



**STORMSHIELD**



NOTE TECHNIQUE

**STORMSHIELD NETWORK SECURITY**

# DÉPLOYER SNS FOR CLOUD (2 INTERFACES RÉSEAU) SUR MICROSOFT AZURE

Produits concernés : SNS 1 et versions supérieures

Date : Aout 2018

Référence : sns-fr-sns\_for\_cloud\_microsoft\_azure\_note\_technique



# Table des matières

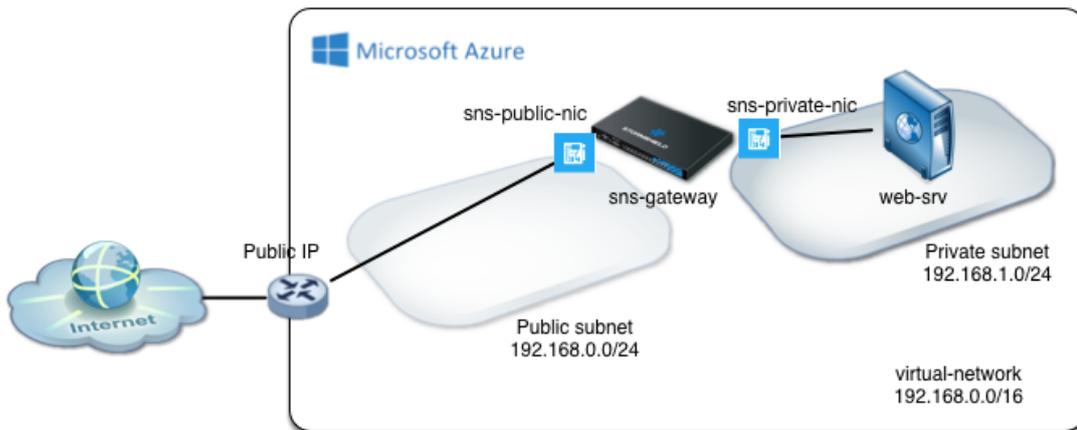
Avant de commencer .....	3
Obtenir la licence du firewall .....	3
Déployer le firewall virtuel .....	4
Déployer un serveur Web virtuel .....	5
Déployer le serveur dans le groupe de ressources .....	5
Configurer le firewall pour autoriser les flux depuis et vers le serveur .....	5
Récupérer l'adresse IP publique du firewall virtuel .....	5
Configurer le firewall pour autoriser les flux entre Internet et le serveur Web .....	6
Créer les objets réseaux nécessaires .....	6
Créer les règles de filtrage et mettre à jour la politique de sécurité .....	6
Créer les règles de translation d'adresse (NAT) .....	7
Installer le service Web sur le serveur .....	8
Tester la configuration .....	8
Tester les flux sortants (depuis la DMZ vers Internet) .....	8
Tester les flux entrants (depuis Internet vers la DMZ) .....	9



## Avant de commencer

Cette note technique présente le déploiement sur la plate-forme d'hébergement Microsoft Azure d'un firewall Stormshield Network Security for Cloud de taille "Standard\_D2s\_v3" doté de deux interfaces réseau : une interface publique (interface non protégée) et une interface privée (interface protégée).

Ce document propose également un exemple de règles de filtrage et de translation d'adresses afin de protéger un serveur Web hébergé sur le réseau privé du firewall.



### Obtenir la licence du firewall

Lorsque le déploiement est terminé, votre firewall virtuel nécessite une licence logicielle pour fonctionner.

Rapprochez-vous de votre distributeur Stormshield afin de commander la licence de votre firewall virtuel. Si vous n'avez pas déjà un distributeur Stormshield, vous pouvez utiliser notre [moteur de recherche](#) afin d'en localiser un près de chez vous.



## Déployer le firewall virtuel

La page Stormshield de la MarketPlace Microsoft Azure ne permet pas le déploiement pas à pas d'un firewall SNS disposant de plus d'une interface réseau.

La méthode présentée repose donc sur l'utilisation d'un modèle personnalisé mis à disposition sur l'espace *GitHub* de Stormshield.

1. Accédez à la page Github de Stormshield en cliquant sur le lien suivant : <https://github.com/stormshield/azure-templates/tree/master/sns/sns-2-nics>,
2. Cliquez sur le bouton **Deploy to Azure**,
3. Identifiez-vous à l'aide votre compte Azure ou de votre compte Microsoft.  
Le formulaire de déploiement pré-rempli s'affiche.
4. Toutes les valeurs proposées dans les champs de ce modèle peuvent être personnalisées.

### Informations de base

- **Abonnement** : sélectionnez un abonnement Azure associé à votre compte.
- Sélectionnez ou créez un groupe de ressources (*SNS-Documentation* dans l'exemple).
- Sélectionnez l'emplacement géographique d'hébergement pour votre firewall.

### Paramètres

- **SNS Admin password** : entrez le mot de passe attribué au compte *admin* du firewall.
- **Vnet Name** : indiquez le nom du réseau virtuel qui regroupe le réseau public et le réseau privé du firewall (*virtual-network* dans le modèle).
- **Vnet Prefix** : indiquez le réseau et le masque de ce réseau virtuel (*192.168.0.0/16* dans le modèle). Ce réseau est à choisir dans les plages d'adresses IP non routées sur Internet.
- **Public Subnet Name** : saisissez le nom du sous-réseau dans lequel se situe l'interface publique du firewall (*Public* dans le modèle).
- **Public Subnet Prefix** : indiquez le réseau et le masque de ce sous-réseau public (*192.168.0.0/24* dans le modèle). Il s'agit obligatoirement d'un sous-réseau de **Vnet Prefix**.
- **Private Subnet Name** : saisissez le nom du sous-réseau dans lequel se situe l'interface privée du firewall (*Private* dans le modèle).
- **Private Subnet Prefix** : indiquez le réseau et le masque de ce sous-réseau privé (*192.168.1.0/24* dans le modèle). Il s'agit obligatoirement d'un sous-réseau de **Vnet Prefix**.
- **SNS Name** : précisez le nom attribué à votre firewall virtuel (*sns-gateway* dans le modèle).
- **SNS If Public Name** : indiquez le nom attribué à l'interface publique du firewall (*sns-gateway-public-nic* dans le modèle).
- **SNS If Public IP** : indiquez l'adresse IP affectée à l'interface publique du firewall (*192.168.0.100* dans le modèle). Cette adresse appartient obligatoirement au réseau défini dans le champ **Public Subnet Prefix**.
- **SNS If Private Name** : indiquez le nom attribué à l'interface privée du firewall (*sns-gateway-private-nic* dans le modèle).
- **SNS If Private IP** : indiquez l'adresse IP affectée à l'interface privée du firewall (*192.168.1.100* dans le modèle). Cette adresse appartient obligatoirement au réseau défini dans le champ **Private Subnet Prefix**.



- **VM Size** : sélectionnez un modèle de machine virtuelle supportant plusieurs interfaces réseau (*Standard\_D2s\_v3* dans le modèle). Les caractéristiques des différents modèles de machines virtuelles sont consultables sur [cette page](#).
- **Public IP Name** : saisissez un nom caractérisant l'adresse IP publique qui est affectée au firewall par Microsoft Azure (*sns-gateway-public-ip* dans le modèle).
- **Route Table Name** : donnez un nom à la table de routage privée du firewall (*route-table-private* dans le modèle).

Lorsque tous les champs obligatoires sont remplis, prenez connaissance des conditions de la Market Place Microsoft Azure, cochez la case "J'accepte les termes et conditions mentionnés ci-dessus" et cliquez sur le bouton **Acheter**.

Le déploiement du firewall débute. Une notification "Déploiement réussi" est affichée lors que le firewall a été créé sur la plate-forme d'hébergement.

## Déployer un serveur Web virtuel

### Déployer le serveur dans le groupe de ressources

Ce chapitre décrit succinctement les étapes permettant de déployer un serveur Web (basé sur une distribution Linux Ubuntu Server) dans le réseau protégé par le firewall virtuel (*Private* dans l'exemple) :

1. Dans la Market Place Microsoft Azure, recherchez "Ubuntu Server XX.XX LTS" et sélectionnez la distribution souhaitée,
2. Sélectionnez un modèle de déploiement et cliquez sur **Créer**,
3. Attribuez un nom à cette machine (*Web-Documentation-Server* par exemple),
4. Créez un utilisateur (*azureuser* par exemple) et son mot de passe,
5. Choisissez l'emplacement géographique d'hébergement,
6. Sélectionnez le groupe de ressources créé lors du déploiement du firewall (*SNS-Documentation* dans l'exemple),
7. Dans les options, sélectionnez le réseau virtuel associé au groupe de ressources, puis le sous-réseau privé créé précédemment (*Private* dans l'exemple).
8. Validez.

## Configurer le firewall pour autoriser les flux depuis et vers le serveur

### Récupérer l'adresse IP publique du firewall virtuel

Depuis l'accueil du portail :

1. Cliquez sur **Groupe de ressources**.
2. Sélectionnez le groupe de ressources du firewall virtuel (*SNS-Documentation* dans l'exemple).
3. Cliquez sur l'entrée **Adresse IP publique** (*sns-gateway-public-ip* dans l'exemple).



4. Notez l'adresse IP publique qui lui a été attribuée.
5. De la même manière, notez l'adresse IP privée attribuée au serveur *Web-Documentation-Server* (192.168.1.4 dans l'exemple).

## Configurer le firewall pour autoriser les flux entre Internet et le serveur Web

1. Dans un navigateur Web, connectez-vous à l'interface d'administration du firewall disponible à l'URI `https://adresse_ip_publique_firewall/admin`.
2. Authentifiez-vous à l'aide du compte *admin* et du mot de passe défini lors de la création du firewall virtuel.
3. N'oubliez pas d'installer votre licence le plus rapidement possible afin de bénéficier de l'ensemble des fonctionnalités souscrites auprès de votre distributeur Stormshield.

## Créer les objets réseaux nécessaires

Au sein du module **Objets** > **Objets réseaux** créez :

- Deux objets de type réseau. Dans l'exemple : **Private\_Net** (192.168.1.0/24) et **Public\_Net** (192.168.0.0/24).
- Un objet de type machine correspondant au serveur Web (dans l'exemple : **Web\_Documentation\_Server** - 192.168.1.4).
- Un objet de type port pour le port SSH personnalisé (dans l'exemple : **sshwebsrv** - 222/TCP).

## Créer les règles de filtrage et mettre à jour la politique de sécurité

1. Dans l'onglet *Filtrage* du module **Politique de sécurité** > **Filtrage et NAT**, sélectionnez la politique de filtrage créée par défaut ([9] Azure default).
2. Créez une règle autorisant les machines hébergées sur le réseau privé à accéder à l'ensemble des machines en utilisant les valeurs suivantes :
  - **Action** : passe,
  - **Source** : l'objet **Private\_Net**,
  - **Destination** : l'objet **Any**,
  - **Port de destination** : l'objet **Any**,
  - **Inspection de sécurité** : IPS.
3. Créez une règle autorisant toutes les machines à se connecter sur votre serveur Web en HTTP et SSH :
  - **Action** : passer,
  - **Source** : l'objet **Any** via l'interface d'entrée **out**,
  - **Destination** : l'objet **Firewall\_out**,
  - **Port de destination** : les objets **http** et **sshwebsrv**,
  - **Inspection de sécurité** : IPS.
4. A l'aide des boutons **Monter** et **Descendre**, placez ces deux règles au dessus de la règle de blocage. Vous pouvez également ajouter des séparateurs de règles afin d'organiser votre politique de filtrage.

La politique de filtrage prend donc la forme suivante :



FILTERING		NAT																	
Searched text																			
+ New rule		Delete		↑ Up		↓ Down		Expand all		Collapse all		Cut		Copy		Paste		Reset rules statistic	
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection												
Administration rules (contains 2 rules, from 1 to 2)																			
1	on	pass	Any interface: out	Any	bootpc		IPS												
2	on	pass	Any interface: out	Firewall_out	ssh		IPS												
Private_Net to internet (contains 1 rules, from 3 to 3)																			
3	on	pass	Private_Net	Any	Any		IPS												
Internet to servers (contains 1 rules, from 4 to 4)																			
4	on	pass	Any interface: out	Firewall_out	http sshwebserv		IPS												
Block all (contains 1 rules, from 5 to 5)																			
5	on	block	Any	Any	Any		IPS												

## Créer les règles de translation d'adresse (NAT)

1. Dans l'onglet *NAT*, créez une règle transférant les flux SSH adressés à l'interface publique du firewall vers le serveur web :

### Trafic original (avant translation)

- **Source** : l'objet *Any* via l'interface entrante *out*.
- **Destination** : l'objet *Firewall\_out*.
- **Port de destination** : l'objet *sshwebserv*.

### Trafic après translation

- **Source** : l'objet *Any*.
- **Destination** : l'objet *Web-Documentation-Server*.
- **Port de destination** : l'objet *ssh*.

2. Créez la règle transférant les flux HTTP adressés à l'interface publique du firewall vers le serveur web :

### Trafic original (avant translation)

- **Source** : l'objet *Any* via l'interface *out*.
- **Destination** : l'objet *Firewall\_out*.
- **Port de destination** : l'objet *http*.

### Trafic après translation

- **Source** : l'objet *Any*.
- **Destination** : l'objet *Web-Documentation-Server*.
- **Port de destination** : l'objet *http*.

3. Créez la règle transférant les flux issus des machines de la DMZ vers les machines situées au delà du firewall :

### Trafic original (avant translation) :



- **Source** : l'objet **Private\_Net**.
- **Destination** : tout ce qui est différent (symbole ) de l'objet **Public\_Net** et sort par l'interface **out**.
- **Port de destination** : l'objet **Any**.

#### Trafic après translation :

- **Source** : l'objet **Firewall\_out**.
- **Port source** : l'objet **ephemeral\_fw**.
- **Destination** : l'objet **Any**.

La politique de translation d'adresses prend donc la forme suivante :

FILTERING		NAT																			
Searched text		+ New rule		Delete		↑ Up		↓ Down		Expand all		Collapse all		Cut		Copy		Paste		Reset rules statistics	
	Status	Original traffic (before translation)				Traffic after translation				Options											
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port													
1	on	Any interface: out	Firewall_out	sshwebserv	Any		Web-Documenta	ssh													
2	on	Any interface: out	Firewall_out	http	Any		Web-Documenta	http													
3	on	Private_Net	Public_Net interface: out	Any	Firewall_out	ephemeral_fw	Any														

4. Activez la politique de sécurité modifiée en cliquant sur le bouton **Sauvegarder et activer**.

## Installer le service Web sur le serveur

1. Connectez-vous sur votre serveur en SSH,
2. Installez le service Apache et ses dépendances.

## Tester la configuration

### Tester les flux sortants (depuis la DMZ vers Internet)

Depuis le serveur Web (machine *Web-Documentation-Server* dans l'exemple), réalisez une connexion HTTP vers un serveur Web externe.

Le firewall analysant les connexions, les traces correspondant à ces connexions peuvent être visualisées au sein de l'application **Traces et rapports d'activités** (module **Traces** > **Vues** > **Trafic réseau**) :



The screenshot shows the 'NETWORK TRAFFIC' interface with a search filter for 'Last hour'. The search results show five entries for traffic from 'Web-Documentation-Server' to 'azure.archive.ubuntu.com' on port 80 (http). The actions for all entries are 'Pass'.

Saved at	Action	Source Name	Destination Name	Dest. Port Name	Argument
08/17/2015 09:22:39 AM	Pass	Web-Documentation-Server	azure.archive.ubuntu.com	http	/ubuntu/dists/trusty/main/i18n/Transla...en_US
08/17/2015 09:22:39 AM	Pass	Web-Documentation-Server	azure.archive.ubuntu.com	http	/ubuntu/dists/trusty/universe/i18n/Tra...en_US.gz
08/17/2015 09:22:39 AM	Pass	Web-Documentation-Server	azure.archive.ubuntu.com	http	/ubuntu/dists/trusty/main/i18n/Transla...en_US.gz
08/17/2015 09:22:39 AM	Pass	Web-Documentation-Server	azure.archive.ubuntu.com	http	/ubuntu/dists/trusty/universe/i18n/Tra...en_US.lzma
08/17/2015 09:22:39 AM	Pass	Web-Documentation-Server	azure.archive.ubuntu.com	http	/ubuntu/dists/trusty/main/i18n/Transla...en_US.lzma

## Tester les flux entrants (depuis Internet vers la DMZ)

Depuis une machine située hors de l'infrastructure Microsoft Azure, établissez une connexion Web vers la page *index.htm* du serveur Web virtuel.

Lorsque la connexion est établie, les traces correspondantes ainsi que les opérations de NAT peuvent être visualisées au sein de l'application **Traces et rapports d'activités** (module **Traces > Vues > Trafic réseau**).



**STORMSHIELD**

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

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

*Copyright © Stormshield 2018. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.*