GUIDE

STORMSHIELD NETWORK SECURITY PAY AS YOU GO

GUIDE DE DÉPLOIEMENT D'UN FIREWALL VIRTUEL SNS PAYG

Produits concernés : SNS 3.11.17 et versions supérieures ou SNS 4.3.9 et versions supérieures

Dernière mise à jour du document : 10 avril 2024

Référence : sns-fr-guide_de_deploiement_pay_as_you_go

Table des matières

Avant de commencer

Bienvenue dans le guide de déploiement d'un firewall virtuel SNS PAYG.

Cette documentation est destinée exclusivement aux partenaires Stormshield revendeurs ou intégrateurs.

Les firewalls virtuels SNS PAYG sont destinés aux fournisseurs de Cloud privé proposant des services hébergés et/ou d'accès à Internet, en SaaS ou en IaaS. En les déployant dans votre infrastructure virtuelle, vous pouvez proposer à vos clients un service de sécurité réseau avec une facturation mensuelle basée sur le nombre et la taille des firewalls virtuels utilisés.

Dans cette documentation, Stormshield Network Security Pay As You Go est désigné sous la forme abrégée SNS PAYG.

IMPORTANT
Cette documentation concerne uniquement les firewalls virtuels SNS PAYG. Pour les firewalls physiques SNS ou virtuels SNS EVA, des guides d'installation spécifiques existent.

Prérequis

Les tableaux ci-dessous reprennent l'ensemble des prérequis techniques.

Versions SNS

3.11.17 et versions supérieures 4.3.9 et versions supérieures

Hyperviseurs

Vous devez être familiarisé avec l'un des environnements virtuels ci-dessous afin de déployer un firewall virtuel SNS PAYG.

	Nombre d'interfaces connectées à la machine virtuelle	Version de l'hyperviseur
VMware ESXi	1 interface min. 10 interfaces max.	Pour plus d'informations, reportez-vous au Guide de cycle de vie produits.
Citrix XenServer	1 interface min. 7 interfaces max.	
Microsoft Hyper-V	1 interface min. 8 interfaces max.	
Linux KVM	1 interface min. Max : dépend de l'éditeur Linux choisi	

Les machines virtuelles doivent disposer d'un accès à Internet en HTTPS (port 443).

Cas d'usage

Les firewalls virtuels SNS PAYG sont principalement utilisés dans deux cas : la protection de l'accès aux services hébergés et la protection de l'accès des utilisateurs à Internet. Cet usage détermine le niveau de protection nécessaire.

Protection de l'accès aux services hébergés

En tant que fournisseur de services, vous hébergez les serveurs et applications de vos clients dans votre infrastructure virtuelle. En déployant SNS PAYG, vous sécurisez les connexions de vos clients vers leurs ressources dans votre centre de données :

- Les connexions des utilisateurs situés dans les locaux de vos clients,
- Les connexions des utilisateurs nomades situés à l'extérieur des locaux.

Dans ce cas, seule la fonction VPN est nécessaire. Choisissez le niveau de protection **Standard** qui permet de protéger les connexions des utilisateurs via un VPN.

Protection de l'accès des utilisateurs à Internet

En tant que fournisseur d'accès à Internet pour vos clients, vous déployez SNS PAYG dans votre infrastructure afin de protéger la navigation des utilisateurs passant par votre centre de données.

Dans ce cas, une protection complète est nécessaire. Choisissez le niveau de protection **Premium** qui assure une protection des serveurs, notamment grâce aux fonctionnalités d'antivirus, de base d'URL Extended Web Control et de management des vulnérabilités.

Enregistrer le produit SNS PAYG

Pour enregistrer votre produit SNS PAYG, 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 ces éléments récupérés, l'enregistrement se réalise depuis l'espace personnel MyStormshield. Il permet notamment d'associer votre produit à votre espace MyStormshield. La procédure d'enregistrement est différente selon si vous possédez ou non déjà un espace.

Vous ne possédez pas d'espace MyStormshield

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

Pour plus d'informations, reportez-vous au guide Créer un compte et enregistrer un produit.

Vous possédez déjà un espace MyStormshield

L'enregistrement de votre produit se réalise depuis votre espace MyStormshield.

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

Télécharger le fichier d'installation

1. Dans votre espace personnel MyStormshield, rendez-vous dans **Téléchargements > Téléchargements**.
2. Dans les catégories, sélectionnez **Stormshield Network Security > Firmware >**, puis **4.X** ou **3.X** selon la branche de version souhaitée.
3. Dans la fenêtre **Stormshield Network Security - Firmware - V X.Y.Z**, avec X.Y.Z supérieur ou égal à 4.3.9 ou 3.11.17, sélectionnez l'image d'installation au format souhaité :
   - *kvm* pour les plate-formes basées sur KVM,
   - *openstack* pour les plate-formes basées sur Openstack,
   - *ova* pour les plate-formes VMware,
   - *vhd* pour les plate-formes basées sur Microsoft Hyper-V.
4. Enregistrez le fichier sur votre poste de travail.

Déployer le fichier d'installation sur une plate-forme

Cette procédure est un exemple basé sur une plate-forme VMware. Vous devez l'adapter si vous utilisez un autre environnement virtuel.

1. Ouvrez vSphere Client depuis votre station d'administration.
2. Indiquez les paramètres de connexion à vCenter Server (Adresse IP / Nom d'hôte, Nom d'utilisateur et Mot de passe).
3. Cliquez sur **Connexion**.
4. Cliquez sur **Fichier > Déployer modèle OVF...**.
5. Cliquez sur **Parcourir**, sélectionnez le fichier d'installation *.ova* téléchargé précédemment, puis cliquez sur **Suivant**.
6. Lisez et acceptez les conditions d'utilisation, puis cliquez sur **Suivant**.
7. Sélectionnez l'emplacement d'inventaire où installer la machine virtuelle et cliquez sur **Suivant**.
8. Sélectionnez l'hôte / cluster qui doit héberger la machine virtuelle et cliquez sur **Suivant**.
9. Sélectionnez l'emplacement de stockage et cliquez sur **Suivant**.
10. Validez le format de disque en cliquant sur **Suivant**.
11. Sélectionnez le réseau utilisé par chaque interface de la machine virtuelle et cliquez sur **Suivant**.
12. Remplissez le formulaire de configuration de base du firewall. Cette étape est optionnelle si vous déployez un firewall virtuel SNS PAYG.
    - Configuration globale :
      - **Customer ID** : identifiant client optionnel. Laissez ce champ vide à cette étape. Vous le remplirez plus tard dans le cadre du déploiement de firewalls virtuels SNS si vous souhaitez les associer à un client particulier,
      - **Hostname** : nom du firewall,
      - **Password** : indiquez puis confirmez le mot de passe du compte administrateur du firewall. Choisissez un mot de passe complexe respectant les recommandations d'organismes comme l'ANSSI.
    - Interface réseau 1 (out) :
      - **Gateway** : adresse IP de la passerelle par défaut du firewall. Laissez vide si DHCP,
      - **IP address 1** : adresse IP de la première interface réseau du firewall. Indiquez **DHCP** pour une attribution dynamique d'adresse,
      - **Netmask** 1 : masque de réseau. Laissez vide si DHCP.
    - Interface réseau 2 (in) :
      - **IP address 2** : adresse IP de la deuxième interface réseau du firewall. Indiquez **DHCP** pour une attribution dynamique d'adresse,
      - **Netmask** 2 : masque de réseau. Laissez vide si DHCP.
13. Cliquez sur **Suivant**.
14. Vérifiez les informations du résumé et cliquez sur **Terminer**.
    Le déploiement de votre firewall virtuel SNS se lance automatiquement.

Activer le firewall virtuel SNS PAYG

Télécharger le kit d'activation

1. Dans votre espace personnel MyStormshield, rendez-vous dans **Produit > Gestion des produits**.
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 concernée. Elle doit correspondre à la version du fichier d'installation téléchargé précédemment.
4. Cliquez sur le lien **Télécharger le kit d'activation**, puis acceptez le téléchargement.

Importer le kit d'activation

1. Démarrez le firewall virtuel SNS PAYG. Par défaut, son numéro de série est *VMSNSX00Z0000A0*.
2. Dans l'interface Web d'administration du firewall virtuel, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Mise à jour du système**.
3. Sélectionnez le kit d'activation (*.maj*) téléchargé précédemment.
4. Cliquez sur **Mettre à jour le firewall**. Le firewall redémarre automatiquement.
5. Connectez-vous à son interface Web d'administration et authentifiez-vous. La mention **VPAYG** dans le bandeau supérieur confirme que vous disposez d'un firewall SNS PAYG.

Créer le modèle de firewall virtuel SNS PAYG

Une fois le firewall SNS PAYG initialisé, vous devez créer un modèle que vous pourrez dupliquer par la suite pour créer tous vos firewalls virtuels SNS PAYG.

Configurer le firewall modèle

Modifiez la configuration du firewall afin de créer un modèle avec une configuration de base. Par exemple :

- Modifiez la politique de filtrage par défaut pour l'adapter à vos besoins,
- Activez le service NTP pour synchroniser l'heure du firewall,
- Activez le service SSHD si vous souhaitez administrer le firewall via SSH.

Cette liste n'est pas exhaustive. Activez les services nécessaires à l'ensemble de vos clients.

Supprimer les paramètres OVF env (VMware uniquement)

Si vous utilisez les propriétés *OVF env* (vApp), il est recommandé d'en réinitialiser les valeurs afin que les firewalls créés à partir du modèle n'en héritent pas.

1. Ouvrez vSphere Client depuis votre station d'administration.
2. Sélectionnez votre machine virtuelle PAYG et cliquez sur l'onglet **Configuration** dans le panneau de droite.
3. Sélectionnez **Paramètres> Options vApp**. Les paramètres *OVF env* s'affichent.
4. Cliquez sur le bouton **Éditer** et supprimez toutes les valeurs des paramètres **Global configuration** et **Network interface**.

Créer une sauvegarde de la machine virtuelle

Nous vous recommandons de réaliser une sauvegarde de la machine virtuelle en vue d'éventuelles modifications du modèle, par exemple une mise à jour de sa version ou des évolutions de sa configuration de base.

Convertir la machine virtuelle en modèle PAYG

Une fois la configuration terminée, vous devez convertir la machine virtuelle en modèle PAYG.

1. Accédez à la console du firewall via l'hyperviseur ou via un client SSH.
2. Exécutez la commande `paygprep`.
   Vous êtes prévenu que la machine virtuelle sera éteinte à la fin du processus.
3. À la question *Voulez-vous continuer ?*, répondez *y* (Oui).
4. À la question *Voulez-vous réinitialiser la configuration ?*, répondez *n* (Non), sauf si vous souhaitez repartir d'une configuration usine.
5. À la question *Voulez-vous configurer la VM avec wizardinit ou un environnement OVF au prochain démarrage ?*, répondez *y* (Oui) si vous souhaitez configurer les paramètres réseau, le nom d'hôte, le mot de passe admin et l'identifiant client de la nouvelle machine déployée à son démarrage.
   Le résumé du paramétrage que vous venez d'effectuer s'affiche.

6. À la question *Voulez-vous continuer ?*, répondez *y* (Oui) si tout vous semble correct.
   La machine virtuelle s'éteint.
7. Dans votre hyperviseur, effectuez un clic droit sur votre machine virtuelle PAYG et sélectionnez le menu **Modèle > Convertir au modèle** dans vSphere ou **Convertir au modèle** dans XenCenter et KVM. Sur Hyper-V, clonez la machine virtuelle pour créer le modèle.

La machine virtuelle est transformée en modèle PAYG. Vous pouvez la dupliquer à votre convenance.

```
VMSNSX08I0038A9>paygprep
This tool will prepare and halt this vm for cloning/template
Do you want to continue ?
[y|N]: y
Do you want to reset the configuration ?
[y|N]:
Do you want to configure the VM with wizardinit or OVF environment at next boot
?
[y|N]: Y

Could you please validate the following settings:
 Reset configuration: No
 VM wizardinit or OVF environment at next boot: Yes
Do you want to proceed ?
[y|N]: ^[[J
```

Déployer le firewall virtuel SNS PAYG à partir d'un modèle

Une fois votre modèle de firewall SNS PAYG créé, vous pouvez déployer de nouvelles machines à partir de ce modèle.

IMPORTANT
Le firewall virtuel doit disposer d'un accès à Internet pour pouvoir s'enrôler auprès du service Cloud Pay As You Go de Stormshield.

Environnement VMware

1. Dans vSphere Client, effectuez un clic droit sur votre modèle et sélectionnez **Nouvelle VM à partir de ce modèle**.
2. Définissez le nom de votre firewall virtuel SNS PAYG et choisissez son emplacement.
3. Choisissez la ressource de calcul et le stockage. Ne sélectionnez pas d'option de clonage.
4. Modifiez les paramètres selon vos besoins : nom d'hôte, ID client, paramètres réseau. Entrez un identifiant client de votre choix (Customer ID) si vous souhaitez associer ce firewall à un client particulier. Cette information accompagnera le numéro de série dans les rapports d'activité qui vous seront envoyés en complément de la facturation mensuelle.
5. Cliquez sur **Terminer** pour valider vos paramètres.
6. Démarrez votre firewall virtuel.
   - **Une fois la connexion réseau établie** : le firewall contacte le service Cloud afin d'obtenir une identité, un certificat et une licence. Cette étape prend quelques minutes. Un message sur la console indique que le firewall est enrôlé et qu'il va redémarrer,
   - **En cas d'erreur d'enrôlement** : vérifiez la connexion à Internet et redémarrez le firewall virtuel afin de relancer le processus d'enrôlement.
7. Une fois le firewall enrôlé et redémarré, il dispose d'un nouveau numéro de série, par exemple *VMSNSX08J0162B9-76DAA1B6*.

Autres environnements de virtualisation

1. Créez un nouveau firewall virtuel SNS PAYG à partir du modèle (pour XenServer et KVM) ou du clone (pour Hyper-V), et démarrez-le.
2. Accédez à la console. Un assistant de première installation vous guide dans la configuration. Il vous permet de choisir un mot de passe pour le super-utilisateur *admin*, de configurer les paramètres réseau de chaque interface détectée et de spécifier un ID client.
   - **Une fois la connexion réseau établie** : le firewall contacte le service Cloud afin d'obtenir une identité, un certificat et une licence. Cette étape prend quelques minutes. Un message sur la console indique que le firewall est enrôlé et qu'il va redémarrer,
   - **En cas d'erreur d'enrôlement** : vérifiez la connexion à Internet et redémarrez le firewall virtuel afin de relancer le processus d'enrôlement.
3. Une fois le firewall enrôlé et redémarré, il dispose d'un nouveau numéro de série, par exemple *VMSNSX08J0162B9-76DAA1B6*.

```
########################################
setting password for admin
enter password:
verify:
Modify SRP/SSH password of user 'admin' successful

############################################
## Configure initial network connection ##
############################################

Current network settings:
 1st interface (out): DHCP
 2nd interface (in): DHCP

Change 1st network interface (out) settings ? [y|N]:
Change 2nd network interface (in) settings ? [y|N]:
Will you configure your virtual appliance through its first interface (out) ?
[Y/n]:

###################################
## Configure customer identifier ##
###################################

Specify Customer Identifier or leave empty (64 chars max): mycustomer
```

Administrer le firewall virtuel SNS PAYG

Les firewalls virtuels SNS PAYG peuvent être administrés via l'interface Web d'administration. Pour un grand nombre de firewalls, utilisez plutôt le serveur Stormshield Management Center ou un orchestrateur combiné à l'API NSRPC.

Pour modifier les paramètres système de la machine virtuelle, utilisez votre hyperviseur.

Consulter le tableau de bord du firewall virtuel dans l'interface Web d'administration

1. Connectez-vous à l'interface Web d'administration du firewall virtuel (https://*adresse_IP_firewall*/admin). S'il est configuré en DHCP, relevez sur la console son adresse IP.
2. La mention **VPAYG-EVA** dans le bandeau supérieur précise le modèle EVA pris en compte pour la facturation mensuelle, qui dépend des ressources de la machine virtuelle.
3. Le widget **Propriétés** du **Tableau de bord** affiche les informations générales du firewall.

Ce tableau présente les caractéristiques techniques de chaque modèle 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

Une machine EVA doit disposer au minimum d'1 Go de mémoire. En cas d'utilisation intensive de l'antivirus et de l'analyse Sandboxing, 2 Go de mémoire minimum sont recommandés.

Modifier la quantité de mémoire du firewall virtuel

Vous pouvez augmenter la mémoire du firewall virtuel SNS PAYG afin de changer de modèle de firewall virtuel et d'exploiter plus de processeurs pour gérer davantage d'utilisateurs.

Notez que l'augmentation de la mémoire entraîne une modification des conditions tarifaires. Pour plus d'informations, contactez votre représentant commercial Stormshield

IMPORTANT
Il n'est pas recommandé de diminuer la mémoire du firewall virtuel. Avant de le faire, assurez-vous que les nouvelles limites appliquées seront compatibles avec la configuration en place.

1. Dans l'interface Web d'administration, rendez-vous dans **Configuration > Système > Maintenance**, onglet **Configuration** et cliquez sur **Arrêter le firewall**.
2. Attendez que le firewall virtuel s'arrête.
3. Dans votre hyperviseur, rendez-vous dans les propriétés de la machine virtuelle et modifiez la mémoire, par exemple de *1024 Mo* à *3072 Mo*. Vous pouvez également ajouter des processeurs si besoin.
4. Redémarrez la machine virtuelle.

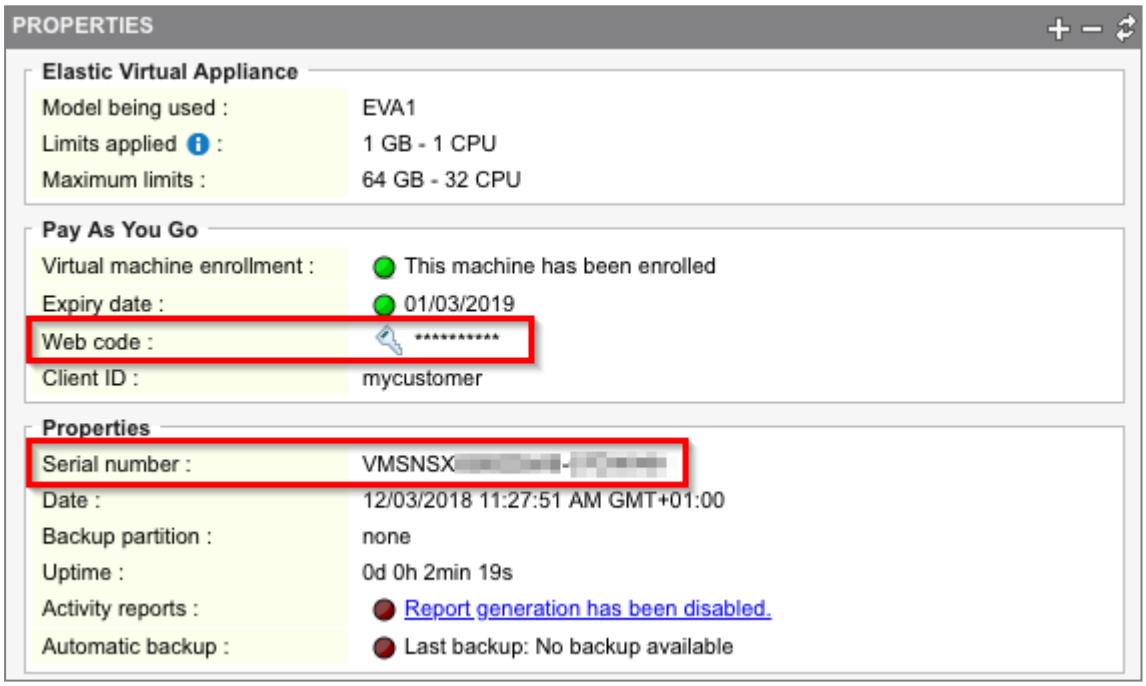
5. Reconnectez-vous à l'interface Web d'administration du firewall virtuel.
   Sur le **Tableau de bord**, le widget **Propriétés** affiche le nouveau modèle de firewall virtuel (par exemple VPAYG-EVA2 pour une mémoire de 3 Go) ainsi que les nouvelles limites de ce modèle. Pour plus d'informations sur les limites de chaque modèle, reportez-vous à la section Consulter le tableau de bord du firewall virtuel dans l'interface Web d'administration.

Enregistrer le firewall virtuel sur MyStormshield

Dans votre espace personnel MyStormshield, vous devez enregistrer votre firewall virtuel SNS PAYG afin de bénéficier des services de support technique et de sauvegarde dans le Cloud.

Complétez les informations demandées jusqu'à l'enregistrement du firewall. Le numéro de série et le mot de passe (Code Web) sont indiqués dans le widget **Propriétés** du **Tableau de bord** de l'interface Web d'administration du firewall.

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



Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions peuvent être disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu