



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

GÉRER LE BYPASS DES FIREWALLS SNS

Dernière mise à jour du document : 15 janvier 2025

Référence : sns-fr-gerer_bypass_note_technique



Table des matières

Historique des modifications	3
Avant de commencer	4
Principe de fonctionnement du bypass	5
Composants du bypass et interactions	5
Microcontrôleur	5
Watchdog	5
Segment bypass	5
Modes de communication du bypass et principe de la commutation	6
Mode de communication normal	6
Mode de communication bypass	6
Délai de commutation	6
Modes de fonctionnement du bypass	7
Mode Sécurité	7
Mode Sûreté	7
Firewalls SNS et modules réseau équipés de bypass	8
SNi40	8
SNi20	8
SN-M-Series-520 (SN520)	8
SN-M-Series-720 (SN720) et SN-M-Series-920 (SN920)	9
SN1100	9
Module réseau 8 ports Cuivre 1Gbit/s (NA-EX-CARD-BP-8xG-C)	9
Configurer les interfaces d'un segment bypass	10
Accéder à la configuration des interfaces	10
Regrouper les interfaces du segment bypass dans un bridge	10
Optimiser la configuration des interfaces et du bridge	11
Paramétrer le même Média sur les deux interfaces du segment bypass	12
Désactiver les protocoles Spanning Tree sur le bridge	12
Configurer le mode Sûreté du bypass	13
Comprendre le fonctionnement du mode Sûreté	13
Événements déclencheurs du mécanisme de bypass en mode Sûreté	13
Délai de reprise	13
Accéder à la configuration du mode Sûreté	14
Activer ou désactiver le mode Sûreté	14
Définir le délai du compte à rebours du watchdog (seuil d'inactivité)	14
Réarmer le mécanisme de bypass (réarmement du mode Sûreté)	15
Vérifier l'état du bypass	16
Dans le module Tableau de bord	16
Dans la console CLI / Serverd	16
Dans la console CLI / SSH	16
Avec l'état des LED des connecteurs des ports réseau RJ45	17
Avec les journaux (logs)	18
Avec les MIB et Traps SNMP	18
Pour aller plus loin	19



Historique des modifications

Date	Description
15 janvier 2025	Nouveau document



Avant de commencer

La fonction de *bypass* présente sur certains firewalls SNS et modules réseau permet, lorsqu'elle est activée (prête à être déclenchée) et en cas de défaillance matérielle ou logicielle critique, de faire passer le trafic réseau au travers du firewall SNS sans qu'aucune analyse ne soit mise en œuvre.

Cette fonction permet d'assurer une continuité de service dans les milieux sensibles. À noter que, compte tenu de leur fonctionnement, la fonctionnalité de haute disponibilité des firewalls SNS et la fonction de *bypass* sont incompatibles.

Cette note technique présente :

- Des informations sur les composants du *bypass*, leurs interactions et les modes de communication et de fonctionnement de celui-ci,
- La liste des firewalls SNS et modules réseau équipés de *bypass*,
- Des informations sur les interfaces des segments *bypass* et l'insertion du module réseau,
- Le fonctionnement du mode Sûreté du *bypass* et sa configuration sur les firewalls SNS,
- Comment vérifier l'état du *bypass* des firewalls SNS.



Principe de fonctionnement du bypass

Cette section présente des informations sur les composants du *bypass*, leurs interactions et les modes de communication et de fonctionnement de celui-ci.

Composants du bypass et interactions

Microcontrôleur

Le microcontrôleur (ou *uController*) est un composant essentiel du *bypass*. Lorsqu'il déclenche le mécanisme de *bypass*, le mode de communication du *bypass* change. Ce changement est appelé "commutation".

On distingue deux commutations possibles :

- Lorsque le mécanisme de *bypass* est activé (prêt à être déclenché) et qu'une défaillance matérielle ou logicielle critique du firewall SNS survient, le microcontrôleur déclenche le mécanisme de *bypass*, ce qui commute le mode de communication du mode normal au mode *bypass*. Selon la défaillance rencontrée, le microcontrôleur déclenche le mécanisme de *bypass* immédiatement ou attend la fin du compte à rebours du *watchdog*.
- Lorsque le mécanisme de *bypass* a été déclenché, le mode de communication reste en mode *bypass* tant que le mécanisme de *bypass* n'est pas réarmé. Réarmer le mécanisme de *bypass* commute le mode de communication du mode *bypass* au mode normal.

Watchdog

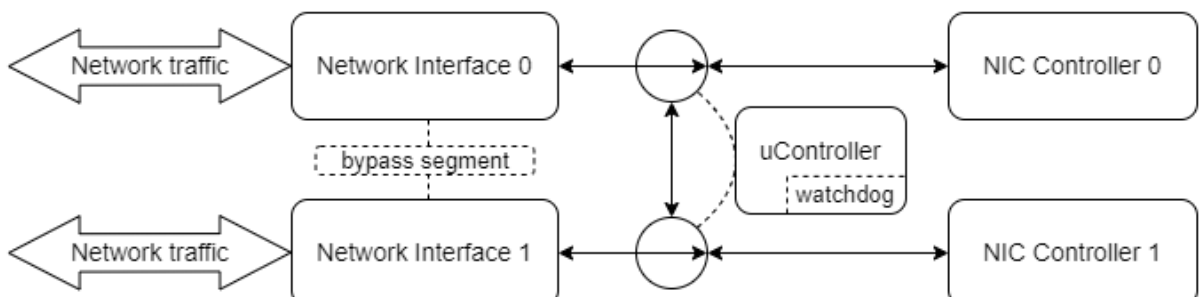
Intégré au microcontrôleur, le *watchdog* sert de compte à rebours dont le temps est défini dans la configuration du firewall SNS.

Lorsque l'état du *watchdog* ne peut plus être rafraîchi par le moteur de gestion du matériel du firewall SNS, notamment lorsque le système d'exploitation du firewall SNS ne répond plus ou est surchargé, le compte à rebours se déclenche. Une fois à zéro, le seuil d'inactivité est atteint et le microcontrôleur déclenche le mécanisme de *bypass* (commutation en mode *bypass*).

Segment bypass

Un segment *bypass* est composé de deux interfaces associées par paire. Cette association est figée matériellement et ne peut pas être modifiée.

Lorsque le mécanisme de *bypass* est déclenché (commutation en mode *bypass*), c'est le trafic réseau du segment *bypass* qui est intégralement dérivé d'une interface à l'autre et passe au travers du firewall SNS sans qu'aucune analyse ne soit mise en œuvre.





Modes de communication du bypass et principe de la commutation

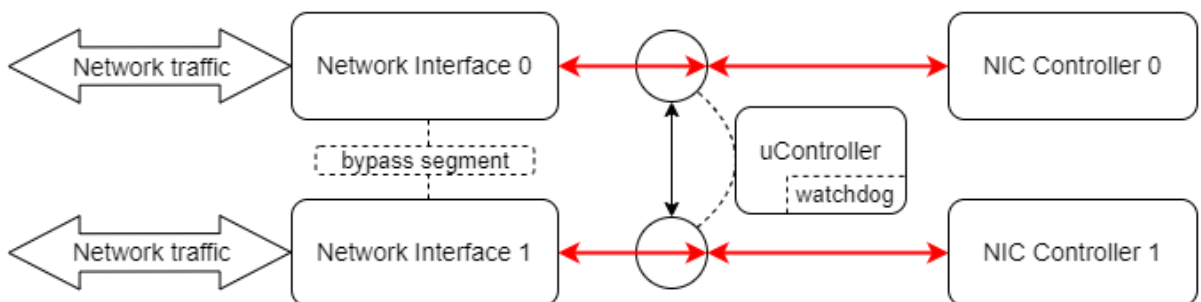
La commutation du mode de communication du *bypass* repose sur le mécanisme de *bypass*. Lorsqu'il est déclenché, le mode de communication des interfaces du segment *bypass* commute d'un mode à un autre.

Il existe deux modes de communication du *bypass*.

Mode de communication normal

C'est le mode de communication par défaut du *bypass*.

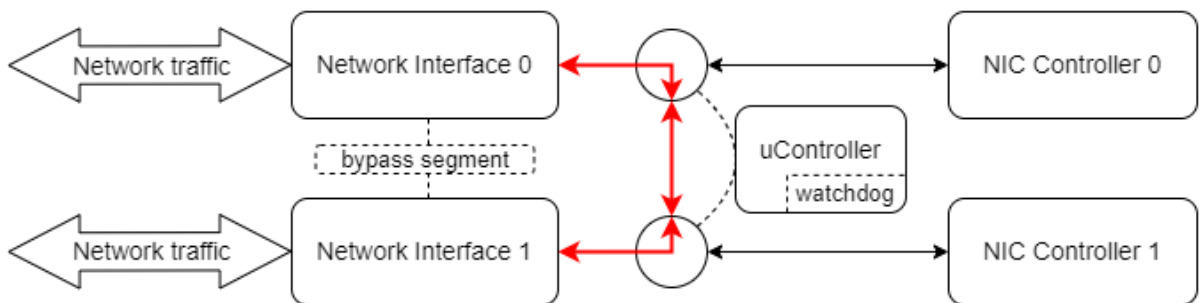
Dans ce mode, les connexions des interfaces réseau du segment *bypass* sont connectées aux contrôleurs réseau. Le trafic réseau est alors soumis aux règles de sécurité du firewall SNS.



Mode de communication bypass

Ce mode est utilisé uniquement lorsque le mécanisme de *bypass* a été déclenché.

Dans ce mode, les connexions des interfaces réseau du segment *bypass* sont déconnectées des contrôleurs réseau et dérivées vers l'autre interface pour créer une connexion croisée en boucle. Le trafic réseau est alors intégralement dérivé d'une interface à l'autre et passe au travers du firewall SNS sans qu'aucune analyse ne soit mise en œuvre.



Délai de commutation

C'est le délai nécessaire au mécanisme de *bypass* pour commuter le mode de communication du *bypass* d'un mode à un autre. Ce délai est de 100 ms environ.

! IMPORTANT

Le délai de commutation ne correspond pas au délai de reprise car d'autres éléments sont à prendre en compte. Ce délai est expliqué dans la section [Configurer le mode Sûreté du bypass](#).



Modes de fonctionnement du bypass

Deux modes de fonctionnement permettent d'interagir avec les modes de communication du *bypass*.

Mode Sécurité	Mode Sûreté
Privilégie la sécurité et la protection du réseau.	Privilégie la continuité de service.
Mode de fonctionnement par défaut tant que le mode Sûreté n'est pas activé.	Mode de fonctionnement à activer manuellement dans la configuration du firewall SNS.
La fonction de <i>bypass</i> reste désactivée en permanence .	Le mécanisme de <i>bypass</i> est activé, c'est-à-dire prêt à être déclenché.
Le mode de communication du <i>bypass</i> reste en permanence en mode normal.	Lorsqu'un événement déclencheur survient, le mécanisme de <i>bypass</i> est alors déclenché, ce qui commute le mode de communication du <i>bypass</i> .

NOTE

Le mode Sûreté est expliqué dans la section [Configurer le mode Sûreté du bypass](#).



Firewalls SNS et modules réseau équipés de bypass

Cette section présente les firewalls SNS et les modules réseau équipés de *bypass*.

i NOTE

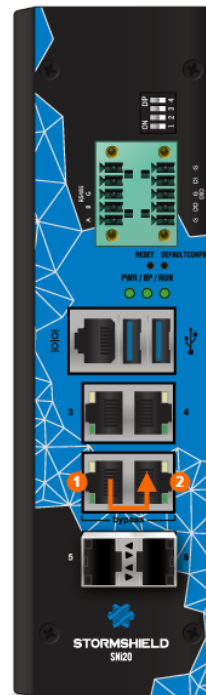
Pour les firewalls SNS nécessitant un module réseau, seul l'emplacement d'insertion du module est précisé. Pour plus d'informations, reportez-vous aux [Procédures d'insertion ou d'extraction de modules d'extension](#) du *Guide de présentation et d'installation SNS*.

SNi40



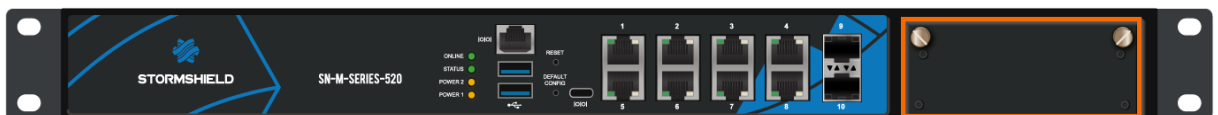
- Nombre de *bypass* : 1,
- *Bypass* inclus,
- Les interfaces "in" et "out" sont associées par paire et forment un segment *bypass*.

SNi20



- Nombre de *bypass* : 1,
- Option de licence requise,
- Les interfaces "in" et "out" sont associées par paire et forment un segment *bypass*.

SN-M-Series-520 (SN520)



- Un module réseau est requis pour bénéficier du *bypass*. Il doit être inséré dans l'emplacement d'extension prévu à cet effet.

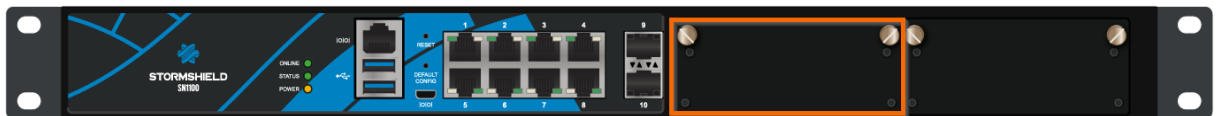


SN-M-Series-720 (SN720) et SN-M-Series-920 (SN920)



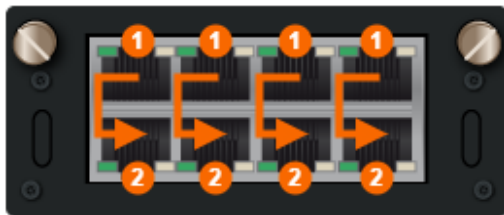
- Un module réseau est requis pour bénéficier du *bypass*. Il doit être inséré dans l'emplacement d'extension prévu à cet effet.

SN1100



- Un module réseau est requis pour bénéficier du *bypass*. Il doit être inséré dans l'emplacement d'extension **de gauche**.
- Le BIOS du firewall SNS doit être en version R1.01 ou supérieure pour assurer le bon fonctionnement du *bypass*. Pour plus d'informations, reportez-vous à la note technique [SN1100 - Mise à jour du BIOS en version R1.01](#).

Module réseau 8 ports Cuivre 1Gbit/s (NA-EX-CARD-BP-8xG-C)



- Nombre de *bypass* : 4,
- Firewalls SNS compatibles : SN-M-Series-520, SN-M-Series-720, SN-M-Series-920 et SN1100,
- Version minimale SNS requise : 4.8.1,
- Les interfaces sont associées verticalement par paire et forment des segments *bypass*.



Configurer les interfaces d'un segment *bypass*

Cette section présente la configuration des interfaces d'un segment *bypass* dans l'interface Web d'administration des firewalls SNS.

Accéder à la configuration des interfaces

Rendez-vous dans **Configuration > Réseau > Interfaces**.

Dans la grille :

- L'icône indique l'interface de connexion au firewall SNS. Si vous modifiez l'adresse IP de cette interface pendant vos manipulations, la connexion au firewall SNS sera perdue et vous devrez utiliser la nouvelle adresse IP pour vous reconnecter.

Interface	Port	Type	Status	IPv4 address	Comm
out	1	Ethernet, 1 Gbit/s			
in	2	Ethernet, 1 Gbit/s			
dmz1	3	Ethernet, 1 Gbit/s			
dmz2	4	Ethernet	Disabled, Not connected		

- L'icône indique qu'une interface est associée à un segment *bypass*. Cette icône n'est pas visible sur les versions SNS 4.3 LTSB. Si plusieurs segments *bypass* sont disponibles, vous pouvez passer votre souris sur l'icône pour afficher le nom de l'autre interface du segment *bypass*.

dmz12	14	Ethernet	Disabled, Not connected
dmz13	15	Ethernet	Disabled, Not connected
dmz14	16	Ethernet	Disabled, Not connected

The bypass mechanism will be enabled on this interface only if it is included in the same bridge as the dmz13 interface.

Type: Ethernet, Protected
Status: Disabled, Not connected
Port: 16
System name: igb5

Regrouper les interfaces du segment *bypass* dans un bridge

Pour activer le mécanisme de *bypass* sur un segment *bypass*, vous devez regrouper ses deux interfaces dans un bridge. Même si ce regroupement n'est pas obligatoire pour les firewalls SNI40 et SNI20, il est fortement recommandé.

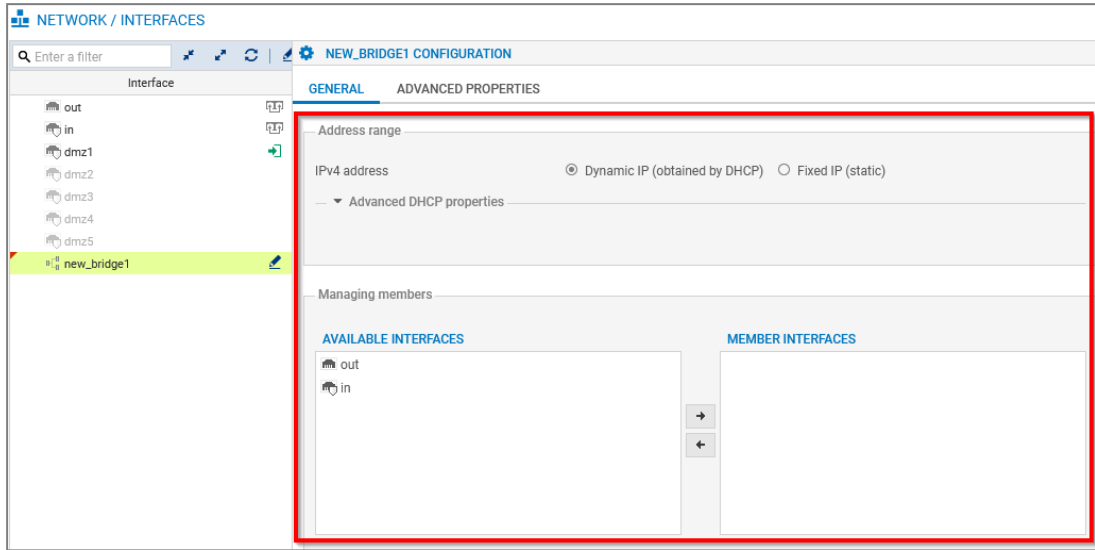
NOTE

Pour les firewalls SNS équipés d'un module réseau, le mécanisme de *bypass* ne peut pas être activé sur des interfaces du module incluses dans un agrégat.

- Accédez à la configuration des interfaces.
- Cliquez sur **Ajouter > Bridge > Sans membre**.
- Définissez un nom au bridge et cliquez sur **Appliquer**.
- La fenêtre de configuration du bridge s'affiche. Dans la zone **Plan d'adressage**, définissez le plan d'adressage souhaité.




5. Dans la zone **Gestion des membres**, sélectionnez les interfaces du segment *bypass* concerné.

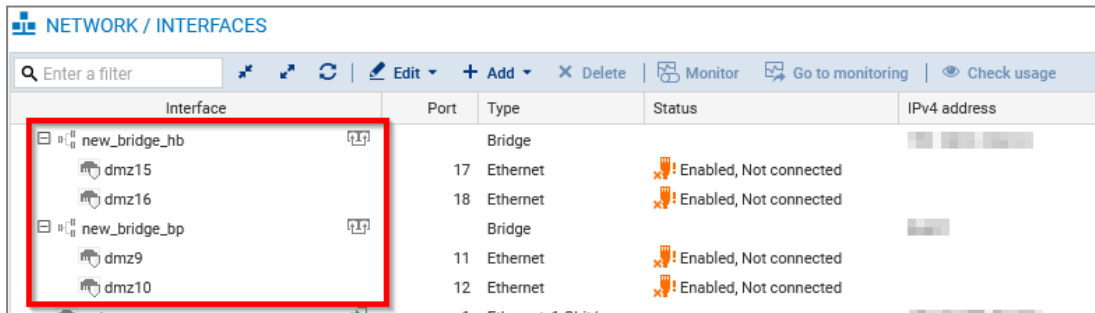



6. Cliquez sur **Appliquer**.

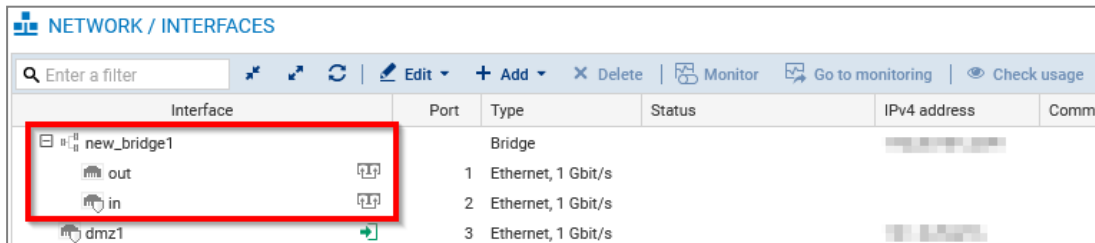
Si les interfaces concernées et/ou le plan d'adressage renseigné sont déjà utilisés dans la configuration du firewall SNS, des erreurs s'affichent dans la zone **Vérification de la configuration**. Dans ce cas, vous devez adapter la configuration du firewall SNS et/ou choisir un autre plan d'adressage avant de pouvoir regrouper les interfaces dans un bridge.

Une fois le bridge créé avec les interfaces du segment *bypass* :

- Pour les firewalls SNS disposant de plusieurs *bypass*, l'icône  est à présent à côté du bridge,



- Pour les firewalls SNi40 et SNi20, l'icône  reste à côté des interfaces du segment *bypass*.



Optimiser la configuration des interfaces et du bridge

Vous pouvez optimiser la configuration des interfaces du segment *bypass* et du bridge pour accélérer le processus de *bypass*. Ces optimisations sont recommandées.



Paramétrer le même Média sur les deux interfaces du segment bypass

1. Accédez à la configuration des interfaces.
2. Double-cliquez sur la première interface du segment *bypass*.
3. Dans l'onglet **Configuration avancée**, sélectionnez le **Média** adapté à votre environnement.
4. Cliquez sur **Appliquer**.

The screenshot shows the 'NETWORK / INTERFACES' configuration page. On the left, a tree view shows a bridge named 'new_bridge1' with two interfaces: 'out' and 'in'. The 'out' interface is selected. The main panel shows the 'OUT CONFIGURATION' for this interface, with the 'ADVANCED PROPERTIES' tab active. Under 'Other settings', there are fields for MTU (1500), MAC address, and Physical MAC address. At the bottom, the 'Media' section is highlighted with a red box, showing a dropdown menu set to '100 Mbit/s full duplex'.

5. Double-cliquez sur la seconde interface du segment *bypass*.
6. Dans l'onglet **Configuration avancée**, sélectionnez le même **Média**.
7. Cliquez sur **Appliquer**.

Désactiver les protocoles Spanning Tree sur le bridge

1. Accédez à la configuration des interfaces.
2. Double-cliquez sur le bridge regroupant les deux interfaces du segment bypass.
3. Dans l'onglet **Configuration avancée**, zone **Détection de boucles (Spanning Tree)**, assurez-vous que **Désactiver les protocoles Spanning Tree** soit sélectionné.
4. Cliquez sur **Appliquer**.

The screenshot shows the 'NETWORK / INTERFACES' configuration page. On the left, a tree view shows a bridge named 'new_bridge1'. The bridge is selected. The main panel shows the 'NEW_BRIDGE1 CONFIGURATION' for this bridge, with the 'ADVANCED PROPERTIES' tab active. Under 'Other settings', there are fields for MTU (1500), MAC address, and Physical MAC address. At the bottom, the 'Loops detection (Spanning Tree)' section is highlighted with a red box. It contains three radio buttons: 'Disable Spanning Tree protocols' (which is selected), 'Enable Rapid Spanning Tree Protocol (RSTP)', and 'Enable Multiple Spanning Tree Protocol (MSTP)'.



Configurer le mode Sûreté du bypass

Cette section présente le fonctionnement du mode Sûreté du *bypass* et sa configuration dans l'interface Web d'administration des firewalls SNS.

Comprendre le fonctionnement du mode Sûreté

Le mode Sûreté privilégie la continuité de service. Lorsque ce mode est activé :

- Le mécanisme de *bypass* est activé (prêt à être déclenché) sur tous les segments *bypass* configurés pour l'utiliser,
- Lorsqu'un événement déclencheur survient, le mécanisme de *bypass* est déclenché, ce qui commute le mode de communication du *bypass* en mode *bypass*,
- Une fois le mécanisme de *bypass* déclenché, seul un réarmement du mécanisme de *bypass* permet de commuter le mode de communication du *bypass* en mode normal.

Si le mode Sûreté n'est pas activé, c'est le **mode Sécurité** qui est utilisé. Dans ce mode, la fonction de *bypass* reste **désactivée en permanence**, même si une défaillance critique survient.

Événements déclencheurs du mécanisme de bypass en mode Sûreté

Le mécanisme de *bypass* est déclenché lorsque l'un de ces événements survient :

- Lors d'une défaillance électrique du firewall SNS ou d'une coupure de courant,
- Lors d'un redémarrage du firewall SNS, une fois le BIOS initialisé,

i NOTE

Le mécanisme de *bypass* est automatiquement réarmé une fois le firewall SNS redémarré.

- Lors d'une défaillance logicielle, notamment lorsque le système d'exploitation du firewall SNS ne répond plus ou est surchargé, après écoulement du compte à rebours du **watchdog**.

Délai de reprise

C'est le délai nécessaire pour assurer la continuité du service. Selon l'événement déclencheur, vous devez additionner tous les délais du tableau ou seulement certains pour déterminer le délai de reprise théorique.

Élément	Délai nécessaire à la reprise (à additionner)
Délai du compte à rebours du <i>watchdog</i>	1 à 4 minutes, selon le délai défini dans la configuration du mode Sûreté. Le compte à rebours démarre lorsque l'état du <i>watchdog</i> ne peut plus être rafraîchi par le moteur de gestion du matériel du firewall SNS, notamment lors d'une défaillance logicielle . Une fois le compte à rebours à zéro, le seuil d'inactivité est atteint et le mécanisme de <i>bypass</i> est déclenché (communication en mode <i>bypass</i>).
Délai de commutation	100 ms environ. C'est le délai nécessaire pour commuter le mode de communication du <i>bypass</i> .
Délai de détection des équipements distants	Généralement de 3 à 10 secondes. Après une commutation, c'est le délai nécessaire aux équipements distants pour détecter le changement d'état ("DOWN" ou "UP") des interfaces du segment <i>bypass</i> . Ce délai varie selon l'équipement distant et la version installée sur le firewall SNS.



Accéder à la configuration du mode Sûreté

1. Rendez-vous dans **Configuration > Système > Configuration**, onglet **Configuration générale**.
2. Dépliez le cadre **Configuration avancée**.
La configuration du mode Sûreté se trouve dans la zone **Matériel**.

Sur les versions SNS 4.3 LTSB, l'interface est légèrement différente mais la configuration du mode Sûreté s'effectue de la même manière.

The screenshot shows the 'SYSTEM / CONFIGURATION' page with tabs for 'GENERAL CONFIGURATION', 'FIREWALL ADMINISTRATION', and 'NETWORK SETTINGS'. Under 'Advanced properties', the 'Idle timeout monitoring (watchdog)' section is visible, with the 'Idle timeout timer (watchdog)' set to '5m'. The 'Hardware' section is highlighted with a red border and contains the 'Enable safety mode' checkbox (unchecked), a dropdown menu set to '1 min', and a 'Reset safety mode' button.

Activer ou désactiver le mode Sûreté

Pour rappel, vous ne pouvez pas activer le mode Sûreté sur un firewall SNS configuré en haute disponibilité.

1. Accédez à la configuration du mode Sûreté.
Sur les firewalls SNS disposant de plusieurs *bypass*, une liste indique les segments *bypass* sur lesquels le mode Sûreté sera activé.
2. Cochez ou décochez la case **Activer le mode Sûreté**.
3. Cliquez sur **Appliquer**.

The screenshot shows the 'Hardware' section with an information message: 'Safety mode will be applied to the next pair of interfaces that are configured as a bridge [dmz9 - dmz10] ; [dmz15 - dmz16]'. Below the message is a link 'Go to network settings'. The 'Enable safety mode' checkbox is highlighted with a red border and is currently unchecked. Below it is a dropdown menu set to '1 min' and a 'Reset safety mode' button.

Définir le délai du compte à rebours du watchdog (seuil d'inactivité)

1. Accédez à la configuration du mode Sûreté.
2. Dans la liste déroulante en dessous de la case **Activer le mode Sûreté**, sélectionnez le délai souhaité. Les valeurs proposées vont de 1 minute à 4 minutes.
3. Cliquez sur **Appliquer**.



Hardware

i Safety mode will be applied to the next pair of interfaces that are configured as a bridge
[dmz9 - dmz10] ; [dmz15 - dmz16]
[Go to network settings](#)

Enable safety mode

1 min

Reset safety mode

Réarmer le mécanisme de bypass (réarmement du mode Sûreté)

Une fois le mécanisme de *bypass* déclenché, seul un réarmement permet de retrouver un fonctionnement où le firewall SNS effectue de nouveau ses analyses. Réarmer le mécanisme de *bypass* commute le mode de communication en mode normal, ce qui implique un **délai de reprise** correspondant aux délais de commutation et de détection des équipements distants.

Le mécanisme de *bypass* est automatiquement réarmé lorsque le firewall SNS termine sa phase de démarrage.

Vous pouvez réarmer manuellement le mécanisme de *bypass* dans l'interface Web d'administration des firewalls SNS.

1. Accédez à la configuration du mode Sûreté.
2. Cliquez sur le bouton **Réarmement du mode sûreté**.

Hardware

i Safety mode will be applied to the next pair of interfaces that are configured as a bridge
[dmz9 - dmz10] ; [dmz15 - dmz16]
[Go to network settings](#)

Enable safety mode

1 min

Reset safety mode

3. Dans la fenêtre qui s'affiche, confirmez le réarmement du mode Sûreté.

RESET SAFETY MODE

? This will reset safety mode. Continue anyway?

CANCEL RESET SAFETY MODE

i IMPORTANT

Après un réarmement manuel, vous devez vérifier le fonctionnement correct des flux réseau. En effet, les connexions initiées pendant la phase active du *bypass* seront interrompues et devront être rétablies à l'initiative des machines distantes.



Vérifier l'état du bypass

Cette section explique comment vérifier l'état du *bypass* des segments *bypass* d'un firewall SNS (mode Sûreté activé, mécanisme de *bypass* déclenché, etc.).

Dans le module Tableau de bord

Ce cas concerne exclusivement les versions SNS 4.8 et supérieures.

Dans l'interface Web d'administration, rendez-vous dans **Monitoring > Tableau de bord**. Le widget **Réseau** contient une représentation graphique des interfaces du firewall SNS :

- Lorsque le mode Sûreté est activé (mécanisme de *bypass* prêt à être déclenché), le numéro des interfaces des segments *bypass* apparaît dans un cercle orange,



- Lorsque le mécanisme de *bypass* a été déclenché, les interfaces des segments *bypass* apparaissent en orange avec une flèche bidirectionnelle les reliant.



Dans la console CLI / Serverd

Vous pouvez interagir avec le *bypass* avec le jeu de commandes **SYSTEM BYPASS** et la commande **MONITOR BYPASS**.

Dans la console CLI / SSH

Le mode de fonctionnement du *bypass* s'affiche dans un message après l'authentification :

- "Operating mode : Security" indique que le **mode Sécurité** est utilisé,
- "Operating mode : Safety" indique que le **mode Sûreté** est activé,
- "Operating mode : Bypass" indique que le mécanisme de *bypass* a été déclenché.

Dans la console CLI / SSH, vous pouvez interagir avec le *bypass* avec la commande **enbypass**.



```
Last login: Tue Dec 10 12:46:09 2024 from [redacted]
[redacted]: FW SNI40 (M / EUROPE)
Firewall software version 4.8.4 RELEASE

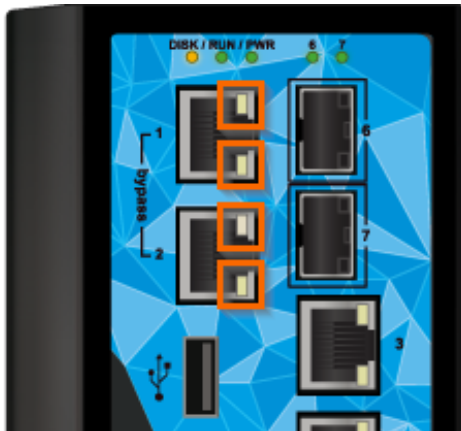
port      name      NS-BSD  state  addressIPv4  addressIPv6
  1        out       igb0    no-link
  2        in        igb1    no-link
  3        dmz1      igb4    up
  4        dmz2      igb5    down
  5        dmz3      igb6    down
  6        dmz4      igb2    down
  7        dmz5      igb3    down
Operating mode : Bypass
```

Avec l'état des LED des connecteurs des ports réseau RJ45

En accédant physiquement à l'emplacement où se situe le firewall SNS, vous pouvez vérifier l'état des LED des connecteurs des ports réseau RJ45 des segments *bypass*.

SNI40 et SNI20

Sur les firewalls SNI40 et SNI20, lorsque le mécanisme de *bypass* a été déclenché, les LED des connecteurs des ports réseau RJ45 du segment *bypass* sont éteintes.



Module réseau 8 ports Cuivre 1Gbit/s (NA-EX-CARD-BP-8xG-C)

Sur les firewalls SNS équipés du module réseau 8 ports Cuivre 1Gbit/s (NA-EX-CARD-BP-8xG-C), lorsque le mécanisme de *bypass* a été déclenché :

- Les LED des connecteurs des ports réseau RJ45 des segments *bypass* sont éteintes,
- Les LED de l'état du module réseau, habituellement vertes, sont rouges.

Mécanisme de *bypass* non déclenché



Mécanisme de *bypass* déclenché





Avec les journaux (logs)

Plusieurs journaux liés au *bypass* peuvent être générés. En voici quelques exemples :

Mécanisme de bypass déclenché car le compte à rebours du watchdog est arrivé à zéro

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz="+0200" starttime="YYYY-MM-DD HH:MM:SS" pri=6  
service=hardwared msg="Bypass mode triggered: timer expired"
```

Mode Sûreté du bypass activé (mécanisme de bypass prêt à être déclenché)

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz="+0200" starttime="YYYY-MM-DD HH:MM:SS" pri=5  
service=enbypass msg="Bypass activated on segments 0,1,2,3"
```

Sur les firewalls SNi40 et SNi20, les segments *bypass* concernés ne s'affichent pas.

Mécanisme de bypass réarmé (mode Sûreté réarmé)

```
id=firewall time="YYYY-MM-DD HH:MM:SS" fw="SNXXXXXXXXXXXX" tz="+0200" starttime="YYYY-MM-DD HH:MM:SS" pri=5  
service=enbypass msg="Run-time bypass watchdog rearmed"
```

Avec les MIB et Traps SNMP

Vous pouvez récupérer des informations sur l'état du *bypass* des segments *bypass* du firewall SNS avec la MIB **STORMSHIELD-SYSTEM-MONITOR-MIB**, table SNMP **snsBypassTable**.

Pour cela, vous devez :

- Récupérer les MIB SNMP depuis votre espace personnel [MyStormshield](#), dans **Téléchargements > Téléchargements > Stormshield Network Security > MIB SNMP**,
- Configurer le module **Agent SNMP** dans l'interface Web d'administration du firewall SNS.

Pour plus d'informations, reportez-vous à la section [Agent SNMP](#) du *Manuel Utilisateur SNS*.



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être 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 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.