



**STORMSHIELD**



NOTE TECHNIQUE

**STORMSHIELD NETWORK SECURITY**

# AGRÉGATION DE LIENS LACP

**Produit concerné :** SNS 1.0 et versions supérieures

**Version du document :** 1.0

**Référence :** sns-fr-agrégation\_de\_liens\_LACP\_note\_technique



## Table des matières

Introduction .....	3
Principes de l'agrégation de liens .....	4
Définition .....	4
LACP Stormshield - Conditions préalables .....	4
Mise en oeuvre par quelques éditeurs .....	5
EtherChannel de Cisco .....	5
Trunk de HP .....	5
Mettre en place l'atelier de tests .....	6
Topologie réseau utilisée dans ce document .....	6
Manipulation de test .....	7
Configurer le commutateur .....	7
Configurer le firewall Stormshield Network .....	8
Configurer le firewall par l'interface d'administration .....	8
Vérifier la configuration .....	10
Diagnostics sur le commutateur .....	11
Diagnostics sur le firewall Stormshield Network .....	12
Pour aller plus loin... ..	14
Activer le mode verbeux du LACP .....	14
Limites de l'agrégation de liens .....	14
Cluster HA SNS et LACP .....	14
Calculer le facteur de qualité de la HA avec LACP .....	15
Cas pratique 1 : un cluster Stormshield Network, un commutateur .....	15
Cas pratique 2 : un cluster Stormshield Network, deux commutateurs empilables .....	16



## Introduction

---

Ce document a pour objet de guider l'administrateur d'un firewall Stormshield Network dans la configuration et l'exploitation du protocole LACP (Link Aggregation Control Protocol), alias IEEE802.3ad.

Dans un premier temps seront décrits les principes de fonctionnement du protocole et les prérequis applicables aux équipements. Une configuration typique de LACP entre un firewall Stormshield Network et les commutateurs de marque Cisco et HP sera par la suite détaillée, accompagnée des informations nécessaires de dépannage.



# Principes de l'agrégation de liens

## Définition

L'agrégation de liens est le regroupement de plusieurs interfaces physiques distinctes en une interface logique.

Elle a pour objectifs :

- D'assurer une tolérance aux pannes en cas de perte d'un lien ou de problèmes sur une interface,
- D'augmenter la bande passante entre deux équipements interconnectés.

L'agrégation de liens peut être mise en place de diverses manières, généralement concurrentes et dépendantes des matériels.

Par exemple, entre un routeur et un commutateur, certains mécanismes comme l'*Adaptive transmit load balancing* ne requièrent aucune configuration sur le commutateur, contrairement au LACP qui nécessite une configuration des 2 équipements interconnectés.

## LACP Stormshield - Conditions préalables

LACP est supporté à partir de SNS v1.0. LACP avec la haute disponibilité est supporté à partir de SNS v2.0.

Il peut être mis en oeuvre sur les firewalls Stormshield Network suivants :

NG1000, NG5000, SN510, SN710, SN910, SN2000, SN3000, SN6000.

Tous les ports physiques agrégés doivent utiliser les mêmes paramètres :

- Vitesse,
- Duplex (half ou full),
- 802.1q (ID de VLAN unique ou liaison étiquetée multi-VLANs).

Le trafic sortant est émis sur les interfaces membres de l'agrégat (8 interfaces maximum).

LACP dispose de deux modes de fonctionnement :

- Le mode actif : l'équipement est à l'initiative de l'établissement de l'agrégat.
- Le mode passif : l'équipement ne fera que répondre aux requêtes LACP qu'il reçoit.

Les firewalls Stormshield Network ne fonctionnent qu'en mode actif. Ainsi, quel que soit le mode (actif ou passif) des commutateurs avec lesquels une négociation LACP sera menée, celle-ci aboutira.



## Mise en oeuvre par quelques éditeurs

### EtherChannel de Cisco

Les commutateurs Cisco sont compatibles avec la plupart des agrégations de liens courantes (LACP, PAgP, Bonding Round Robin,...). L'invite de commandes permet de regrouper plusieurs interfaces d'un commutateur dans un agrégat nommé EtherChannel (8 ports maximum), puis de configurer le mode de fonctionnement de cet agrégat. Tous les ports membres d'un agrégat EtherChannel doivent avoir la même vitesse.

### Trunk de HP

Les commutateurs HP utilisent par défaut le protocole normalisé LACP mais permettent la reconnaissance d'autres types d'agrégats de liens, en configuration statique. Cet agrégat est nommé Trunk.

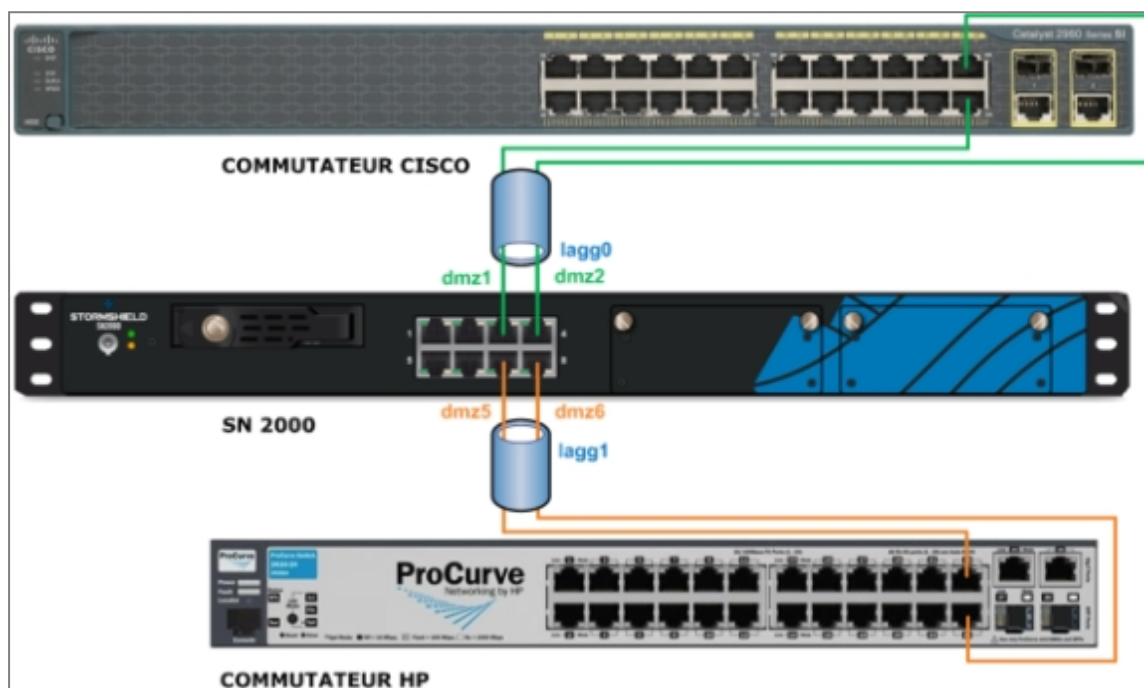
L'appellation Trunk chez Cisco représente une liaison entre deux éléments actifs, autorisant le passage de trames marquées 802.1q pour l'identification de réseaux VLANs. Pour ne pas créer d'ambiguïté, il est préférable de parler d'agrégation de liens plutôt que de Trunk ou d'EtherChannel.



## Mettre en place l'atelier de tests

### Topologie réseau utilisée dans ce document

Un agrégat de deux interfaces est défini sur un firewall Stormshield Network SN2000, pour chaque commutateur.



Le tableau suivant fournit les informations relatives aux interfaces d'un firewall Stormshield Network SN2000 :

Nom / numéro affiché (IHM)	Nom commun (fichier network)	Numéro de port visuel (boîtier)
mgmt1 /(1)	Ethernet0	1 (derrière)
mgmt2 /(2)	Ethernet1	2 (derrière)
out /(3)	Ethernet2	1 (devant)
in /(4)	Ethernet3	2 (devant)
dmz1 /(5)	Ethernet4	3 (devant)
dmz2 /(6)	Ethernet5	4 (devant)
dmz3 /(7)	Ethernet6	5 (devant)
dmz4 /(8)	Ethernet7	6 (devant)
dmz5 /(9)	Ethernet8	7 (devant)
dmz6 /(10)	Ethernet9	8 (devant)

Pour connaître le nom système, utilisez la commande `portinfo`.



## Manipulation de test

Lors de l'atelier, toutes les interfaces du SN 2000 appartiennent au bridge usine. Des pings sont effectués depuis un poste du réseau (Network\_bridge) vers l'adresse IP du bridge (firewall\_bridge) via l'interface agrégée du firewall.

Une règle de filtrage est configurée pour autoriser les notifications ICMP de type Echo Request.

## Configurer le commutateur

Puisque le firewall est en mode actif, le commutateur peut rester en mode passif.

La configuration détaillée ici suppose une connaissance préalable de l'interface en ligne de commande du constructeur.

Seule la mise en place de l'agrégation de liens sera présentée.

CLI CISCO	CLI HP	COMMENTAIRES
Switch(config)# interface range Gi 0/23-24	ProCurve(config)# trunk 23-24 trkl lacp	Configuration de l'agrégation en mode LACP passif sur les ports 23 et 24 dans cet exemple.
Switch(config-if-range)# channel-group 1 mode passive		
Switch(config-if-range)# channel-protocol lacp		
Switch(config-if-range)# exit	ProCurve(config)# vlan 2 tagged trkl	Commandes facultatives, permettant un marquage 802.1q sur le lien logique commutateur-routeur, en cas d'utilisation des VLANs 2 à 10 dans cet exemple.
Switch(config)# interface Port-channel 1	ProCurve(config)# vlan 3 tagged trkl	
Switch(config-if)#switchport mode trunk	...	
	...	
Switch(config-if)#switchport trunk allowed vlan 2-10	ProCurve(config-vlan)# vlan 10 tagged trkl	

### ! IMPORTANT

Pour éviter tout souci de couche 2 (instabilité de la table d'adresses MAC, tempête de diffusion, ...), réalisez la configuration de l'agrégat sur le firewall et sur le commutateur avant d'interconnecter les deux équipements.



## NOTES

- Après vérification du bon fonctionnement de l'agrégat (en provoquant une coupure de lien par exemple), vous devez sauvegarder la configuration du commutateur.
- La dénomination et la numérotation des interfaces varient en fonction du modèle de commutateur choisi. Consultez la notice de ce dernier.
- La fonctionnalité *Port-Security*, disponible sur les commutateurs Cisco et HP, n'est pas compatible avec LACP. Elle ne doit pas être configurée sur une ou plusieurs interfaces membres de l'agrégat.

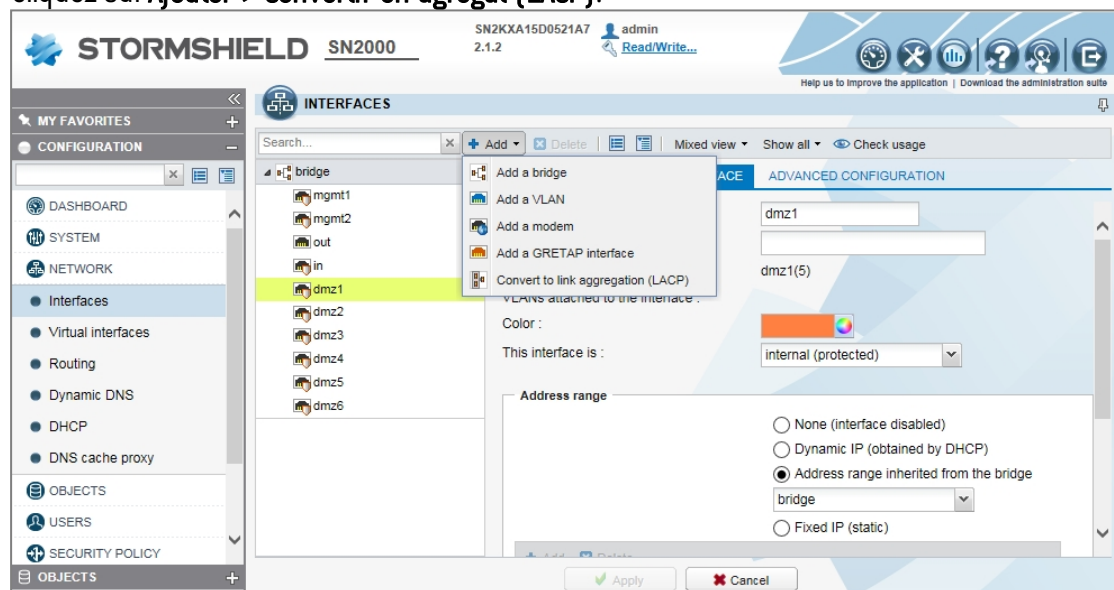
## Configurer le firewall Stormshield Network

La mise en œuvre d'une agrégation de liens sur un firewall Stormshield Network crée une interface dont le nom système est laggX, la numérotation de X commençant à zéro.

Le nombre maximum d'agrégats possibles sur un firewall Stormshield Network équivaut à N/2 [où N est le nombre de ports Ethernet].

## Configurer le firewall par l'interface d'administration

1. Dans l'écran de configuration des interfaces, sélectionnez la première interface à agréger, puis cliquez sur **Ajouter > Convertir en agrégat (LACP)**.



2. Dans la boîte de dialogue qui s'affiche, cliquez sur **Convertir** pour valider.
3. Dans l'onglet *Configuration de l'interface*, renommez l'interface dans le champ **Nom**.





The screenshot shows the 'INTERFACES' management page. On the left, a tree view shows a bridge with several interfaces, including 'dmz1' through 'dmz6'. The 'lACP\_cisco' interface is selected. The main panel shows the 'CONFIGURATION OF THE INTERFACE' tab. Fields include: Name (lACP\_cisco), Comments (empty), Physical ports (Ethernet\_4), VLANs attached to the interface (empty), Color (orange), and This interface is (internal (protected)). The 'Address range' section has four radio buttons: 'None (interface disabled)', 'Dynamic IP (obtained by DHCP)', 'Address range inherited from the bridge' (selected), and 'Fixed IP (static)'. The 'Address range' dropdown is set to 'bridge'. At the bottom are 'Apply' and 'Cancel' buttons.

4. Dans l'onglet *Agrégation de liens (LACP)*, ajoutez une interface à l'agrégat.

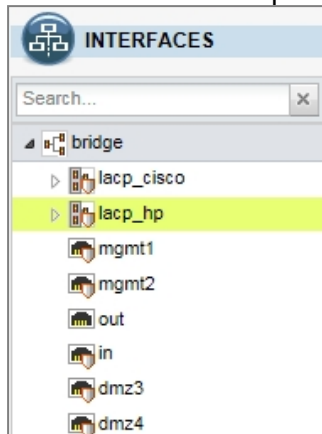
The screenshot shows the 'LINK AGGREGATION (LACP)' tab. It features two main panels: 'AVAILABLE INTERFACES' on the left and 'MEMBERS OF THE LINK AGGREGATION' on the right. The 'AVAILABLE INTERFACES' panel lists 'mgmt1', 'mgmt2', 'out', 'in', 'dmz3', 'dmz4', 'dmz5', and 'dmz6'. The 'MEMBERS OF THE LINK AGGREGATION' panel lists 'Ethernet\_4' and 'dmz2'. Arrows between the panels allow moving interfaces. At the bottom are 'Apply' and 'Cancel' buttons.

5. Vérifiez la prise en compte de la configuration.

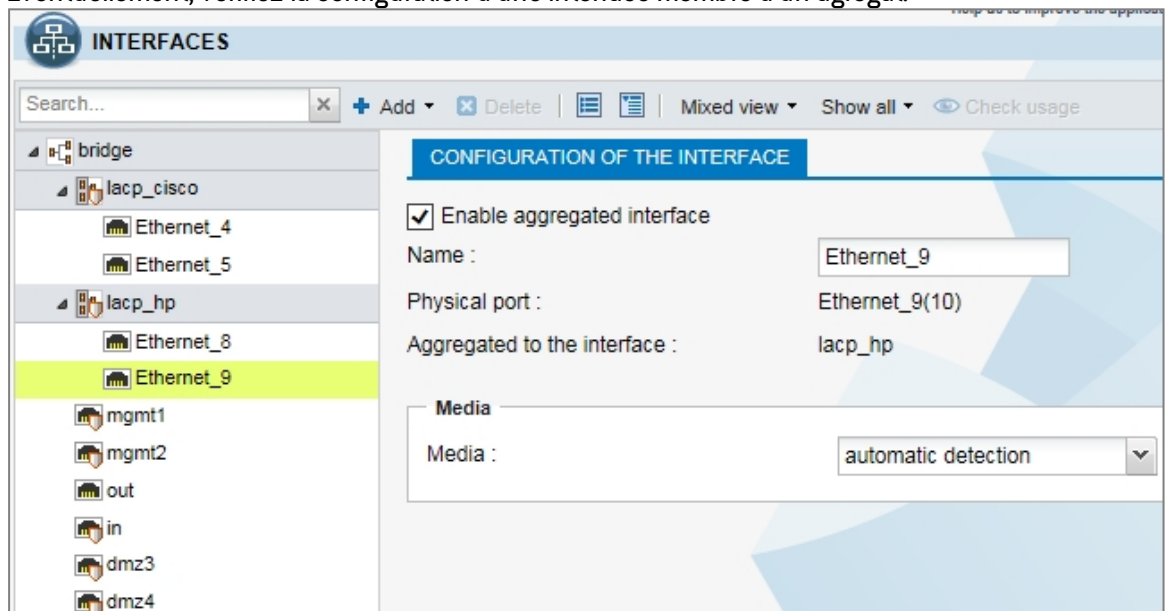
The screenshot shows the 'CONFIGURATION OF THE INTERFACE' tab for 'lACP\_cisco' after configuration. The 'Physical ports' field now shows '[ Ethernet\_4, Ethernet\_5 ]', indicating that two interfaces are aggregated. Other fields remain the same as in the previous screenshot. At the bottom are 'Apply' and 'Cancel' buttons.



6. Refaites la même manipulation pour les interfaces agrégées côté commutateur HP.



7. Éventuellement, vérifiez la configuration d'une interface membre d'un agrégat.



## Vérifier la configuration

CLI SN2000					Commentaires
<pre>SN2KXA15D0521A7&gt;portinfo port      name      NS-BSD    state    addressIPv4 addressIPv6 1         mgmt1     igb8      no-link  10.10.30.193/27 2         mgmt2     igb9      no-link  10.10.30.193/27 3         out       igb4      no-link  10.10.30.193/27 4         in        igb5      up       10.10.30.193/27 5         lACP_cisco lagg0/igb6 no-link  10.10.30.193/27 6         lACP_cisco lagg0/igb7 no-link  10.10.30.193/27 7         dmz3      igb0      no-link  10.10.30.193/27 8         dmz4      igb1      no-link  10.10.30.193/27 9         lACP_hp   lagg1/igb2 no-link  10.10.30.193/27 10        lACP_hp   lagg1/igb3 no-link  10.10.30.193/27</pre>					<p>Avec la commande <code>portinfo</code>, les ports sont décrits selon la numérotation visible dans l'interface.</p> <p>Visualisez le nom NS-BSD des interfaces, qui sera utilisé dans les journaux.</p>



CLI SN2000	Commentaires
<pre>SN2KXA15D0521A7&gt;ifinfo interface list: bridge   10.10.30.193/27   out (igb4)   dmz3 (igb0)   dmz4 (igb1)   lacp_cisco (protected,lagg0) { igb7, igb6, }   lacp_hp (protected,lagg1) { igb3, igb2, }   mgmt1 (protected,igb8)   mgmt2 (protected,igb9)   in (protected,igb5)   sslvpn (protected,tun0) loopback5 (lo5) loopback4 (lo4) loopback3 (lo3) loopback2 (lo2) loopback1 (lo1) ipsec (enc0)</pre>	<p>Le nom NS-BSD des interfaces agrégées apparaît dans la description des agrégats.</p>

Puisque la configuration des agrégats est terminée sur le firewall Stormshield Network comme sur les commutateurs, la connexion des câbles Ethernet est désormais possible.

## Diagnostics sur le commutateur

CLI CISCO	CLI HP
<pre>Switch#show interface port-channel 1 Port-channel1 is up, line protocol is up (connection) Hardware is EtherChannel, address is 001d.4608.e217 (bia 001d.4608.e217) MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,</pre>	Pas d'équivalent sur HP
Des lignes sont omises ici mais affichées à l'écran.	

**Commentaires :** Remarquez la bande passante côté Cisco : **BW = 2000000 Kbit** (2x1 Gbps).

CLI CISCO	CLI HP
<pre>Switch#show etherchannel 1 detail Group state = L2 Ports: 2 Maxports = 8 Port-channels: 1 Max Port-channels = 8 Protocol: LACP Minimum Links: 0</pre>	<pre>ProCurve(config)#show lacp</pre>
<pre>Ports in the Port-channel: Index Load Port EC state No of bits -----+-----+-----+-----+----- 0 00 Gi0/23Passive 0 0 00 Gi0/24Passive 0</pre>	<pre> LACP PORT  LACP  TRUNK  PORT  LACP NUMB  ENABLED GROUP STATUS PARTNER 1      Passive 1      Down  No  2      Passive 2      Down  No</pre>
Des lignes sont omises ici mais affichées à l'écran.	
Des lignes sont omises ici mais affichées à l'écran.	
Des lignes sont omises ici mais affichées à l'écran.	
Des lignes sont omises ici mais affichées à l'écran.	

**Commentaires :** Le protocole LACP est associé au mode d'agrégation choisi. Attention ! Le terme **Passive** affiché dans la CLI HP concerne l'interface, il ne se rapporte pas au mode de configuration du protocole LACP.



CLI CISCO	CLI HP
<pre>Switch#debug etherchannel PAGP/LACP Shim/FEC debugging is on 00:14:44: FEC: Un-Bndl msg NOT send to PM for port Gi0/23 from Pol 00:14:44: FEC: delete port (Gi0/23) from agport (Pol) 00:14:44: FEC: lacp_switch_remove_port_from_ associated_list_internal: Gi0/23 deleted from the associated list for Pol 00:14:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/23, changed state to down</pre>	<pre>ProCurve(config)#show log Keys: W=Warning I=Information M=Major D=Debug --- Event Log listing: Events Since Boot --- I 13/10/15 00:00:57 ports: trunk Trk1 is now active I 13/10/15 00:00:57 ports: port 23 in Trk1 is now on-line I 13/10/15 00:00:57 ports: port 24 in Trk1 is now on-line</pre>
Des lignes sont omises ici mais affichées à l'écran.	Des lignes sont omises ici mais affichées à l'écran.
<pre>00:59:50: %LINK-3-UPDOWN:Interface GigabitEthernet0/23, changed state to up</pre>	
Des lignes sont omises ici mais affichées à l'écran.	
<pre>00:59:51: FEC: add port (Gi0/23) to agport (Pol) 00:59:52: FEC: lacp_fec_bundle_internal: Determine if msg to PM to bundle port Gi0/23 with Pol is needed 00:59:52: FEC: pagp_switch_want_to_bundle: Bndl msg to PM for port Gi0/23 to Agport Pol 00:59:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/23, changed state to up</pre>	<pre>I 13/10/15 09:52:58 ports: port 23 in Trk1 is now off-line I 13/10/15 09:52:58 ports: port 25 is Blocked by LACP I 02/10/13 09:52:58 ports: port 23 in Trk5 is now on-line</pre>

**Commentaires :** Des paquets ping sont envoyés au firewall SN, depuis un poste connecté au commutateur.

Le câble connecté au premier port de l'agrégat est débranché.

Le mode debug de Cisco ou log de HP montre les modifications.

Le câble est rebranché, l'agrégat bascule sur son état normal.

Ne pas oublier de sortir du mode debug sur le commutateur Cisco.

Aucun ping passant par le commutateur HP n'est perdu, en revanche, un ping est perdu sur le commutateur Cisco à chaque changement d'état (lorsque l'un des 2 câbles a été débranché, ou rebranché).

## Diagnostics sur le firewall Stormshield Network

Commandes SN2000	Commentaires
<pre>SN2KXA15D0521A7&gt;grep -i "alarmid=3\  alarmid=8" /log/1_alarm</pre>	Des paquets ping sont envoyés au firewall SN, depuis des postes connectés aux commutateurs Cisco et HP.
<pre>id=firewall time="2015-11-09 14:47:49" fw="SN2KXA15D0521A7" tz="+0000 starttime="2015- 11-09 14:47:49" pri=4 msg="Lien agrégé activé: igb6" class=system alarmid=84</pre>	Les alarmid relatifs à LACP commencent par 3 ou 8.
<pre>id=firewall time="2015-11-09 14:47:49" fw="SN2KXA15D0521A7" tz="+0000 starttime="2015- 11-09 14:47:49" pri=4 msg="Interface activée: lagg0" class=system alarmid=37</pre>	Connexion du lien 1 vers Cisco : dmz1 alias igb6 (comme vu dans le résultat de la commande portinfo).
	L'agrégation vers Cisco ne fonctionne que sur le lien 1, les paquets ping passent.



Commandes SN2000	Commentaires
<code>id=firewall time="2015-11-09 15:08:05" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:08:05" pri=4 msg="Lien agrégé activé: igb7" class=system alarmid=84</code>	Connexion du lien 2 vers Cisco : dmz2 alias igb7.
<code>id=firewall time="2015-11-09 15:08:18" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:08:18" pri=4 msg="Lien agrégé désactivé: igb6" class=system alarmid=85</code>	Déconnexion du lien 1, les paquets ping passent toujours.
<code>id=firewall time="2015-11-09 15:08:35" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:08:34" pri=4 msg="Lien agrégé activé: igb6" class=system alarmid=84</code>	Reconnexion du lien 1.
<code>id=firewall time="2015-11-09 15:10:12" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:10:11" pri=4 msg="Interface désactivée: lagg0" class=system alarmid=38</code>	Déconnexion des deux liens, l'interface lagg0 se désactive (plus de ping via le Cisco...)
<code>id=firewall time="2015-11-09 15:10:17" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:10:17" pri=4 msg="Lien agrégé activé: igb2" class=system alarmid=84</code>	Connexion du lien 3 vers HP : dmz5 alias igb2.
<code>id=firewall time="2015-11-09 15:10:17" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:10:17" pri=4 msg="Interface activée: lagg1" class=system alarmid=37</code>	L'agrégation vers HP ne fonctionne que sur le lien 3.
<code>id=firewall time="2015-11-09 15:11:04" fw="SN2KXA15D0521A7" tz="+0000 starttime= "2015-11-09 15:11:04" pri=4 msg="Lien agrégé activé: igb3" class=system alarmid=84</code>	Connexion du lien 4 vers HP : dmz6 alias igb3.

En résumé, lorsqu'un lien de l'agrégat est connecté, une alarme système id= 84 est levée, et une alarme système id=37 indique que l'agrégat est devenu opérationnel.

Si tous les liens d'un agrégat tombent, une alarme système=38 indique que l'agrégat lui-même est désactivé, la désactivation d'un seul lien lève une alarme système id=85.



## Pour aller plus loin...

### Activer le mode verbeux du LACP

1. Connectez-vous en SSH au firewall et exécutez les commandes suivantes :

```
cp /etc/syslog.conf /etc/syslog.conf.bak  
touch /log/lacp.log
```

2. Editez le fichier `/etc/syslog.conf` et modifiez la ligne `kern.*` en précisant le chemin du fichier précédemment créé :

```
kern.*                                /log/lacp.log
```

3. Modifiez le niveau de journalisation pour activer le mode verbeux LACP :

```
sysctl net.link.lagg.lacp.debug=3
```

4. Relancez le processus de journalisation :

```
killall -HUP syslogd || syslogd
```

Les journaux LACP en mode verbeux sont accessibles dans `/log/lacp.log`.

Pour désactiver le mode verbeux, connectez-vous en SSH au firewall et exécutez les commandes suivantes :

```
sysctl net.link.lagg.lacp.debug=0  
mv /etc/syslog.conf.bak /etc/syslog.conf
```

### Limites de l'agrégation de liens

Tous les ports physiques d'un même agrégat doivent figurer sur un commutateur unique, voire sur un ASIC unique de ce commutateur, comme pour le Procurve HP. Un ASIC (Application Specific Integrated Circuits) représente ici un regroupement de ports

Pour les commutateurs empilables (stackable) en revanche, la répartition peut se faire sur des commutateurs distincts.

Par exemple, sur la gamme des commutateurs Cisco 3750, la technologie se nomme Cross-Stack EtherChannel et sa mise en place nécessite deux commutateurs en configuration VSS (Virtual Switching System), permettant à deux commutateurs physiques de fonctionner comme un commutateur logique.

Un autre exemple est le protocole propriétaire DMLT (Distributed Multi-Link Trunking) du constructeur Avaya.

Ainsi, il est possible de mettre en œuvre une infrastructure hautement résiliente, mais au prix d'investissements importants sur le matériel de couche 2 (commutateurs), et en termes de temps d'administration. Des exemples d'infrastructures avec tolérance aux pannes sont détaillés dans la suite de ce document.

### Cluster HA SNS et LACP

Cette section ne détaille pas la configuration complète d'un cluster HA.



## Calculer le facteur de qualité de la HA avec LACP

Pour rappel, le facteur de qualité est une formule mathématique dépendante de l'état (et éventuellement du poids) des interfaces actives, calculée sur les deux nœuds d'un cluster, pour permettre l'élection du nœud actif.

Lorsqu'un agrégat est présent, le calcul s'effectue selon l'état de l'interface agrégée, et non selon celui des interfaces membres de l'agrégat, afin que la perte d'une seule interface de l'agrégat ne modifie pas le facteur de qualité.

### Exemple

Le boîtier SN 2000 préalablement utilisé dispose de 10 interfaces Ethernet actives, de poids égal par défaut.

Toutes les interfaces ont un lien opérationnel.

Un agrégat *lagg0* contient deux interfaces agrégées : 8 interfaces simples et un agrégat, soit 9 interfaces.

Le poids est par défaut de 100.

Avec cette configuration, le facteur de qualité est calculé comme suit :

$$(9 \times 100 / 9 \times 100) \times 100 = 100\%$$

Si l'une des deux interfaces agrégées perd sa connexion, le facteur de qualité reste le même car il reste dans l'agrégat une interface active.

Si l'agrégat perd sa connexion, le facteur de qualité est modifié comme suit :

$$(8 \times 100 / 9 \times 100) \times 100 = 89\%.$$

#### NOTE

Même en SSH, ce comportement n'est pas modifiable.

## Cas pratique 1 : un cluster Stormshield Network, un commutateur

### Topologie conseillée



Le cluster HA est muni de deux liens de contrôle sur des interfaces dédiées.

Pour un commutateur connecté au cluster, créez un agrégat par nœud du cluster à relier.

### Configurer le cluster avec LACP

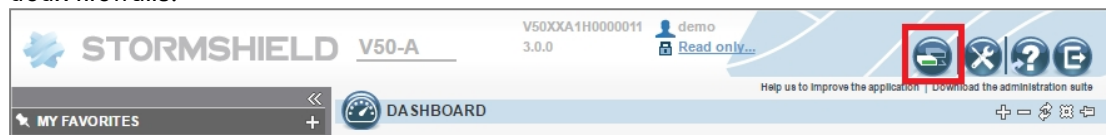
En cas de bascule (modification du nœud actif du cluster), la renégociation LACP effectuée par le nouveau nœud actif pourrait prendre une trentaine de secondes, empêchant tout trafic sur l'agrégat.



La bonne pratique pour éviter cette renégociation consiste à configurer la négociation LACP sur les deux nœuds du Cluster selon la procédure suivante correspondant à votre version de SNS :

### SNS à partir de v3

1. Dans l'interface d'administration du firewall actif, choisissez **Système > Haute disponibilité**.
2. Dans la zone **Configuration du basculement**, cochez la case **Activer l'agrégation de liens lorsque le firewall est passif**.
3. Dans le bandeau supérieur de l'interface, cliquez sur l'icône Cluster pour synchroniser les deux firewalls.



L'agrégat LACP est alors configuré sur les deux nœuds.

### SNS v2 (non disponible en v1)

1. Connectez-vous en SSH au nœud actif et exécutez la commande suivante :  
`setconf ~/ConfigFiles/HA/highavailability Global LACPWhenPassive 1`
2. Synchronisez la configuration sur le nœud passif en exécutant les commandes suivantes :  
`enha -f -v`  
`hasync -v`

L'agrégat LACP est alors configuré sur les deux nœuds.

## Cas pratique 2 : un cluster Stormshield Network, deux commutateurs empilables

### Topologie conseillée

Logiquement, le schéma de configuration est le même que dans le cas précédent, les deux commutateurs étant vus comme un seul commutateur logique. Mais le commutateur n'est plus un SPOF (Single Point Of Failure).

Le schéma physique de configuration suivant permet donc une tolérance complète aux pannes :



Deux firewalls Stormshield Network forment un cluster haute disponibilité disposant d'un nœud actif et d'un nœud passif.

Chaque nœud du cluster est relié à deux commutateurs distincts par le biais d'une agrégation de liens.

Les deux commutateurs sont empilables. En fonction des marques et modèles, il y aura un commutateur actif et un commutateur passif, ou deux commutateurs en mode actif. Les commutateurs permettent une répartition des agrégats car deux interfaces agrégées peuvent être réparties sur les deux commutateurs physiques.

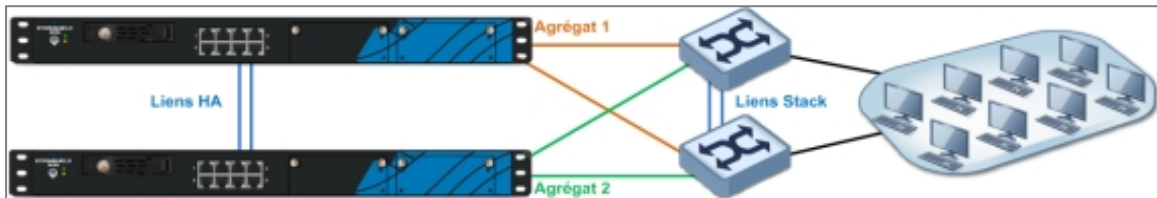




### Configurer le cluster et les commutateurs avec LACP

Configurez le cluster de la même façon que pour le cas d'usage précédent. Pour plus d'informations, reportez-vous à la section [Configurer le cluster avec LACP](#).

Dans le schéma réseau ci-dessous (où apparaissent des postes de travail), la question des boucles réseau peut se poser.



Une boucle apparaît dans un réseau lorsque plusieurs liens différents de niveau 2 (couche Liaisons de données du modèle OSI) existent entre deux éléments actifs.

Les commutateurs empilables doivent être munis d'un système anti-boucle (loop-free) pour éviter les problèmes d'instabilité de la table d'adresses MAC, ou se trouver en mode actif-passif.

En revanche, sur le cluster SNS, aucune modification n'est à prévoir : qu'une trame Ethernet contenant l'adresse MAC source d'un poste de travail soit passée par le commutateur 1 ou le commutateur 2, elle se présente au cluster sur l'interface agrégée du nœud actif.



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)