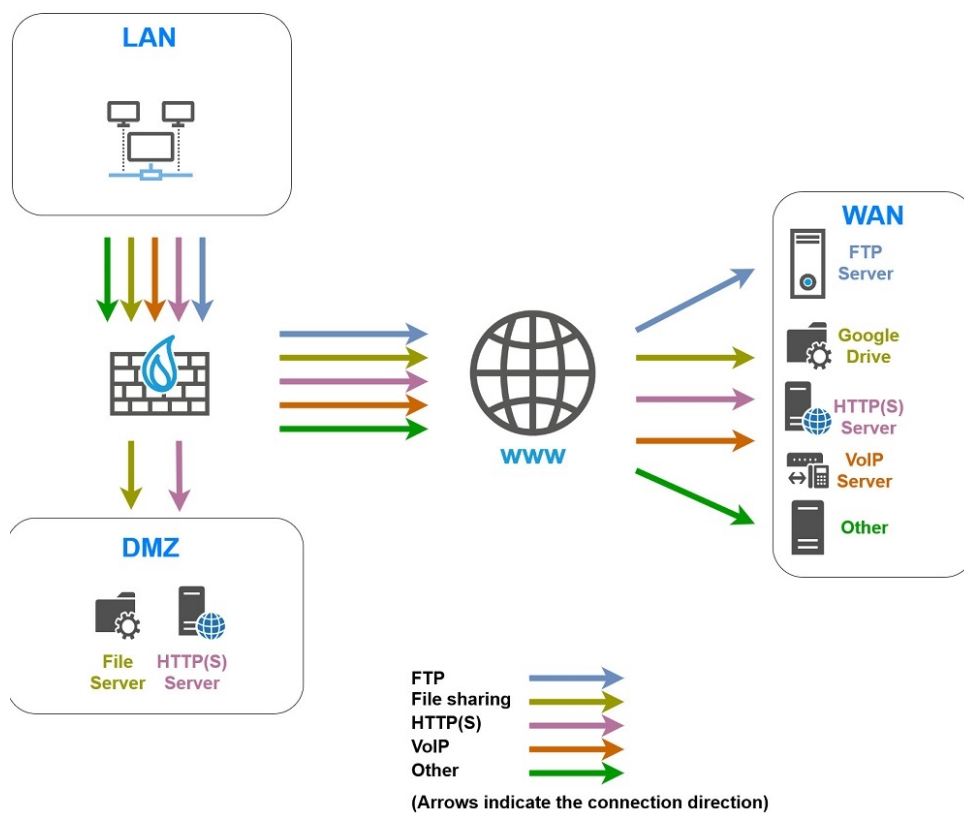


Application : limitation et réservation de bande passante dans une architecture de type LAN / WAN / DMZ

Cet exemple suppose que la **configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ** est existante.

Il décrit l'ajout des composants nécessaires à l'application de réservation et limitation de bande passante pour certains flux transitant par les liens attachés aux interfaces *LAN*, *WAN* et *DMZ*.

Le détail de la politique de gestion de trafic mise en place par l'administrateur est décrit ci-dessous.



Limitation et réservation de bande passante sur le lien WAN

i NOTE

La somme des réservations de bande passante pour un lien doit être au maximum égale à 85% de la bande passante totale de ce lien. En effet, la bande passante utilisable pour ces réservations est égale à la bande passante affectée au Traffic shaper correspondant (90% de la bande passante totale) moins la bande passante affectée à la file d'attente d'acquittement (5% de la bande passante totale).

Transferts de fichiers métier (FTP)

On définit une file d'attente nommée *FTP_WAN_Q* :



- Réserve de 10 Mbit/s et limitation à 20 Mbit/s pour les flux sortants,
- Réserve de 10 Mbit/s et limitation à 20 Mbit/s pour les flux retour.

Hébergement et partage de fichiers sur des serveurs externes (exemple : Google Drive)

On utilise une file d'attente nommée *GD_WAN_Q* dans cet exemple :

- Réserve de 10 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 10 Mbit/s et limitation à 20 Mbit/s pour les flux retour.

i NOTE

Cette file d'attente sera utilisée dans une règle de filtrage à destination du service Web *Google Drive*.

Cet objet prédéfini rassemble toutes les adresses IP et FQDN connus des services *Google Drive*. Il est automatiquement mis à jour via le service Active Update du firewall.

Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier externe

On définit une file d'attente nommée *HTTP_WAN_Q* :

- Réserve de 40 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 40 Mbit/s et pas de limitation pour les flux retour.

Communications en VoIP (SIP)

On définit une file d'attente nommée *SIP_WAN_Q* :

- Réserve de 15 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 15 Mbit/s et pas de limitation pour les flux retour.

Réserve de bande passante sur le lien DMZ

Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier local

On définit une file d'attente nommée *HTTP_DMZ_Q* :

- Réserve de 600 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 600 Mbit/s et pas de limitation pour les flux retour.

Partage de fichiers sur un serveur

On définit une file d'attente nommée *SMB_DMZ_Q* :

- Réserve de 100 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 100 Mbit/s et pas de limitation pour les flux retour.

Créer les files d'attente

Dans cet exemple, on considère que les files d'attente d'acquiescement (ACK) par défaut et les files d'attente par défaut pour les interfaces *LAN*, *WAN* et *DMZ* sont existantes et ont été créées



comme décrit dans la section [Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ](#).

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente**.

Créer les files d'attente pour l'interface WAN

Créer la file d'attente pour les flux FTP

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*FTP_WAN_Q* dans cet exemple).
4. Sur la ligne **Bp garantie**, spécifiez 10 Mbit/s.
5. Sur la ligne **Bp max**, spécifiez 20 Mbit/s.
6. Sur la ligne **Bp inv. garantie**, spécifiez 10 Mbit/s.
7. Sur la ligne **Bp inv. max**, spécifiez 20 Mbit/s.
8. Validez en cliquant sur **Appliquer**.

Créer la file d'attente pour le partage de fichiers

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>GD_WAN_Q</i>
Bp garantie	10 Mbit/s
Bp max	illimité
Bp inv. garantie	10 Mbit/s
Bp inv. max	20 Mbit/s

Créer la file d'attente pour les flux métier HTTP / HTTPS

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>HTTP_WAN_Q</i>
Bp garantie	40 Mbit/s
Bp max	illimité
Bp inv. garantie	40 Mbit/s
Bp inv. max	illimité

Créer la file d'attente pour les flux VoIP (SIP)

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :



Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>SIP_WAN_Q</i>
Bp garantie	15 Mbit/s
Bp max	illimité
Bp inv. garantie	15 Mbit/s
Bp inv. max	illimité

Créer les files d'attente pour l'interface *DMZ*

Créer la file d'attente pour les flux métier HTTP / HTTPS

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>HTTP_DMZ_Q</i>
Bp garantie	600 Mbit/s
Bp max	illimité
Bp inv. garantie	600 Mbit/s
Bp inv. max	illimité

Créer la file d'attente pour le partage de fichiers

1. Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>SMB_DMZ_Q</i>
Bp garantie	100 Mbit/s
Bp max	illimité
Bp inv. garantie	100 Mbit/s
Bp inv. max	illimité

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :



QUEUES						
Q 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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.

Traffic shapers

Dans cet exemple, on considère que les Traffic shapers des interfaces *LAN*, *WAN* et *DMZ* sont existants et ont été créés comme décrit dans la section [Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ](#).

! IMPORTANT

La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :

TRAFFIC SHAPER				
Q 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

Configurer la QoS sur les interfaces *LAN*, *WAN* et *DMZ*

Dans cet exemple, on considère que les interfaces soumises à la QoS (interfaces *LAN*, *WAN* et *DMZ*) ont été configurées comme décrit dans les sections [Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN](#) et [Créer la configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / DMZ](#).

La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :



INTERFACES WITH QOS			
🔍 Enter a filter			
Select all + Add X 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

Créer les règles de filtrage

i NOTE

Cette section décrit la création des règles de filtrage utilisant des files d'attente de QoS spécifiques, autres que les files d'attente par défaut. La création des règles de filtrage pour les autres flux depuis le LAN vers le WAN ou la DMZ n'est pas abordée.

i NOTE

Il est déconseillé de préciser les files d'attente acquittement (ACK) au sein des règles de filtrage. Il est en effet préférable de laisser les flux de type ACK emprunter automatiquement les files d'attente d'acquittement (ACK) définies par défaut pour les interfaces concernées par ces flux.

Placez-vous dans le module **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.

Créer la règle de filtrage vers le serveur FTP distant

1. Dans la liste déroulante située au-dessus de la grille de filtrage, sélectionnez la politique de sécurité à modifier.
2. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches
4. Effectuez un double clic sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
5. Cliquez sur le menu de gauche **Général**.
6. Dans le champ **État**, sélectionnez la valeur *On*.
7. Cliquez sur le menu de gauche **Action**.
8. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
9. Dans l'onglet **Qualité de service**, pour le champ **File d'attente** du cadre **QoS** : sélectionnez la file d'attente créée pour les flux FTP (*FTP_WAN_Q* dans cet exemple).
10. Cliquez sur le menu de gauche **Source**.
11. Dans l'onglet **Général**, pour le champ **Machines sources** sélectionnez les machines, les groupes de machines ou les réseaux autorisés à utiliser le protocole FTP (réseau *LAN_Clients* dans cet exemple).
12. Cliquez sur le menu de gauche **Destination**.




13. Dans l'onglet **Général**, pour le champ **Machines destinations**, cliquez sur **Ajouter** et sélectionnez le serveur ou le groupe de serveurs FTP (machine *WAN_FTP_Server* dans cet exemple).
14. Cliquez sur le menu de gauche **Port / Protocole**.
15. Dans le cadre **Port**, sélectionnez l'objet *ftp* comme **Port destination**.
16. Validez la création de la règle en cliquant sur **OK**.

i NOTE

Dans le cas d'un protocole générant des connexions filles (FTP dans cet exemple), la file d'attente précisée dans la règle de filtrage s'applique automatiquement aux connexions filles.

Créer la règle de filtrage pour les flux vers les serveurs *Google Drive*

1. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
2. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches .
3. Effectuez un double clic sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
4. Cliquez sur le menu de gauche **Général**.
5. Dans le champ **État**, sélectionnez la valeur *On*.
6. Cliquez sur le menu de gauche **Action**.
7. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
8. Dans l'onglet **Qualité de service**, pour le champ **File d'attente** du cadre **QoS**, sélectionnez la file d'attente créée pour les flux *Google Drive* (*GD_WAN_Q* dans cet exemple).
9. Cliquez sur le menu de gauche **Source**.
10. Dans l'onglet **Général**, pour le champ **Machines sources** sélectionnez les machines, les groupes de machines ou les réseaux autorisés à accéder à *Google Drive* (réseau *LAN_Clients* dans cet exemple).
11. Cliquez sur le menu de gauche **Destination**.
12. Dans le cadre **Services Web et Réputation** de l'onglet **Géolocalisation / Réputation**, sélectionnez l'objet *Google Drive*.
13. Cliquez sur le menu de gauche **Port / Protocole**.
14. Dans le cadre **Port**, sélectionnez l'objet *https* comme **Port destination**.
15. Validez la création de la règle en cliquant sur **OK**.

Créer la règle de filtrage vers le serveur HTTP / HTTPS distant

Suivez la procédure détaillée dans [Créer la règle de filtrage vers le serveur FTP distant](#) avec les valeurs suivantes pour cet exemple :

État	<i>on</i>
Action	<i>passer</i>
File d'attente	<i>HTTP_WAN_Q</i>



Machines sources	<i>LAN_Clients</i>
Machines destinations	l'objet correspondant au serveur HTTP /HTTPS distant (<i>WAN_PROD_Server</i> dans cet exemple)
Port destination	les objets <i>http</i> et <i>https</i>

Créer la règle de filtrage vers le serveur VoIP distant

Suivez la procédure détaillée dans [Créer la règle de filtrage vers le serveur FTP distant](#) avec les valeurs suivantes pour cet exemple :

État	<i>on</i>
Action	<i>passer</i>
File d'attente	<i>SIP_WAN_Q</i>
Machines sources	<i>LAN_VoIP_Clients</i>
Machines destinations	l'objet correspondant au serveur SIP distant (<i>WAN_VoIP_Server</i> dans cet exemple)
Port destination	l'objet <i>sip</i>

i NOTE

Dans le cas d'un protocole générant des connexions filles (SIP dans cet exemple), la file d'attente précisée dans la règle de filtrage s'applique automatiquement aux connexions filles.

Créer la règle de filtrage vers le serveur HTTP / HTTPS en DMZ

Suivez la procédure détaillée dans [Créer la règle de filtrage vers le serveur FTP distant](#) avec les valeurs suivantes :

État	<i>on</i>
Action	<i>passer</i>
File d'attente	<i>HTTP_DMZ_Q</i>
Machines sources	<i>LAN_Clients</i>
Machines destinations	l'objet correspondant au serveur HTTP /HTTPS distant (<i>LOCAL_PROD_Server</i> dans cet exemple)
Port destination	les objets <i>http</i> et <i>https</i>

Créer la règle de filtrage vers le serveur de fichiers en DMZ

Suivez la procédure détaillée dans [Créer la règle de filtrage vers le serveur FTP distant](#) avec les valeurs suivantes pour cet exemple :

État	<i>on</i>
------	-----------



Action	passer
File d'attente	SMB_DMZ_Q
Machines sources	LAN_Clients
Machines destinations	l'objet correspondant au serveur de fichiers local (<i>LOCAL_FILE_Server</i> dans cet exemple)
Port destination	l'objet <i>microsoft-ds</i>

Appliquer la politique de sécurité modifiée

Pour valider les modifications et appliquer la nouvelle politique de sécurité, cliquez sur **Appliquer** puis sur **Oui, Activer la politique**.

Les règles de filtrage utilisant des files d'attente de QoS spécifiques prennent donc la forme suivante :

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_Serve	microsoft-ds		IPS



Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2

Cette section suppose que la [configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN](#) est existante et décrit l'ajout des composants nécessaires à l'application de QoS aux flux vers le deuxième accès WAN2 (bande passante dans cet exemple : 100 Mbit/s).

La répartition des flux soumis à la QoS entre les 2 accès WAN est entièrement compatible avec toutes les méthodes de routage suivantes :

- Routage statique,
- Routage dynamique,
- PBR (*Policy Based Routing* - Routage par politique de filtrage),
- Utilisation d'objets routeurs, avec ou sans partage de charge.

Créer les files d'attente

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente**.

Créer la file d'attente par défaut pour l'interface WAN2

1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*DEF_WAN2_0* dans cet exemple).
4. Sur la ligne **Bp garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (10 Mbit/s dans cet exemple).
5. Sur la ligne **Bp max**, laissez la valeur proposée par défaut (10 Gbit/s).
6. Sur la ligne **Bp inv. garantie**, indiquez la valeur souhaitée pour la réservation de bande passante (10 Mbit/s dans cet exemple).
7. Sur la ligne **Bp inv. max**, laissez la valeur proposée par défaut (10 Gbit/s).
8. Validez en cliquant sur **Appliquer**.

i NOTE

Dans une configuration utilisant des flux IPsec, ces flux emprunteront automatiquement la file d'attente par défaut pour l'interface WAN2. C'est la raison pour laquelle une réservation de bande passante est appliquée à cette file d'attente.

Notez que l'application de QoS aux flux IPsec n'est pas traitée dans cette Note Technique.

Créer la file d'attente d'acquiescement (ACK) de l'interface WAN2

Dans cet exemple, le lien connecté à l'interface WAN2 présente une bande passante maximale de 100 Mbit/s : la file d'attente d'acquiescement (ACK) sera donc de 5 Mbit/s (réservation égale à 5% de la bande passante maximale du lien).



1. Suivez la procédure détaillée dans [Créer la file d'attente par défaut pour l'interface WAN2](#) avec les valeurs suivantes :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	DEF_WAN2_ACK_Q
Bp garantie	5 Mbit/s
Bp max	illimité
Bp inv. garantie	5 Mbit/s
Bp inv. max	illimité

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :

QUEUES						
Q Enter a filter		+ Add	×	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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.

Créer le Traffic shaper pour l'interface WAN2

! IMPORTANT

La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper** :

1. Cliquez sur **Ajouter**.
2. Nommez le Traffic shaper (*TS_WAN2* dans cet exemple).
3. Dans la colonne **Bande passante sortante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *DMZ* (90 [Mbit/s] dans cet exemple).
4. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
5. Dans la colonne **Bande passante entrante**, indiquez la valeur correspondant à 90% de la bande passante du lien rattaché à l'interface *DMZ* (90 [Mbit/s] dans cet exemple).
6. Dans la colonne **Unité**, indiquez l'unité de bande passante (Mbit/s dans cet exemple).
7. Validez la création du Traffic shaper en cliquant sur **Appliquer**.
8. Validez en cliquant sur **Appliquer**.

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :



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

Configurer la QoS sur l'interface WAN2

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Traffic shaper**.

Configurer la QoS sur l'interface WAN2

1. Cliquez sur **Ajouter**.
2. Sélectionnez l'interface **WAN2**.
3. Sélectionnez le **Traffic shaper** de cette interface (**TS_WAN2** dans cet exemple).
4. Sélectionnez la **File d'attente par défaut** de cette interface (**DEF_WAN2_Q** dans cet exemple).
5. Sélectionnez la **File d'attente d'acquittement (ACK) par défaut** (**DEF_WAN2_ACK_Q** dans cet exemple).
6. Validez la configuration de la QoS sur l'interface **WAN2** en cliquant sur **Appliquer**.
7. Cliquez sur **Appliquer**.

La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :

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



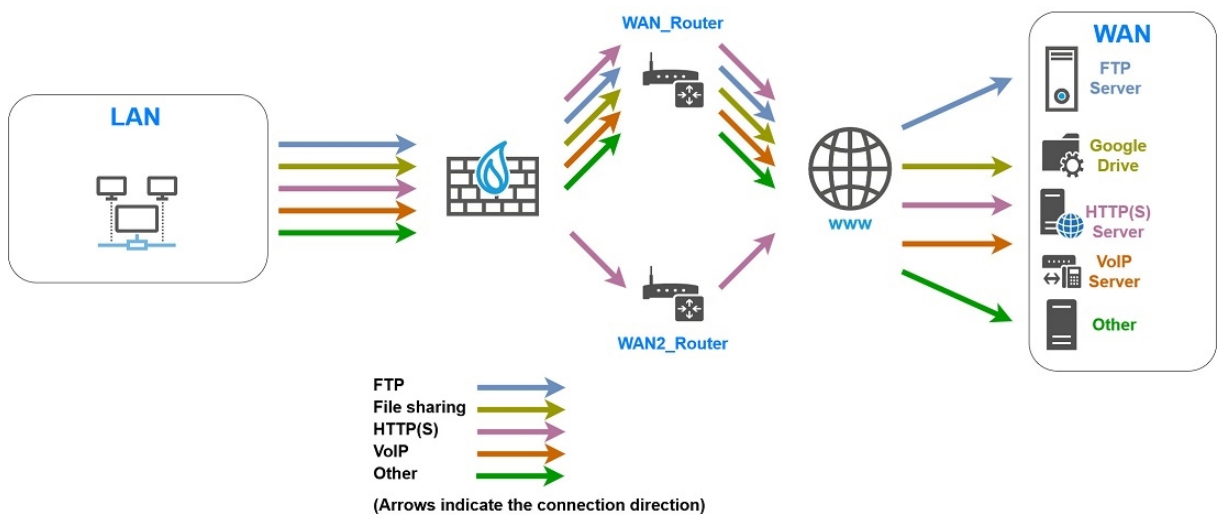
Application : limitation et réservation de bande passante dans une architecture de type LAN / WAN / WAN2

Cet exemple suppose que la **configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2** est existante.

Il décrit l'ajout des composants nécessaires à l'application de limitation et réservation de bande passante pour certains flux transitant par les liens attachés aux interfaces LAN, WAN et WAN2.

Dans cet exemple, la répartition des flux HTTP / HTTPS entre les accès WAN et WAN2 est réalisée grâce à du routage par politique de filtrage (PBR) basé sur un objet routeur avec partage de charge.

Le détail de la politique de gestion de trafic mise en place par l'administrateur est décrit ci-dessous.



Limitation et réservation de bande passante sur le lien WAN

i NOTE

La somme des réservations de bande passante pour un lien doit être au maximum égale à 85% de la bande passante totale de ce lien. En effet, la bande passante utilisable pour ces réservations est égale à la bande passante affectée au Traffic shaper correspondant (90% de la bande passante totale) moins la bande passante affectée à la file d'attente d'acquittement (5% de la bande passante totale).

Transferts de fichiers métier (FTP)

On définit une file d'attente nommée *FTP_WAN_Q* :

- Réservation de 10 Mbit/s et limitation à 20 Mbit/s pour les flux sortants,
- Réservation de 10 Mbit/s et limitation à 20 Mbit/s pour les flux retour.



Partage de fichiers sur un serveur externe (exemple : *Google Drive*)

On définit une file d'attente nommée *GD_WAN_Q* :

- Réserve de 10 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 10 Mbit/s et limitation à 20 Mbit/s pour les flux retour.

Communications en VoIP et flux de visioconférence

On définit une file d'attente nommée *SIP_WAN_Q* :

- Réserve de 15 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 15 Mbit/s et pas de limitation pour les flux retour.

Limitation et réservation de bande passante sur les liens WAN et WAN2

Transferts de fichiers HTTP / HTTPS vers et depuis le serveur métier externe

On définit une file d'attente nommée *HTTP_WAN_Q* :

- Réserve de 40 Mbit/s et pas de limitation pour les flux sortants,
- Réserve de 40 Mbit/s et pas de limitation pour les flux retour.

Créer l'objet routeur à utiliser dans la règle de PBR HTTP / HTTPS

i NOTE

Pour plus d'informations sur l'utilisation et la configuration d'objets routeur, consultez le **Manuel Utilisateur SNS v4** (section [Objets réseau > Les différents types d'objets > Routeur](#)) ainsi que la **Note Technique SD-WAN - Sélectionner le meilleur lien réseau**.

Dans cet exemple, la disponibilité des liens WAN et WAN2 est testée à l'aide de la méthode de détection *ICMP*. Ces tests de disponibilités sont dirigés vers le serveur hébergeant le service à joindre (*WAN_Prod_Server* dans cet exemple).

Dans le menu **Configuration > Objets > Réseau** :

1. Cliquez sur **Ajouter**.
La fenêtre de création et d'édition d'objets s'affiche.
2. Dans le menu de gauche, sélectionnez **Routeur**.
3. Nommez l'objet (exemple : *WAN_WAN2_Router* dans cet exemple).

Supervision

4. Pour la **Méthode de détection**, sélectionnez *ICMP*.

i NOTE

Si vous souhaitez utiliser un objet routeur pour les flux SIP, il est recommandé de cocher la case **SLA SD-WAN** et de configurer des seuils pour la **Latence (ms)**, la **Gigue (ms)** et / ou le **Taux de perte de paquets (%)**.
Pour ce faire, reportez-vous à la **Note Technique SD-WAN - Sélectionner le meilleur lien réseau**.

Passerelles



5. Dans l'onglet **Passerelles utilisées**, cliquez sur **Ajouter**.
6. Dans la colonne **Passerelle**, sélectionnez l'objet correspondant au routeur du lien WAN (*WAN_Router* dans cet exemple).
7. Dans la colonne **Cible(s) des tests**, sélectionnez l'objet *WAN_Prod_Server*.
8. Répétez les étapes 6 à 8 pour ajouter l'objet correspondant au routeur du lien WAN2 (*WAN2_Router* dans cet exemple).
La cible des tests pour cette passerelle est également l'objet *WAN_Prod_Server*.

Configuration avancée

Afin de conserver une qualité de lien optimale dans un maximum de cas, l'objet routeur *WAN_WAN2_Router* est configuré avec de la répartition de charge entre les liens utilisés.

9. Dans le cadre **Configuration avancée**, sélectionnez l'option de **Répartition de charge Par connexion**.
10. Cliquez sur **Appliquer** puis **Sauvegarder**.

L'objet routeur *WAN_WAN2_Router* défini dans cet exemple prend donc la forme suivante :

The screenshot shows the configuration page for the object *WAN_WAN2_Router*. It includes a 'Monitoring' section with the following settings:

- Detection method: ICMP
- Timeout (s): 1
- Interval (s): 5
- Failures before degradation: 5
- SD-WAN SLA (thresholds)

Below the monitoring section, there are two tabs: 'USED GATEWAYS' and 'BACKUP GATEWAYS'. The 'USED GATEWAYS' tab is active, showing a table with two entries:

	Gateway	Weight	Device(s) for testing availa...	Comments
1	WAN_Router	1	WAN_PROD_Server	
2	WAN2_Router	1	WAN_PROD_Server	

At the bottom, there is an 'Advanced configuration' section with a 'Load balancing' dropdown menu set to 'By connection'.

Créer les files d'attente

Dans cet exemple, on considère que les files d'attente d'acquittement (ACK) par défaut et les files d'attente par défaut pour les interfaces *LAN*, *WAN* et *WAN2* sont existantes et ont été créées comme décrit dans la section [Configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2](#).

Créer la file d'attente pour les flux FTP

Placez-vous dans le module **Politique de sécurité** > **Qualité de service** > onglet **Files d'attente** :



1. Cliquez sur **Ajouter**.
2. Sélectionnez **Réservation ou limitation de bande passante (CBQ)**.
3. Nommez la file d'attente (*FTP_WAN_Q* dans cet exemple).
4. Sur la ligne **Bp garantie**, spécifiez 10 Mbit/s.
5. Sur la ligne **Bp max**, spécifiez 20 Mbit/s.
6. Sur la ligne **Bp inv. garantie**, spécifiez 10 Mbit/s.
7. Sur la ligne **Bp inv. max**, spécifiez 20 Mbit/s.
8. Validez en cliquant sur **Appliquer**.

Créer la file d'attente pour le partage de fichiers *Google Drive*

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>GD_WAN_Q</i>
Bp garantie	10 Mbit/s
Bp max	illimité
Bp inv. garantie	10 Mbit/s
Bp inv. max	20 Mbit/s

Créer la file d'attente pour les flux métier HTTP / HTTPS

Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>HTTP_WAN_Q</i>
Bp garantie	40 Mbit/s
Bp max	illimité
Bp inv. garantie	40 Mbit/s
Bp inv. max	illimité

Créer la file d'attente pour les flux SIP

1. Suivez la procédure détaillée dans [Créer la file d'attente pour les flux FTP](#) avec les valeurs suivantes pour cet exemple :

Type de file d'attente	Réservation ou limitation de bande passante (CBQ)
Nom	<i>SIP_WAN_Q</i>
Bp garantie	15 Mbit/s



Bp max	illimité
Bp inv. garantie	15 Mbit/s
Bp inv. max	illimité

La grille des files d'attente de QoS définies dans cet exemple prend donc la forme suivante :

QUEUES						
Q 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. Validez les modifications de la configuration de la QoS en cliquant sur **Appliquer**.

Créer les Traffic shapers

Dans cet exemple, on considère que les Traffic shapers des interfaces *LAN*, *WAN* et *WAN2* sont existants et ont été créés comme décrit dans la section [Créer la configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2](#).

! IMPORTANT

La QoS ne peut pas être mise en œuvre sur des Traffic shapers supérieurs à 1 Gbit/s.

La grille des Traffic shapers définis dans cet exemple prend donc la forme suivante :

TRAFFIC SHAPER				
Q 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

Configurer les interfaces concernées par la QoS

Dans cet exemple, on considère que les interfaces soumises à la QoS (interfaces *LAN*, *WAN* et *WAN2*) ont été configurées comme décrit dans les sections [Configuration minimale nécessaire pour appliquer de la QoS : exemple d'une architecture de type LAN / WAN](#) et [Créer la](#)



configuration minimale nécessaire pour appliquer de la QoS dans une architecture de type LAN / WAN / WAN2.

La grille des interfaces concernées par la QoS dans cet exemple prend donc la forme suivante :

INTERFACES WITH QOS			
🔍 Enter a filter			
Select all + Add X 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

Créer les règles de PBR et de filtrage utilisant des files d'attente de QoS

i NOTE


Dans cette section, seule la création des règles de PBR et de filtrage utilisant des files d'attente de QoS spécifiques, autres que les files d'attente par défaut, est décrite. La création des règles de filtrage pour les flux non soumis à la QoS n'est pas abordée.

i NOTE

Il est déconseillé de préciser les files d'attente acquittement (ACK) au sein des règles de filtrage. Il est en effet préférable de laisser les flux de type ACK emprunter automatiquement les files d'attente d'acquittement (ACK) définies par défaut pour les interfaces concernées par ces flux.

Placez-vous dans le module **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage**.

Créer la règle de filtrage vers le serveur FTP distant

1. Dans la liste déroulante située au-dessus de la grille de filtrage, sélectionnez la politique de sécurité à modifier.
2. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches .
4. Double cliquez sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
5. Cliquez sur le menu de gauche **Général**.
6. Dans le champ **État**, sélectionnez la valeur *On*.
7. Cliquez sur le menu de gauche **Action**.
8. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
9. Dans l'onglet **Qualité de service**, pour le champ **File d'attente** du cadre **QoS**, sélectionnez la file d'attente créée pour les flux FTP (*FTP_WAN_Q* dans cet exemple).
10. Cliquez sur le menu de gauche **Source**.
11. Dans l'onglet **Général**, pour le champ **Machines sources**, sélectionnez les machines, les groupes de machines ou les réseaux autorisés à utiliser le protocole FTP (réseau *LAN_Clients* dans cet exemple).




12. Cliquez sur le menu de gauche **Destination**.
13. Dans l'onglet **Général**, pour le champ **Machines destinations**, cliquez sur **Ajouter** et sélectionnez le serveur ou le groupe de serveurs FTP (machine *WAN_FTP_Server* dans cet exemple).
14. Cliquez sur le menu de gauche **Port / Protocole**.
15. Dans le cadre **Port**, sélectionnez l'objet *ftp* comme **Port destination**.
16. Validez la création de la règle en cliquant sur **OK**.


i NOTE

Dans le cas d'un protocole générant des connexions filles (FTP dans cet exemple), la file d'attente précisée dans la règle de filtrage s'applique automatiquement aux connexions filles.

Créer la règle de filtrage vers le serveur de fichiers distant

1. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
2. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches .
3. Effectuez un double clic sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
4. Cliquez sur le menu de gauche **Général**.
5. Dans le champ **État**, sélectionnez la valeur *On*.
6. Cliquez sur le menu de gauche **Action**.
7. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
8. Dans l'onglet **Qualité de service**, pour le champ **File d'attente** du cadre **QoS**, sélectionnez la file d'attente créée pour les flux Google Drive (*GD_WAN_Q* dans cet exemple).
9. Cliquez sur le menu de gauche **Source**.
10. Dans l'onglet **Général**, pour le champ **Machines sources**, sélectionnez les machines, les groupes de machines ou les réseaux autorisés à accéder à *Google Drive* (réseau *LAN_Clients* dans cet exemple).
11. Cliquez sur le menu de gauche **Destination**.
12. Dans le cadre **Services Web et Réputation** de l'onglet **Géolocalisation / Réputation**, sélectionnez l'objet *Google Drive*.
13. Cliquez sur le menu de gauche **Port / Protocole**.
14. Dans le cadre **Port**, sélectionnez l'objet *https* comme **Port destination**.
15. Validez la création de la règle en cliquant sur **OK**.

Créer la règle de PBR vers le serveur HTTP / HTTPS distant

1. Sélectionnez la règle au-dessous de laquelle vous souhaitez ajouter une nouvelle règle de filtrage.
2. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
Une nouvelle règle inactive est ajoutée à la politique de filtrage.
Vous pouvez déplacer cette nouvelle règle à l'aide des flèches .



- Effectuez un double clic sur cette règle.
La fenêtre de configuration de la règle s'ouvre.
- Cliquez sur le menu de gauche **Général**.
- Dans le champ **État**, sélectionnez la valeur *On*.
- Cliquez sur le menu de gauche **Action**.
Dans l'onglet **Général** :
 - Dans le cadre **Général**, pour le champ **Action**, choisissez *passer*.
 - Dans le cadre **Routing**, pour le champ **Passerelle - routeur**, sélectionnez l'objet *WAN_WAN2_Router*.
- Dans l'onglet **Qualité de service**, pour le champ **File d'attente** du cadre **QoS**, sélectionnez la file d'attente créée pour les flux HTTPS / HTTPS (*HTTP_WAN_Q* dans cet exemple).
- Cliquez sur le menu de gauche **Source**.
- Dans l'onglet **Général**, pour le champ **Machines sources** sélectionnez les machines, les groupes de machines ou les réseaux autorisés à accéder au serveur de production distant (réseau *LAN_Clients* dans cet exemple).
- Cliquez sur le menu de gauche **Destination**.
- Dans l'onglet **Général**, pour le champ **Machines destinations**, cliquez sur **Ajouter** et sélectionnez l'objet correspondant au serveur HTTP /HTTPS distant (*WAN_PROD_Server* dans cet exemple).
- Cliquez sur le menu de gauche **Port / Protocole**.
- Dans le cadre **Port**, sélectionnez les objets *http* et *https* comme **Port destination**.
- Validez la création de la règle en cliquant sur **OK**.

Créer la règle de filtrage vers le serveur VoIP distant

Suivez la procédure détaillée dans [Créer la règle de filtrage vers le serveur FTP distant](#) avec les valeurs suivantes pour cet exemple :

État	<i>on</i>
Action	<i>passer</i>
File d'attente	<i>SIP_WAN_Q</i>
Machines sources	<i>LAN_VoIP_Clients</i>
Machines destinations	l'objet correspondant au serveur VoIP distant (<i>WAN_VoIP_Server</i> dans cet exemple)
Port destination	l'objet <i>sip</i>

i NOTE

Dans le cas d'un protocole générant des connexions filles (SIP dans cet exemple), la file d'attente précisée dans la règle de filtrage s'applique automatiquement aux connexions filles.

Appliquer la politique de sécurité modifiée

Pour appliquer la nouvelle politique de sécurité, cliquez sur **Appliquer** puis sur **Oui, Activer la politique**.



Les règles de PBR et filtrage utilisant des files d'attente de QoS prennent donc la forme suivante :

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



Superviser la QoS

L'interface Web d'administration vous permet de visualiser de manière graphique la bande passante utilisée par les files d'attente définies sur votre firewall SNS.

Configurer la supervision

Placez-vous dans le module **Configuration > Notifications > Configuration de la supervision > onglet Configuration de la QoS**.

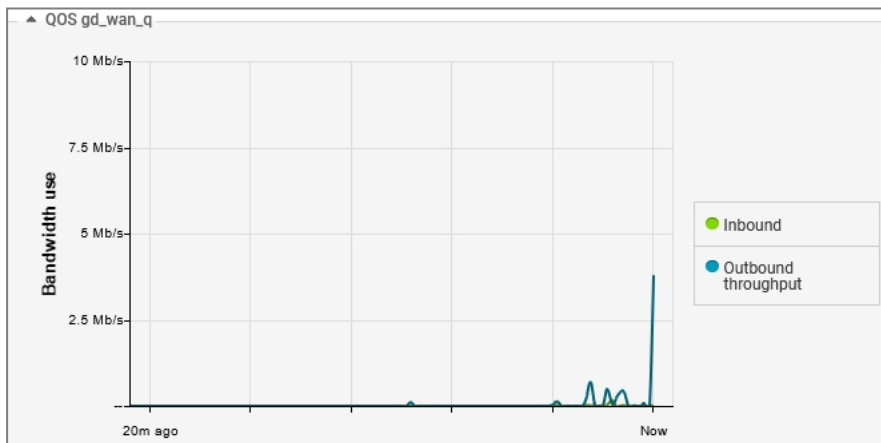
1. Cliquez sur **Ajouter**.
2. Sélectionnez la file d'attente que vous souhaitez superviser.
3. Répétez les étapes 1 et 2 pour toutes les files d'attentes à superviser.
4. Cliquez sur **Appliquer**.

Visualiser les graphes de bande passante utilisée par les files de QoS

Placez-vous dans le module **Monitoring > Supervision > QoS**.

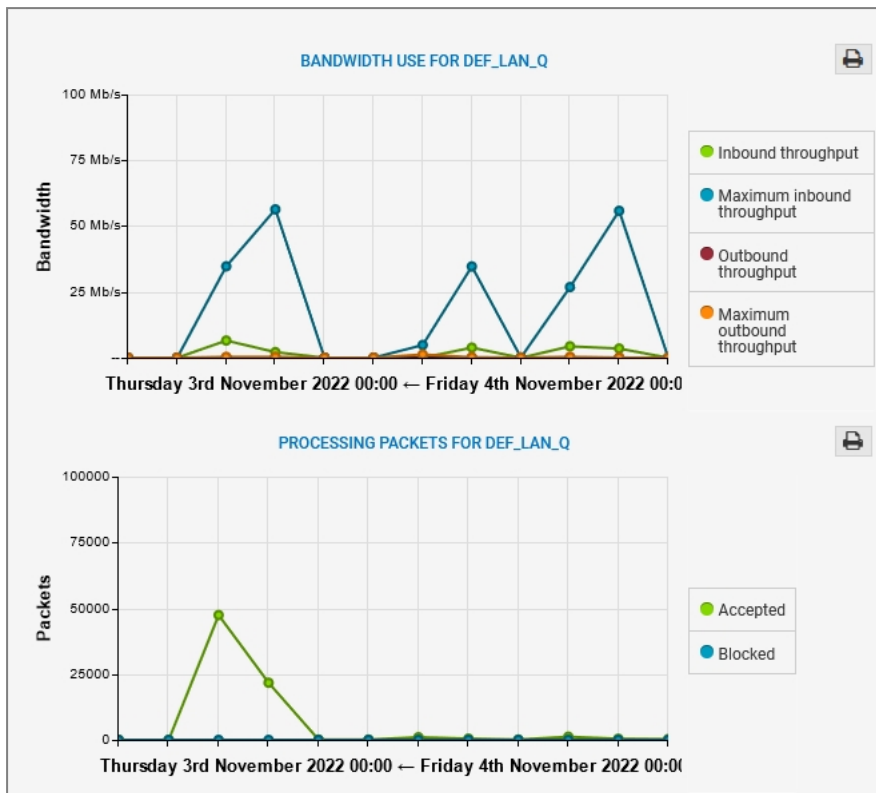
Onglet Temps réel

L'onglet **Temps réel** propose un graphe d'utilisation de bande passante pour chaque file d'attente de QoS supervisée. Ces graphes sont mis à jour en temps réel :



Onglet Historique

L'onglet **Historique** propose une agrégation des données d'utilisation de bande passante et de traitement des paquets pour chaque file d'attente de QoS supervisée :



La barre d'outils permet de sélectionner la période représentée :

- Dernière heure,
- Un jour en particulier,
- Les 7 derniers jours,
- Les 30 derniers jours.



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2024. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.