NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY ELASTIC VIRTUAL APPLIANCE

DÉPLOYER UN FIREWALL VIRTUEL SNS EVA SUR MICROSOFT AZURE

Produits concernés : SNS 4.x

Dernière mise à jour du document : 9 septembre 2022

Référence : sns-fr-eva_sur_microsoft_azure_note_technique

Table des matières

Avant de commencer ... 3

Prérequis et caractéristiques techniques ... 4

Prérequis ... 4
Caractéristiques techniques des instances Microsoft Azure ... 4
Caractéristiques techniques des firewalls SNS EVA ... 4

Enregistrer le produit SNS EVA ... 5

Vous possédez déjà un compte MyStormshield ... 5
Vous ne possédez pas de compte MyStormshield ... 5

Déployer le firewall virtuel SNS EVA ... 6

Déployer le firewall depuis le Portail Microsoft Azure ... 6
Déployer le firewall ... 6
Ajouter une nouvelle interface au firewall ... 6
Déployer le firewall depuis l'espace azure-templates de Stormshield sur GitHub ... 7

Activer le firewall virtuel SNS EVA ... 8

Récupérer l'adresse IP publique du firewall ... 8
Télécharger le kit d'activation ... 8
Importer le kit d'activation ... 8
Vérifier si le firewall doit être mis à jour ... 8

Déployer un serveur virtuel ... 9

Déployer le serveur dans le groupe de ressources ... 9
Récupérer l'adresse IP publique du serveur virtuel ... 9
Installer le service souhaité sur le serveur ... 9

Autoriser sur le firewall virtuel SNS EVA les flux depuis et vers le serveur virtuel ... 10

Créer les objets réseau nécessaires ... 10
Configurer la politique de filtrage et NAT ... 10
Configurer la politique de filtrage ... 10
Configurer la politique de NAT ... 11

Tester la configuration et la sauvegarder ... 13

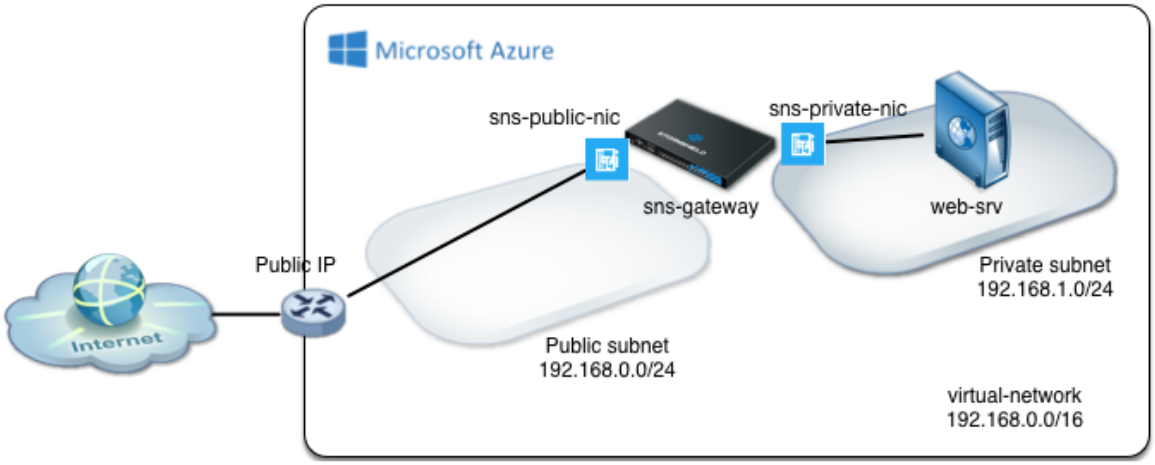
Tester la configuration ... 13
Sauvegarder la configuration ... 13

Pour aller plus loin ... 14

Avant de commencer

Cette note technique présente le déploiement sur Microsoft Azure d'un firewall virtuel SNS EVA doté de deux interfaces réseau : une interface publique (interface non protégée) et une interface privée (interface protégée).

Cette documentation présente certaines manipulations que vous pouvez réaliser dans le cadre du déploiement d'un firewall virtuel SNS EVA. Certaines sont communes à toutes les situations et d'autres sont en lien avec une architecture servant d'exemple. Les possibilités de configuration étant nombreuses, adaptez ces éléments selon vos besoins.



Dans cette documentation, Stormshield Network Security Elastic Virtual Appliance est désigné sous la forme abrégée SNS EVA.

Prérequis et caractéristiques techniques

Prérequis

- **Un compte Azure ou un compte Microsoft.**
  Pour créer un compte, accédez à la page Stormshield Elastic Virtual Appliance sur la Place de marché Microsoft Azure et cliquez sur **Obtenir Maintenant**.
- **Un abonnement Azure actif.**
  Pour vérifier ou gérer vos abonnements, connectez-vous au Portail Microsoft Azure et cliquez sur **Abonnements**.
- **Une licence d'un produit SNS EVA.**
  Rapprochez-vous de votre distributeur Stormshield afin de la commander. Utilisez notre moteur de recherche pour trouver un distributeur proche de chez vous.

Caractéristiques techniques des instances Microsoft Azure

Instance Azure	vCPU	RAM	Interfaces réseau	Bande passante (Mb/s)	Modèle EVA
F1	1	2	2	Modérée : 750	EVA1
F2	2	4	2	Élevée : 1500	EVA2 ou EVA3
F4	4	8	4	Élevée : 3000	EVA4
F8	8	16	8	Élevée : 6000	EVAU
F16	16	32	8	Très élevée : 12000	EVAU

Caractéristiques techniques des firewalls SNS EVA

Modèle	RAM	HDD	vCPU
EVA1	max = 2 Go	10 Go (2 Go de swap)	max = 1
EVA2	max = 3 Go	10 Go (2 Go de swap)	max = 2
EVA3	max = 6 Go	10 Go (2 Go de swap)	max = 4
EVA4	max = 8 Go	10 Go (2 Go de swap)	max = 4
EVAU	max = 64 Go	10 Go (4 Go de swap)	max = 16

Enregistrer le produit SNS EVA

Pour enregistrer votre produit SNS EVA, vous devez posséder son numéro de série et son mot de passe d'enregistrement. Ils se situent dans l'e-mail que vous avez reçu après avoir passé votre commande.

Une fois les éléments récupérés, l'enregistrement se réalise depuis l'espace personnel MyStormshield. Il permet notamment d'associer votre produit à votre compte MyStormshield. La procédure d'enregistrement est différente selon si vous possédez ou non déjà un compte.

Vous possédez déjà un compte MyStormshield

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Produit** > **Enregistrer un produit**.
3. Cliquez sur **Enregistrer une appliance SNS**.
4. Si les conditions générales d'utilisations et licence d'utilisation apparaissent, prenez-en connaissance, puis acceptez-les.
5. Complétez les informations demandées jusqu'à l'enregistrement de votre produit.

Pour plus d'informations, reportez-vous au guide Enregistrer des produits.

Vous ne possédez pas de compte MyStormshield

L'enregistrement de votre produit se réalise en même temps que la création de votre compte.

Pour cela, reportez-vous au guide Créer un compte et enregistrer un produit.

Déployer le firewall virtuel SNS EVA

Il existe deux méthodes pour déployer le firewall virtuel SNS EVA sur Microsoft Azure :

- Depuis le Portail Microsoft Azure : cette méthode permet de déployer un firewall avec une seule interface. Une manipulation supplémentaire sera nécessaire après le déploiement pour ajouter une interface supplémentaire,
- Depuis l'espace *azure-templates* de Stormshield sur GitHub : cette méthode permet de déployer un firewall avec deux interfaces pré-configurées grâce à un modèle personnalisé.

Réalisez le déploiement de votre firewall virtuel SNS EVA selon la méthode souhaitée. Pour rappel, vous devez disposer d'un abonnement Azure actif (voir les prérequis).

Déployer le firewall depuis le Portail Microsoft Azure

Déployer le firewall

1. Connectez-vous au Portail Microsoft Azure.
2. Cliquez sur **Créer une ressource**.
3. Recherchez la ressource **Stormshield Elastic Virtual Appliance** et accédez à sa page.
4. Cliquez sur **Créer**.
5. Dans **Détails du projet** :
   - Champ **Abonnement** : sélectionnez un abonnement Azure associé à votre compte,
   - Champ **Groupe de ressources** : sélectionnez ou créez un groupe de ressources (*SNS-Documentation* dans l'exemple).
6. Complétez les informations du formulaire de déploiement.
7. Cliquez sur **Vérifier + créer**.

Ajouter une nouvelle interface au firewall

1. Toujours sur le Portail Microsoft Azure, cliquez sur **Créer une ressource**.
2. Recherchez la ressource **Interface réseau** (ou **Network interface**) et accédez à sa page.
3. Cliquez sur **Créer**.
4. Dans **Détails du projet** :
   - Champ **Abonnement** : sélectionnez un abonnement Azure associé à votre compte,
   - Champ **Groupe de ressources** : sélectionnez le groupe de ressources du firewall.
5. Complétez les informations du formulaire et cliquez sur **Vérifier + créer**.
6. Recherchez la machine virtuelle du firewall et cliquez sur son nom.
7. Cliquez sur **Arrêter** et validez. Attendez que l'état de la machine virtuelle passe à **Arrêté**.
8. Dans **Paramètres > Mise en réseau**, cliquez sur **Attacher l'interface réseau**.
9. Sélectionnez l'interface réseau à attacher et validez.
10. Recherchez la nouvelle interface réseau et sélectionnez-la pour afficher ses informations.
11. Dans **Paramètres > Configurations IP**, activez **Transfert IP**. Ce paramètre permet au firewall de diriger le trafic des machines virtuelles protégées.
12. Redémarrez la machine virtuelle du firewall.

Une fois terminé, poursuivez vers le chapitre Activer le firewall virtuel SNS EVA.

Déployer le firewall depuis l'espace *azure-templates* de Stormshield sur GitHub

1. Accédez à la page de l'espace *azure-templates* de Stormshield sur GitHub.
2. Cliquez sur **Deploy to Azure**.
3. Identifiez-vous sur le Portail Microsoft Azure. Le formulaire de déploiement personnalisé s'affiche. Toutes les valeurs peuvent être personnalisées selon vos besoins.
4. Dans **Détails du projet** :
   - Champ **Abonnement** : sélectionnez un abonnement Azure associé à votre compte,
   - Champ **Groupe de ressources** : sélectionnez ou créez un groupe de ressources (*SNS-Documentation* dans l'exemple),
5. Dans **Détails de l'instance**, vérifiez et complétez les informations des champs suivants :

Champ	Description
Région	Emplacement géographique d'hébergement du firewall.
SNS Admin password	Mot de passe du compte *admin* du firewall.
Vnet Name	Nom du réseau virtuel qui regroupe le réseau public et le réseau privé du firewall (*virtual-network* dans le modèle).
Vnet Prefix	Réseau virtuel et son masque (*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	Nom du sous-réseau où se situe l'interface publique du firewall (*Public* dans le modèle).
Public Subnet Prefix	Sous-réseau public et son masque (*192.168.0.0/24* dans le modèle). Il s'agit obligatoirement d'un sous-réseau de **Vnet Prefix**.
Private Subnet Name	Nom du sous-réseau où se situe l'interface privée du firewall (*Private* dans le modèle).
Private Subnet Prefix	Sous-réseau privé et son masque (*192.168.1.0/24* dans le modèle). Il s'agit obligatoirement d'un sous-réseau de **Vnet Prefix**.
SNS Name	Nom du firewall (*sns-gateway* dans le modèle).
SNS If Public Name	Nom de l'interface publique du firewall (*sns-gateway-public-nic* dans le modèle).
SNS If Public IP	Adresse IP de l'interface publique du firewall (*192.168.0.100* dans le modèle). Elle appartient obligatoirement au sous-réseau **Public Subnet Prefix**.
SNS If Private Name	Nom de l'interface privée du firewall (*sns-gateway-private-nic* dans le modèle).
SNS If Private IP	Adresse IP de l'interface privée du firewall (*192.168.1.100* dans le modèle). Elle appartient obligatoirement au sous-réseau **Private Subnet Prefix**.
VM Size	Instance Azure dont les caractéristiques techniques correspondent au modèle de firewall virtuel SNS EVA de vos besoins (voir les caractéristiques techniques).
Public IP Name	Nom de l'adresse IP publique attribuée au firewall par Microsoft Azure (*sns-gateway-public-ip* dans le modèle).
Route Table Name	Nom de la table de routage privée du firewall (*route-table-private* dans le modèle).

6. Une fois les informations complétées, cliquez sur **Vérifier + créer**.

Une fois le déploiement terminé, poursuivez vers le chapitre Activer le firewall virtuel SNS EVA.

Activer le firewall virtuel SNS EVA

Vous devez activer votre firewall afin de lui attribuer son modèle EVA, son numéro de série définitif, sa licence et les options souscrites.

Récupérer l'adresse IP publique du firewall

1. Connectez-vous au Portail Microsoft Azure.
2. Cliquez sur **Groupe de ressources**.
3. Sélectionnez le groupe de ressources du firewall (*SNS-Documentation* dans l'exemple).
4. Cliquez sur l'entrée **Adresse IP publique** (*sns-gateway-public-ip* dans l'exemple).
5. Notez l'adresse IP publique.

Télécharger le kit d'activation

1. Connectez-vous à votre espace personnel MyStormshield.
2. Naviguez dans la liste de vos produits jusqu'à identifier le produit concerné. Cliquez dessus.
3. À droite dans le cadre **Téléchargement**, sélectionnez la branche de version **4.x**.
4. Cliquez sur le lien **Télécharger le kit d'activation**, puis acceptez le téléchargement.

Importer le kit d'activation

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresse_ip_publique_firewall*/admin.
2. Authentifiez-vous à l'aide du compte *admin* et du mot de passe associé.
3. Dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**, champ **Sélectionnez la mise à jour**, sélectionnez le kit d'activation téléchargé précédemment.
4. Cliquez sur **Mettre à jour le firewall**. Le firewall redémarre automatiquement.

Vérifier si le firewall doit être mis à jour

1. Dans l'interface d'administration du firewall, visualisez dans le bandeau supérieur la version SNS actuellement installée.
2. Dans l'espace personnel MyStormshield, identifiez la version la plus récente dans **Téléchargements > Téléchargements > Stormshield Network Security > Firmware > 4.X**.
3. Si votre firewall dispose déjà de la dernière version, poursuivez vers le chapitre Déployer un serveur virtuel. Si ce n'est pas le cas, consultez les notes de version pour connaître le contenu de la dernière version disponible.
4. Cliquez sur le lien correspondant au modèle de firewall EVA pour télécharger la version.
5. Dans l'interface d'administration du firewall, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
6. Dans le champ **Sélectionnez la mise à jour**, sélectionnez le fichier de mise à jour.
7. Cliquez sur **Mettre à jour le firewall**. Le firewall redémarre automatiquement.

Déployer un serveur virtuel

Vous pouvez déployer un serveur virtuel pour y héberger le service de votre choix. Ce serveur sera déployé dans le réseau protégé par le firewall virtuel SNS EVA.

Ce chapitre décrit succinctement les étapes permettant de déployer le serveur virtuel. Dans cet exemple, nous installons *Ubunbu Server* afin de mettre en place un serveur personnalisé de sauvegardes. Les possibilités étant nombreuses, adaptez ces éléments selon vos besoins.

Déployer le serveur dans le groupe de ressources

1. Connectez-vous au Portail Microsoft Azure.
2. Recherchez la ressource que vous souhaitez installer et accédez à sa page.
3. Cliquez sur **Créer**.
4. Attribuez un nom à cette machine (*Web-Documentation-Server* dans l'exemple).
5. Créez un utilisateur et son mot de passe.
6. Choisissez l'emplacement géographique d'hébergement du serveur.
7. Sélectionnez le groupe de ressources du firewall (*SNS-Documentation* dans l'exemple).
8. Dans les options, sélectionnez le réseau virtuel associé au groupe de ressources ainsi que le sous-réseau privé.
9. Validez.

Récupérer l'adresse IP publique du serveur virtuel

1. Toujours sur le Portail Microsoft Azure, cliquez sur **Groupe de ressources**.
2. Sélectionnez le groupe de ressources concerné (*SNS-Documentation* dans l'exemple).
3. Cliquez sur l'entrée **Adresse IP publique** (*Web-Documentation-Server* dans l'exemple).
4. Notez l'adresse IP publique.

Installer le service souhaité sur le serveur

1. Connectez-vous sur votre serveur.
2. Installez le service souhaité et ses dépendances. Dans l'exemple, nous installons *Apache*.

Autoriser sur le firewall virtuel SNS EVA les flux depuis et vers le serveur virtuel

Maintenant que le firewall et le serveur virtuel sont déployés, vous devez autoriser dans la politique de filtrage du firewall les flux depuis et vers le serveur virtuel.

Les manipulations de ce chapitre sont à réaliser en étant connecté à l'interface d'administration du firewall à l'adresse : https://*adresse_ip_publique_firewall*/admin.

Créer les objets réseau nécessaires

1. Rendez-vous dans **Configuration > Objets > Réseau**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez le type d'objet souhaité à gauche.
4. Définissez un nom à l'objet.
5. Complétez les informations selon la configuration requise.
6. Cliquez sur **Créer**.

Dans l'exemple, nous ajoutons les objets suivants :

Type de l'objet	Nom de l'objet	Informations de l'objet
Réseau	Private_Net	Adresse IPv4 : 192.168.1.0/24
Réseau	Public_Net	Adresse IPv4 : 192.168.0.0/24
Machine	Web_Documentation_Server	Adresse IPv4 : 192.168.1.4
Port	sshwebsrv	Port / Protocole : 222/TCP

Configurer la politique de filtrage et NAT

La politique de filtrage et NAT regroupe un ensemble de règles de filtrage et de règles de NAT. Par défaut, le firewall utilise la politique **(9) Azure Default** qui permet à un administrateur du firewall d'accéder à l'interface d'administration et de bloquer toutes les autres connexions.

Lors de la configuration de la politique de filtrage et NAT de votre firewall :

- Sauvegardez à tout moment les modifications en cours en cliquant sur **Appliquer**,
- Veillez à ne pas activer une politique de filtrage et NAT incomplète ou incorrecte qui pourrait rendre inaccessible l'interface d'administration de votre firewall,
- Gardez en mémoire que le firewall est bloquant : tout flux non explicitement décrit dans la politique est rejeté sans journalisation, même si cette règle n'apparaît pas.

Configurer la politique de filtrage

La configuration s'effectue dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **Filtrage**. Nous ajoutons trois règles afin de répondre aux besoins suivants :

1. Autoriser les machines hébergées sur le réseau privé à accéder à l'ensemble des machines.
2. Autoriser toutes les machines à se connecter sur le serveur virtuel en HTTP.
3. Autoriser toutes les machines à se connecter sur le serveur virtuel en SSH.

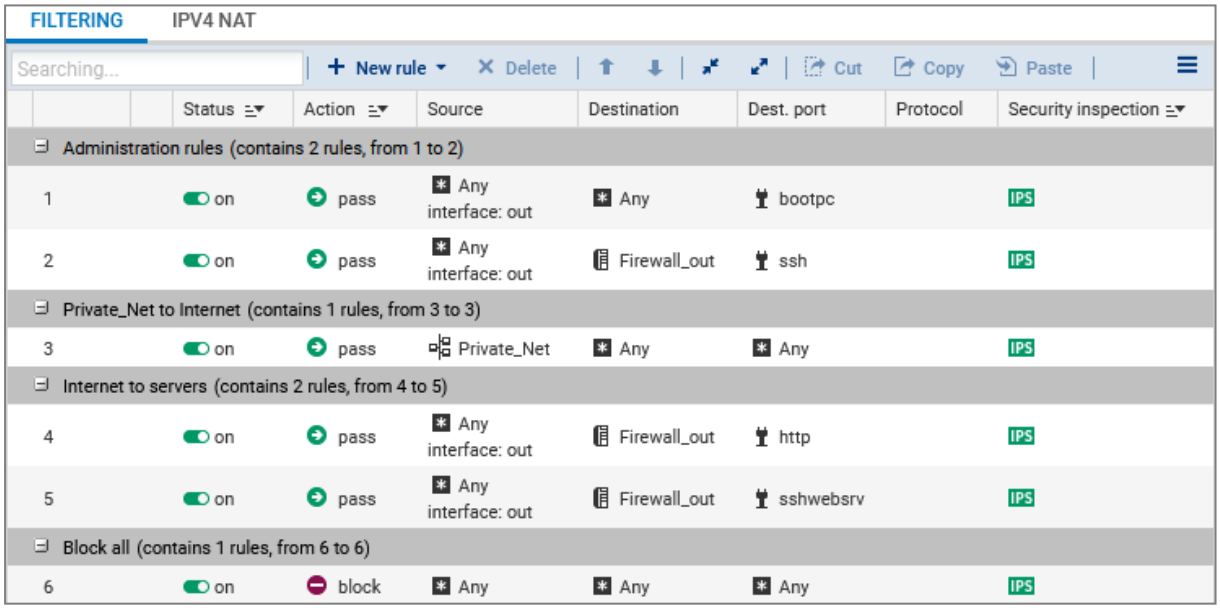
ASTUCE
Ajoutez des séparateurs dans votre politique de filtrage afin d'optimiser son organisation.

Pour ajouter vos règles :

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État**, sélectionnez **On**.
4. Configurez la règle selon vos besoins en naviguant dans les onglets sur la gauche.
5. Cliquez sur **OK**.
   Placez ces règles au-dessus de la règle de blocage avec les boutons **Monter** et **Descendre**.

Dans notre exemple, nous ajoutons les règles suivantes :

Action	Source	Destination	Port dest.	Inspection de sécurité
passer	Private_Net	Any	Any	IPS
passer	Any, via l'interface out	Firewall_out	http	IPS
passer	Any, via l'interface out	Firewall_out	sshwebsrv	IPS



Configurer la politique de NAT

La configuration s'effectue dans **Configuration > Politique de sécurité > Filtrage et NAT**, onglet **NAT**. Nous ajoutons trois règles afin de répondre aux besoins suivants :

1. Transférer les flux SSH adressés à l'interface publique du firewall vers le serveur web.
2. Transférer les flux HTTP adressés à l'interface publique du firewall vers le serveur web.
3. Transférer les flux issus des machines de la DMZ vers celles situées au-delà du firewall.

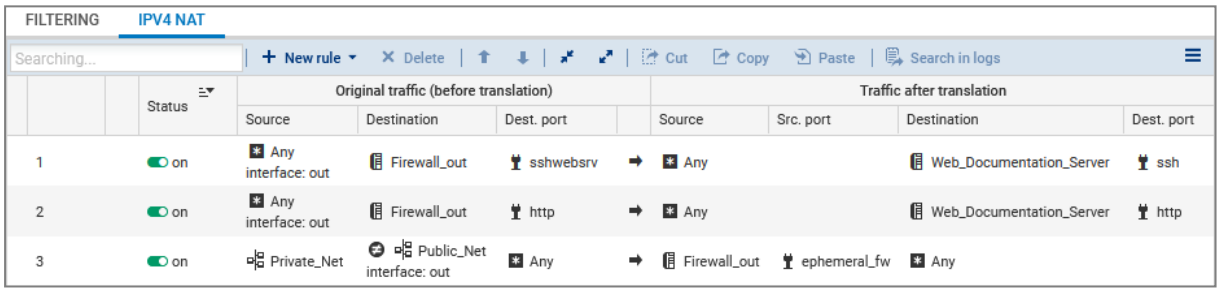
Pour ajouter vos règles :

1. Cliquez sur **Nouvelle règle > Règle simple**.
2. Double-cliquez sur le numéro de la règle pour ouvrir sa fenêtre d'édition.
3. Dans l'onglet **Général**, champ **État**, sélectionnez **On**.

4. Configurez la règle selon vos besoins en naviguant dans les onglets sur la gauche.
5. Cliquez sur **OK**.

Dans notre exemple, nous ajoutons les règles suivantes :

Trafic original (avant translation)			Trafic après translation			
Source	**Destination**	**Port dest.**	**Source**	**Port src.**	**Destination**	**Port dest.**
Any, via l'interface out	Firewall_out	sshwebsrv	Any		Web_Documentation_Server	ssh
Any, via l'interface out	Firewall_out	http	Any		Web_Documentation_Server	http
Private_Net	Différent de Public_Net, via l'interface out	Any	Firewall_out	ephemeral_fw	Any	



Tester la configuration et la sauvegarder

Maintenant que votre firewall est configuré, assurez-vous que tout fonctionne correctement. Si tel est le cas, nous vous recommandons de sauvegarder la configuration du firewall afin de pouvoir la restaurer en cas de besoin.

Tester la configuration

Si des accès ne fonctionnent pas une fois la configuration finalisée, identifiez si le dysfonctionnement est lié à la configuration de votre firewall. Pour cela :

- Procédez à une vérification des règles de votre politique de filtrage et NAT afin d'identifier une éventuelle erreur,
- Il est possible de positionner une règle de *pass all* en premier dans la politique de filtrage afin d'identifier si une règle est trop restrictive. Attention toutefois, ceci compromet la sécurité de votre environnement le temps de réaliser vos tests.

Dans notre exemple, nous réalisons les tests suivants :

1. **Test des flux sortants (depuis la DMZ vers Internet)**
   - Réalisez une connexion HTTP depuis le serveur Web (*Web-Documentation-Server* dans l'exemple) vers un serveur Web externe,
   - Visualisez les traces de ces connexions dans l'interface d'administration du firewall dans **Monitoring > Logs - Journaux d'audit > Trafic réseau**.
2. **Test des flux entrants (depuis Internet vers la DMZ)**
   - Établissez une connexion Web depuis une machine située hors de l'infrastructure Microsoft Azure vers la page *index.htm* du serveur Web virtuel,
   - Visualisez les traces des connexions établies ainsi que les opérations de NAT dans l'interface d'administration du firewall dans **Monitoring > Logs - Journaux d'audit > Trafic réseau**.

Sauvegarder la configuration

Réalisez une sauvegarde manuelle de la configuration du firewall dans **Configuration > Système > Maintenance**, onglet **Sauvegarder**. Activez une sauvegarde automatique de sa configuration depuis ce même module.

Pour plus d'informations, reportez-vous sur le chapitre **Maintenance** du manuel utilisateur SNS.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles sur les liens suivants :

- Documentations techniques liées aux topologies VPN.
- Site web de la documentation technique SNS (notes de version, guides, notes techniques).
- Outil de recherche d'un partenaire si besoin d'accompagnement pour une configuration plus complexe.
- Base de connaissances Stormshield (authentification nécessaire).
- Aide en ligne MyStormshield.

documentation@stormshield.eu