NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

EVA SUR 3DS OUTSCALE

Produits concernés : SNS 3.11.8 LTSB et versions supérieures, SNS 4.x

Dernière mise à jour du document : 4 juin 2021

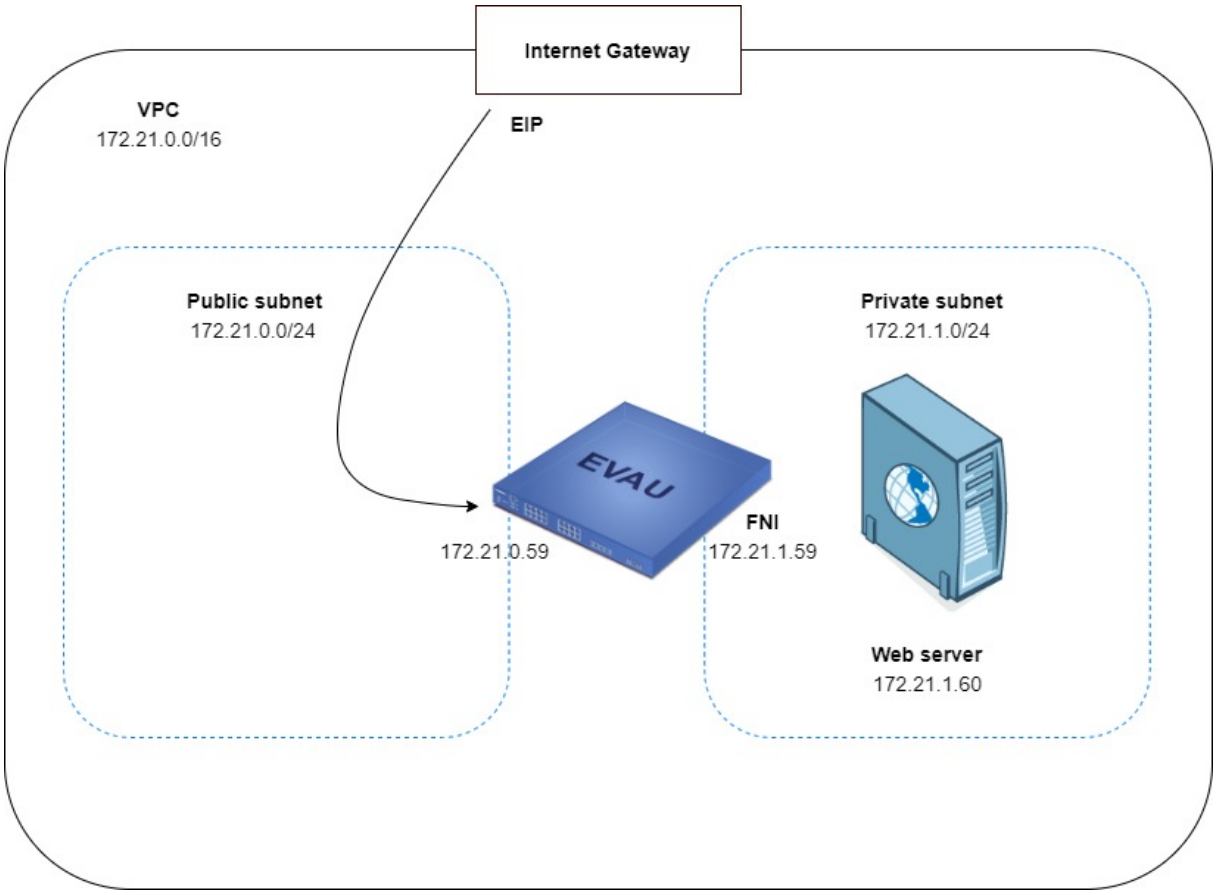
Référence : sns-fr-eva_sur_3DS_OUTSCALE_note_technique

Table des matières

Avant de commencer

Cette note technique présente le déploiement, sur la plate-forme d'hébergement 3DS OUTSCALE, d'un firewall Stormshield Network Security Elastic Virtual Appliance (EVA) et d'un serveur Web protégé par ce firewall.

Le firewall déployé est doté de deux interfaces réseau : une interface publique (interface non protégée) et une interface privée (interface protégée).



Obtenir la licence du firewall

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

Rapprochez-vous de votre distributeur Stormshield afin de commander la licence de votre EVA. 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 SNS EVA

Le déploiement d'un firewall SNS EVA sur la plate-forme Outscale nécessite un certain nombre d'étapes, toutes réalisées depuis la console d'administration Outscale.

Pour ce faire, connectez-vous à la console COCKPIT 3DS OUTSCALE.

Les étapes de configuration nécessaires sont les suivantes :

- Créer une clé SSH (*Keypair)*,
- Créer un Cloud Privé Virtuel (*VPC - Virtual Private Cloud*),
- Créer une passerelle Internet (*Gateway*),
- Créer une route par défaut,
- Créer un groupe de sécurité pour les flux avec l'extérieur,
- Créer un groupe de sécurité pour les flux entre machines protégées,
- Créer l'instance du firewall SNS EVA,
- Allouer une adresse IP externe (EIP) à l'instance SNS,
- Créer l'interface réseau privée de l'instance SNS,
- Désactiver l'option **Vérifier source / destination,**
- Créer une nouvelle table de routage et une route par défaut pour le réseau privé,
- Activer le firewall SNS EVA.

Créer une clé SSH (*Keypair*)

Cette clé permet de s'authentifier sur les machines déployées sur la plate-forme Outscale (firewall SNS, serveur Web...) au travers du protocole SSH.

Créer une clé SSH

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Keypairs**.
2. Cliquez sur **Créer.**
3. Entrez un nom pour la nouvelle clé SSH (exemple : *Documentation-keypair*) et cliquez sur **Créer**.
   Une clé SSH est générée et une boite de dialogue s'ouvre pour la télécharger.
4. Téléchargez la clé SSH et enregistrez-la sur votre poste de travail.

Créer un VPC pour les instances à déployer

Le VPC (*Virtual Private Cloud*) est le réseau virtuel dans lequel seront déployés le firewall SNS EVA et les machines qu'il protège. Le VPC est constitué de deux sous-réseaux :

- Un sous-réseau public auquel sera attachée l'interface publique (out) du firewall SNS EVA,
- Un sous-réseau privé auquel seront attachées l'interface privée (in) du firewall SNS EVA et les interfaces des machines protégées.

Créer le VPC

Dans la console COCKPIT 3DS OUTSCALE, menu **VPC** :

1. Sélectionnez **VPC**.
2. Cliquez sur **Créer** puis **Mode expert**.
3. Entrez un nom pour le VPC (exemple : *Documentation-VPC*) ainsi que le réseau associé en notation CIDR (exemple : *172.21.0.0/16*).
4. Validez en cliquant sur **Créer**.

Créer le sous-réseau publique du VPC

1. Cliquez sur le VPC précédemment créé pour le sélectionner (*Documentation-VPC* dans l'exemple).
   Le détail du VPC s'affiche dans la partie inférieure de l'écran de configuration.
2. Cliquez sur **Créer un subnet**.
3. Entrez un nom (exemple : *Documentation-VPC-Public*) ainsi que le réseau associé en notation CIDR (exemple : *172.21.0.0/24*).
   Ce sous-réseau est obligatoirement inclus dans le réseau du VPC.
4. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible (*eu-west-2a* dans l'exemple).
5. Validez en cliquant sur **Créer**.

Créer le sous-réseau privé du VPC

1. Cliquez de nouveau sur **Créer un subnet**.
2. Entrez un nom (exemple : *Documentation-VPC-Private*) ainsi que le réseau associé en notation CIDR (exemple : *172.21.1.0/24*).
   Ce sous-réseau est obligatoirement inclus dans le réseau du VPC.
3. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible (*eu-west-2*a dans l'exemple).
4. Validez en cliquant sur **Créer**.

Créer une passerelle Internet (*Internet Gateway*)

Il s'agit de la passerelle d'accès à Internet pour le firewall SNS EVA et pour les machines qu'il protège.

Créer la passerelle Internet

Dans la console COCKPIT 3DS OUTSCALE, menu **VPC :**

1. Sélectionnez **Internet gateways**.
2. Cliquez sur **Créer.**
3. Validez en cliquant sur **Créer**.

Rattacher la passerelle Internet au VPC du firewall

1. Sélectionnez la passerelle créée dans l'étape précédente.
2. Cliquez sur **Attacher**.
3. Sélectionnez le VPC du firewall (*Documentation-VPC* dans l'exemple).
4. Validez en cliquant sur **Attacher**.

Créer une route par défaut

L'objectif est de créer une route par défaut vers la passerelle internet pour tous les flux sortants.

Créer la route par défaut dans la table de routage du VPC

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Route tables**.
2. Sélectionnez la table de routage correspondant au VPC précédemment créé (*Documentation-VPC* dans l'exemple).
   Le détail de la table de routage s'affiche dans la partie inférieure de l'écran de configuration.
3. Dans le détail de la table de routage, cliquez sur **Créer une route**.
4. Dans le champ **Cible**, sélectionnez votre passerelle Internet.
5. Cliquez sur le bouton **Toutes les IP**.
   Le champ **Destination** est automatiquement complété avec la valeur 0.0.0.0/0.
6. Validez en cliquant sur **Créer**.

Attacher cette table de routage au sous-réseau public du VPC

1. Sélectionnez la table de routage correspondant au VPC précédemment créé (*Documentation-VPC* dans l'exemple).
2. Cliquez sur **Attacher**
3. Sélectionnez le sous réseau public du VPC (*Documentation-VPC-Public* dans l'exemple).
4. Cliquez sur **Attacher** pour valider la configuration.
   La colonne **Associations** reflète ce nouvel état (passage de 0 à 1).

Créer un groupe de sécurité pour les flux depuis et vers l'extérieur

Ce groupe de sécurité rassemble les règles de flux autorisés depuis les réseaux externes vers le firewall et les machines protégées, et depuis les réseaux protégés vers l'extérieur.
Dans le cadre de cette note technique, les flux entrants autorisés sont les suivants :

- SSH : accès en console au firewall,
- Port de redirection SSH (exemple : TCP/2222) : accès en console au serveur Web protégé,
- HTTPS : accès à l'interface Web d'administration du firewall,
- HTTP : accès au serveur Web protégé par le firewall.

Créer le groupe de sécurité

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Security groups**.
2. Cliquez sur **Créer**.
3. Nommez le groupe de sécurité (exemple : *Documentation-Security-Group*).
4. Ajoutez une description (exemple : *SSH HTTPS HTTP Inbound access*).
5. Sélectionnez le VPC (*Documentation-VPC* dans l'exemple).
6. Cliquez sur **Créer**.

Créer les règles de sécurité correspondant aux flux autorisés avec l'extérieur

1. Sélectionnez le groupe de sécurité précédemment créé (*Documentation-Security-Group* dans l'exemple).
   La liste des règles attachées au groupe de sécurité s'affiche dans la partie inférieure de l'écran de configuration.
2. Dans la liste des règles, cliquez sur **Créer une règle**.
3. Sélectionnez le mode **Entrant**.
4. Sélectionnez le protocole **SSH**.
5. Cliquez sur **Toutes les IP**.
6. Cliquez sur le symbole "+".
7. Recommencez les étapes 3 à 6 avec les protocoles **HTTP** et **HTTPS**.
8. Recommencez les étapes 3 à 6 avec les valeurs **Entrant**, **Personnalisé, TCP**, **2222** et **Toutes les IP**.
9. Validez les règles en cliquant sur **Créer**.

IMPORTANT
Une règle autorisant des flux sortants est automatiquement créée.
Cette règle ne doit pas être supprimée car elle autorise, notamment, les flux sortants nécessaires pour les mises à jour de sécurité des instances déployées dans le VPC.

La liste des règles de flux autorisés pour le groupe de sécurité prend donc la forme suivante :

Details for Documentation-Security-Group (sg-50df5ea2)

+ CREATE RULE | − DELETE RULE

Service	Type	Protocol	From Port	To Port	CIDR	Group
SSH	inbound	tcp	22	22	0.0.0.0/0	
HTTP	inbound	tcp	80	80	0.0.0.0/0	
HTTPS	inbound	tcp	443	443	0.0.0.0/0	
Custom	outbound	-1			0.0.0.0/0	

Créer un groupe de sécurité pour les flux entre machines protégées

Ce groupe de sécurité rassemble les règles de flux autorisés entre les machines protégées.

Dans cet exemple, tous les protocoles sont autorisés : le filtrage et l'inspection de sécurité des flux entre les machines protégées peuvent en effet être réalisés de manière fine au niveau du firewall SNS.

Créer le groupe de sécurité

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

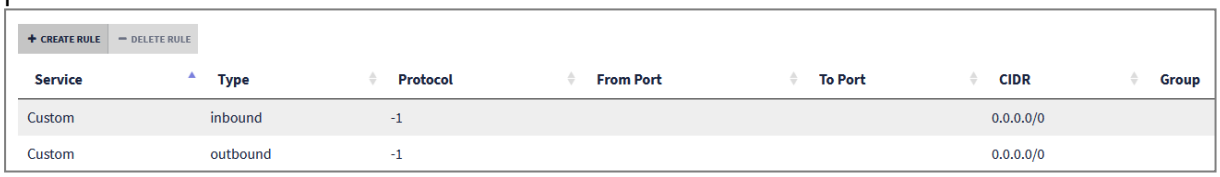
1. Sélectionnez **Security groups**.
2. Cliquez sur **Créer**.
3. Nommez le groupe de sécurité (*Documentation-Pass-All* dans l'exemple).
4. Ajoutez une description (*Pass all* dans l'exemple).
5. Sélectionnez le VPC (*Documentation-VPC* dans l'exemple).
6. Cliquez sur **Créer**.

Créer les règles de sécurité correspondant aux flux entre machines protégées

1. Sélectionnez le groupe de sécurité précédemment créé (*Documentation-Pass-All* dans l'exemple).
   La liste des règle du groupe de sécurité s'affiche dans la partie inférieure de l'écran de configuration.
2. Dans la liste des règles, cliquez sur **Créer une règle**.
3. Sélectionnez le mode **Entrant**.
4. Sélectionnez le protocole **Personnalisé**.
5. Sélectionnez le port **Tous**.
6. Cliquez sur **Toutes les IP**.
7. Cliquez sur le symbole "+".
8. Validez la règle en cliquant sur **Créer**.

IMPORTANT
Une règle autorisant des flux sortants est automatiquement créée.
Cette règle ne doit pas être supprimée.

La liste des règles de flux autorisés pour le groupe de sécurité attribué aux machines protégées prend donc la forme suivante :



Service	Type	Protocol	From Port	To Port	CIDR	Group
Custom	inbound	-1			0.0.0.0/0	
Custom	outbound	-1			0.0.0.0/0	

Créer l'instance du firewall SNS EVA

L'instance de firewall SNS EVA déployée est rattachée aux VPC, groupe de sécurité pour les flux avec l'extérieur, clé SSH et réseau public précédemment créés.

Créer l'instance de firewall

Dans la console COCKPIT 3DS OUTSCALE, menu **Calcul** :

1. Sélectionnez **Instances**.
2. Cliquez sur **Créer** puis **Mode expert**.
3. Nommez l'instance (exemple : *Documentation-SNS-EVA*) et cliquez sur **Suivant**.
4. Indiquez SNS dans le champ de recherche puis sélectionnez le modèle de firewall souhaité.
5. Cliquez sur **Suivant**.
6. Sélectionnez les caractéristiques de votre instance, en lien avec les caractéristiques choisies lors de l'acquisition de votre licence EVA auprès de Stormshield (cf. fiche produit Stormshield Network Security Elastic Virtual Appliances – EVA) :
   - Le type de **CPU**,
   - Le niveau de **Performance** souhaité (paramètre 3DS OUTSCALE),
   - Le nombre de **Cœurs**,
   - La quantité de **Mémoire** (Go) allouée à la machine virtuelle.

> **IMPORTANT**
> Pour obtenir des performances optimales, veillez à l'adéquation entre ces caractéristiques et celles liées à la licence de votre EVA.

7. Cliquez sur **Suivant**.
8. Sélectionnez le **VPC** (*Documentation-VPC* dans l'exemple).
9. Sélectionnez le sous-réseau public du VPC (*Documentation-VPC-Public* dans l'exemple).
10. Choisissez l'adresse IP à associer à l'interface publique du firewall.
    Cette adresse (172.21.0.59 dans l'exemple) doit appartenir au sous-réseau sélectionné à l'étape 9.
11. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible (*eu-west-2a* dans l'exemple).
12. Cliquez sur **Suivant**.
13. Sélectionnez le groupe de sécurité pour les flux avec l'extérieur (*Documentation-Security-Group* dans l'exemple).
14. Cliquez sur **Suivant**.
15. Sélectionnez la clé SSH créée en tout début de procédure (*Documentation-Keypair* dans l'exemple).
16. Cliquez deux fois sur **Suivant**.
    Un résumé de l'instance vous est proposé.
17. Validez la création de l'instance en cliquant sur **Créer**.

> **NOTE**
> Le mot de passe du compte *admin* est égal à l'ID de l'instance.
> Ce compte *admin* permet de se connecter :
>
> - En SSH sur l'adresse IP publique du firewall à l'aide d'un outil de type *Putty*,
> - En HTTPS sur l'interface Web d'administration du firewall (https://adresse_IP_publique_firewall/admin).
>
> Pour des raisons de sécurité, ce mot de passe devra être changé lors de la première connexion au firewall.

Allouer une adresse IP externe (EIP) à l'instance SNS

Créer l'adresse IP externe

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité :**

1. Sélectionnez **IP externes**.
2. Cliquez sur **Allouer**
3. Nommez l'adresse IP externe (exemple : *Documentation-Public-IP*).
4. Validez en cliquant sur **Allouer**.
   Une adresse IP externe est créée.

Allouer l'adresse à l'instance

1. Sélectionnez l'adresse IP externe précédemment créée (*Documentation-Public-IP* dans l'exemple)
2. Cliquez sur **Associer instance**.
3. Sélectionnez votre instance SNS EVA (*Documentation-SNS-EVA* dans l'exemple).
4. Validez en cliquant sur **Associer**.

Créer l'interface privée de l'instance SNS

Il s'agit de créer une deuxième interface réseau (située dans le réseau privé) pour l'instance SNS dans le VPC.

Cette interface sera associée à l'interface protégée (interface *in*) du firewall.

Créer l'interface (Flexible Network Interface) privée

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité :**

1. Sélectionnez **Flexible network interfaces**.
2. Cliquez sur **Créer**.
3. Nommez l'interface (exemple : *Documentation-Private-Interface*).
   Vous pouvez ajouter une **Description** (optionnel).
4. Sélectionnez le sous réseau privé de votre VPC (*Documentation-VPC-Private* dans l'exemple).
5. Choisissez une adresse IP pour cette interface privée (exemple : *172.21.1.59*). Cette adresse doit appartenir au sous-réseau privé sélectionné à l'étape 5.
6. Sélectionnez le groupe de sécurité pour les flux entre machines protégées (*Documentation-Pass-All* dans l'exemple).
7. Cliquez sur **Créer**.

Attacher cette interface à l'instance SNS EVA

Dans la liste des interfaces :

1. Sélectionnez l'interface précédemment créée (*Documentation-Private-Interface* dans l'exemple)
2. Cliquez sur **Attacher**.
3. Sélectionnez l'instance EVA (*Documentation-SNS-EVA* dans l'exemple).
4. Pour le périphérique : sélectionner la valeur 1 (l'interface externe du firewall SNS créée par défaut avec l'instance ayant l'index 0).

Redémarrer le firewall

Pour prendre en compte la nouvelle interface privée, le firewall SNS EVA doit être redémarré :

1. Dans le menu **Calcul**, cliquez sur **Instances**.
2. Sélectionnez l'instance à redémarrer *(Documentation-SNS-EVA* dans l'exemple).
3. Cliquez sur **Redémarrer**.
4. Validez

Désactiver l'option Vérifier source / destination

Pour autoriser le routage transparent du trafic (qui sera filtré par le firewall SNS), il est nécessaire de désactiver cette option.

Dans la console COCKPIT 3DS OUTSCALE, menu **Calcul :**

1. Sélectionnez **Instances**.
2. Sélectionnez votre instance SNS EVA (*Documentation-SNS-EVA* dans l'exemple).
3. Cliquez sur le menu ··· situé dans la partie supérieure droite de la page de configuration des instances.
4. Sélectionnez **Attributs**.
5. Déroulez le champ **Vérifier source / destination**.
6. Cliquez sur le sélecteur pour afficher la valeur **False**.
7. Validez la configuration en cliquant sur **Fermer**.

Créer une nouvelle table de routage et une route par défaut pour le réseau privé

L'objectif est de créer une route par défaut vers l'interface privée du firewall SNS pour les machines protégées.

Créer la table de routage privée

Dans la console COCKPIT 3DS OUTSCALE, menu **Réseau / Sécurité** :

1. Sélectionnez **Route tables**.
2. Cliquez sur **Créer**.
3. Nommez votre table de routage (exemple : *Documentation-Private-Route-Table*).
4. Sélectionnez le VPC associé (*VPC Documentation* dans l'exemple).
5. Validez en cliquant sur **Créer**.

Créer la route dans la table de routage privée du VPC

1. Sélectionnez la table de routage privée précédemment créée (*Documentation-Private-Route-Table* dans l'exemple).
   Le détail de la table de routage s'affiche dans la partie inférieure de l'écran de configuration.
2. Dans le détail de la table de routage, cliquez sur **Créer une route**.
3. Dans le champ **Cible**, sélectionnez l'interface privée de votre instance SNS EVA (*Documentation-Private-Interface* dans l'exemple).
4. Cliquez sur le bouton **Toutes les IP**.
   Le champ **Destination** est automatiquement complété avec 0.0.0.0/0.
5. Validez en cliquant sur **Créer**.

Attacher cette table de routage au sous-réseau privé du VPC

1. Sélectionnez la table de routage privée précédemment créée (*Documentation-Private-Route-Table* dans l'exemple).
2. Cliquez sur **Attacher**
3. Sélectionnez le sous réseau privé du VPC (*Documentation-VPC-Private* dans l'exemple).

4. Cliquez sur **Attacher** pour valider la configuration.
   La colonne **Associations** reflète ce nouvel état (passage de 0 à 1).

Activer le firewall SNS EVA

Par défaut, le numéro de série des firewalls virtuels EVA est VMSNSX00Z0000A0.

L'activation du firewall permet d'attribuer le modèle au firewall virtuel, son numéro de série définitif, sa licence ainsi que les options souscrites.

Télécharger le kit d'initialisation

1. Connectez-vous à votre espace privé Mystormshield
2. Accédez au menu **Produit** > **Gestion des produits**.
3. Sélectionnez le modèle puis le numéro de série de votre firewall dans la liste des firewalls enregistrés.
4. Dans la fenêtre **Téléchargements**, indiquez la version de kit d'activation que vous souhaitez installer.
5. Cliquez sur le lien **Télécharger le kit d'activation**.
6. Enregistrez ce fichier sur votre poste de travail.

Changer le mot de passe du compte *admin*

1. Connectez-vous à l'interface Web d'administration du firewall : https://adresse_ip_publique_firewall/admin.
2. Renseignez le nom d'utilisateur *admin* et son mot de passe (ID de l'instance).
3. Allez dans l'onglet **Configuration** > menu **Système** > **Administrateurs** > onglet **Compte admin**.
4. Saisissez l'**Ancien mot de passe** (ID de l'instance)
5. Saisissez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.
6. Cliquez sur le bouton **Appliquer** puis sur **Sauvegarder** pour valider la modification.

Installer le kit d'initialisation sur le firewall

1. Allez dans l'onglet **Configuration** > menu **Système** > **Maintenance** > onglet **Mise à jour du système**.
2. Cliquez sur le sélecteur à droite du champ **Sélectionnez la mise à jour** et sélectionnez le kit d'activation précédemment téléchargé (fichier *.maj).
3. Cliquez sur **Mettre à jour le firewall**.
   Lors de l'installation du kit d'initialisation, le firewall redémarre.
   Cette opération dur plusieurs minutes.

Créer l'instance du serveur Web

L'objectif est de déployer une instance de serveur (distribution Linux/Ubuntu dans le cadre de la note technique), rattachée au VPC, au groupe de sécurité pour les flux entre machines protégées, au sous-réseau privé et à la clé SSH créés dans les étapes précédentes.

Créer l'instance du serveur

Dans la console COCKPIT 3DS OUTSCALE, menu **Calcul** :

1. Sélectionnez **Instances**.
2. Cliquez sur **Créer** puis **Mode expert**.
3. Nommez l'instance (exemple : *Documentation-Web-Server*) et cliquez sur **Suivant**.
4. Indiquez le type de système d'exploitation souhaité dans le champ de recherche (Ubuntu dans l'exemple) puis sélectionnez le modèle souhaité.
5. Cliquez sur **Suivant**.
6. Choisissez selon vos besoins :
   - Le type de **CPU**,
   - Le niveau de **Performance** souhaité (paramètre 3DS OUTSCALE),
   - Le nombre de **Cœurs**,
   - La quantité de **Mémoire** (Go) allouée à la machine virtuelle.
7. Cliquez sur **Suivant**.
8. Sélectionnez le **VPC** (*Documentation-VPC* dans l'exemple).
9. Sélectionnez le sous-réseau privé du VPC (*Documentation-VPC-Private* dans l'exemple).
10. Indiquez l'adresse IP du serveur.
    Cette adresse (exemple : 172.21.1.60) doit appartenir au sous-réseau sélectionné à l'étape 9.
11. Sélectionnez la zone géographique dans laquelle ce sous-réseau est disponible (*eu-west-2a* dans l'exemple).
12. Cliquez sur **Suivant**.
13. Sélectionnez le groupe de sécurité pour les flux entre machines protégées (*Documentation-Pass-All* dans l'exemple).
14. Cliquez sur **Suivant**.
15. Sélectionnez la clé SSH (*Documentation-Keypair* dans l'exemple).
16. Cliquez deux fois sur **Suivant**.
    Un résumé de l'instance vous est proposé.
17. Validez la création de l'instance en cliquant sur **Créer**.

Configurer le firewall SNS

Cette section présente la configuration minimale à réaliser pour protéger et rendre accessible le serveur Web au travers du firewall SNS.

Créer les objets réseau relatifs au serveur Web

Cette section détaille la création des objets réseau relatifs au serveur Web et qui seront utilisés dans la configuration du firewall :

- Un objet de type machine portant l'adresse IP de l'instance du serveur Web,
- Un objet de type port, distinct du SSH standard, afin d'autoriser la connexion SSH au serveur Web.

Se connecter au firewall

1. Connectez-vous à l'interface Web d'administration du firewall : https://adresse_ip_publique_firewall/admin.
2. Renseignez le nom d'utilisateur *admin* et son mot de passe.

Créer l'objet de type machine pour le serveur web

Dans l'onglet **Configuration** > menu **Objets** > **Objets réseau :**

1. Cliquez sur **Ajouter**.
2. Dans le menu de gauche, sélectionnez Machine.
3. Saisissez le **Nom de l'objet** (exemple : *webserver*).
4. Saisissez l'**Adresse IPv4** que vous avez attribuée au serveur lors de la création de l'instance du serveur Web (172.21.1.60 dans l'exemple).
5. Cliquez sur **Créer** pour valider la création de l'objet.

Créer l'objet de type port pour la redirection SSH

Dans l'onglet **Configuration** > menu **Objets** > **Objets réseau :**

1. Cliquez sur **Ajouter**.
2. Dans le menu de gauche, sélectionnez **Port**.
3. Saisissez le **Nom de l'objet** (exemple : *SSH-Webserver*).
4. Saisissez le **Port** (2222 dans l'exemple).
5. Sélectionnez le **Protocole** TCP.
6. Cliquez sur **Créer** pour valider la création de l'objet.

Créer la politique de filtrage

Allez dans l'onglet **Configuration** > menu **Politique de sécurité** > **Filtrage et NAT**.

La politique de sécurité active créée automatiquement lors du déploiement de l'instance SNS est affichée : slot *(9) Outscale*. Cette politique contient une règle qui autorise l'accès SSH au firewall.

Ajouter la règle d'accès HTTP au serveur Web

1. Sélectionnez (simple clic) la règle d'accès SSH au firewall.
2. Cliquez sur **Nouvelle règle** puis **Règle simple**.
   Une règle inactive est ajoutée immédiatement après la règle sélectionnée à l'étape 1.
3. Faites un double-clic sur la nouvelle règle inactive.
   La fenêtre d'édition de cette règle s'affiche.

Menu Général

Positionnez l'**État** à *On*.

Menu Action

1. Sélectionnez l'onglet **Général.**
2. Positionnez l'**Action** à *passer*.

Menu Source

1. Sélectionnez l'onglet **Général.**
2. Dans le champ **Interface d'entrée**, sélectionnez l'interface *out*.

Menu Destination

1. Cliquez sur l'onglet **Général.**
2. Cliquez sur le menu **Ajouter** du champ **Machines destinations**.
3. Tapez *firewall* pour filtrer les machines puis sélectionnez l'objet *Firewall_out*.
4. Sélectionnez l'onglet **Configuration avancée.**
5. Dans le champ **NAT sur la destination** > **Destination**, tapez *web* pour filtrer les machines puis sélectionnez l'objet *webserver*.

Menu Port / Protocole.

1. Dans le champ **Port destination**, cliquez sur **Ajouter**.
2. Tapez *http* pour filtrer les ports puis sélectionnez l'objet *http*.
3. Validez la règle en cliquant sur **OK**.

Ajouter la règle d'accès en SSH au serveur Web

1. Sélectionnez (simple clic) la règle d'accès HTTP au serveur Web précédemment créée.
2. Cliquez sur **Nouvelle règle** puis **Règle simple**.
   Une règle inactive est ajoutée immédiatement après la règle sélectionnée à l'étape 1.
3. Faites un double-clic sur la nouvelle règle inactive.
   La fenêtre d'édition de cette règle s'affiche.

Menu Général

Positionnez l'**État** à *On*.

Menu Action

1. Sélectionnez l'onglet **Général.**
2. Positionnez l'**Action** à *passer*.

Menu Source

1. Sélectionnez l'onglet **Général.**
2. Dans le champ **Interface d'entrée**, sélectionnez l'interface *out*.

Menu Destination

1. Cliquez sur l'onglet **Général.**
2. Cliquez sur le menu **Ajouter** du champ **Machines destinations**.
3. Tapez *firewall* pour filtrer les machines puis sélectionnez l'objet *Firewall_out*.
4. Sélectionnez l'onglet **Configuration avancée.**
5. Dans le champ **NAT sur la destination** > **Destination**, tapez *web* pour filtrer les machines puis sélectionnez l'objet *webserver*.

Menu Port / Protocole.

1. Dans le champ **Port destination**, cliquez sur **Ajouter**.
2. Tapez *ssh* pour filtrer les ports puis sélectionnez l'objet *SSH-Webserver*
3. Dans le champ Port destination translaté, sélectionnez l'objet *ssh*.
4. Validez la règle en cliquant sur **OK**.

Ajouter la règle d'accès à Internet pour les machines protégées

1. Sélectionnez (simple clic) la règle de redirection SSH vers le serveur Web précédemment créée.
2. Cliquez sur **Nouvelle règle** puis **Règle simple**.
   Une règle inactive est ajoutée immédiatement après la règle sélectionnée à l'étape 1.
3. Faites un double-clic sur la nouvelle règle inactive.
   La fenêtre d'édition de cette règle s'affiche.

Menu Général

Positionnez l'**État** à *On*.

Menu Action

1. Sélectionnez l'onglet **Général.**
2. Positionnez l'**Action** à *passer*.

Menu Source

1. Sélectionnez l'onglet **Général.**
2. Dans le champ **Interface d'entrée**, sélectionnez l'interface *in*.

Menu Destination

1. Cliquez sur l'onglet **Général.**
2. Cliquez sur le menu **Ajouter** du champ **Machines destinations**.
3. Tapez *inter* pour filtrer les machines puis sélectionnez l'objet *Internet*.
4. Validez la règle en cliquant sur **OK**.

Ajouter des séparateurs de règles (optionnel)

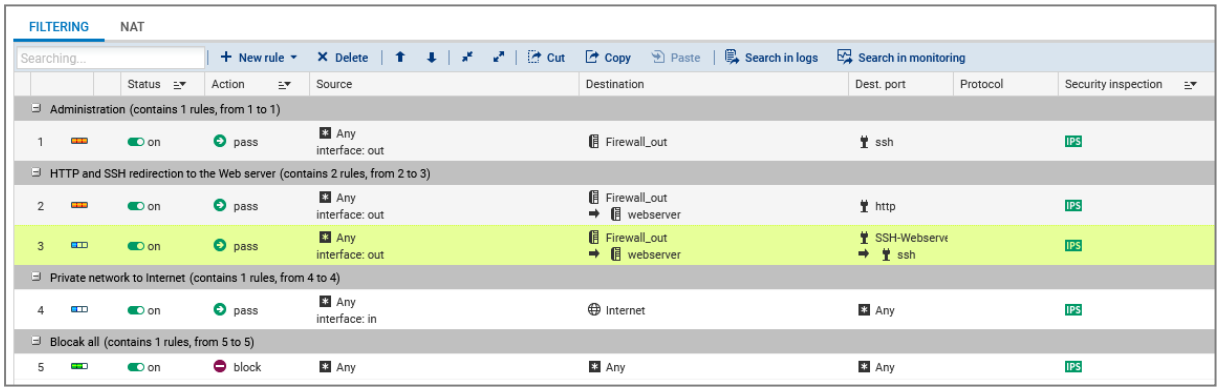
Pour rendre la politique de filtrage plus lisible, il peut être utile d'ajouter des séparateurs de règle.

1. Sélectionnez (simple clic) la règle devant laquelle vous souhaitez insérer un séparateur.
2. Cliquez sur **Nouvelle règle** puis **Séparateur - regroupement de règles**.
   Un séparateur de règles est ajouté immédiatement devant la règle sélectionnée à l'étape 1.
3. Faites un double-clic sur le séparateur.
4. Saisissez le texte de votre choix.

EXEMPLES
Dans la configuration proposée, 4 séparateurs peuvent être ajoutés. Par exemple :

- Administration,
- Redirection HTTP et SSH vers le serveur Web,
- Réseau privé vers Internet,
- *Block all*.

La politique de filtrage créée prend donc la forme suivante :



Créer la politique de NAT

Une règle de NAT est nécessaire pour les connexions des machines protégées vers Internet.

Créer la règle de NAT

1. Allez dans l'onglet **Configuration** > menu **Politique de sécurité** > **Filtrage et NAT** > onglet **NAT**.
2. Cliquez sur **Nouvelle règle** puis sur **Règle simple**.
   Une règle inactive est ajoutée immédiatement après la règle sélectionnée à l'étape 1.
3. Faites un double-clic sur la nouvelle règle inactive.
   La fenêtre d'édition de cette règle s'affiche.

Menu Général

Positionnez l'**État** à *On*.

Menu Source originale

1. Sélectionnez l'onglet **Général.**
2. Dans le champ **Interface d'entrée**, sélectionnez l'interface *in*.

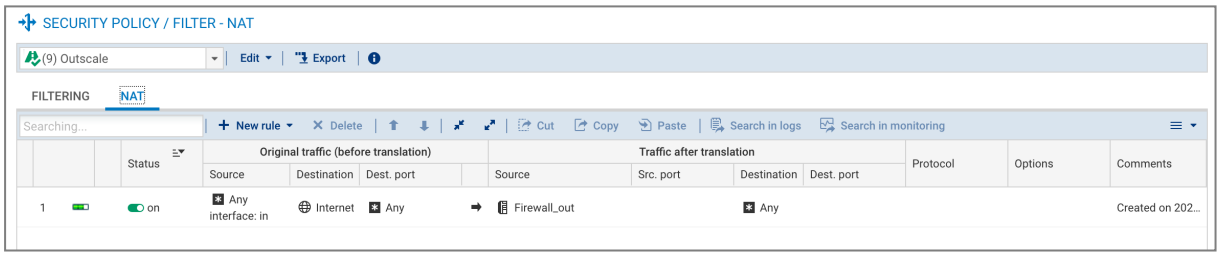
Menu Destination originale

1. Cliquez sur l'onglet **Général.**
2. Cliquez sur le menu **Ajouter** du champ **Machines destinations**.
3. Tapez *inter* pour filtrer les machines puis sélectionnez l'objet *Internet*.

Menu Source translatée

1. Cliquez sur l'onglet **Général.**
2. Dans le champ **Machine source translatée**, tapez *firew* pour filtrer les machines et sélectionnez *Firewall_out*.
3. Validez la règle en cliquant sur **OK**.
4. Cliquez sur **Appliquer** puis sur **Oui, activer la politique** pour prendre en compte les modifications.

La politique de NAT créée prend donc la forme suivante :



Installer le service Serveur Web

Cette section décrit comment se connecter au serveur Web pour y installer le service Apache.

Le port de connexion utilisé est le port de redirection SSH (TCP/2222 dans l'exemple) ajouté dans le groupe de sécurité pour les flux depuis l'extérieur.

Se connecter en SSH au serveur Web

1. Lancez une fenêtre de commande *Powershell* (poste Microsoft Windows) ou une fenêtre *shell* (poste Linux).
2. Utilisez la commande *cd* pour vous placer dans le répertoire contenant la clé SSH téléchargée lors de sa création.

EXEMPLE
`cd c:\Temp` (poste Microsoft Windows)
`cd \home\documentation` (poste Linux)

3. Le nom d'utilisateur prédéfini pour se connecter à l'instance de serveur Web est *outscale*. Tapez la commande :

```
ssh -i nom_fichier_clé_SSH -p port_redirection_ssh outscale@adresse_ip_publique
```

EXEMPLE
```
ssh -i Documentation-keypair.rsa -p 2222 outscale@1.2.3.4
```

Vous êtes connecté au serveur.

Installer le service Apache sur le serveur Web (cas d'un serveur Linux/Ubuntu)

1. Tapez la commande `sudo apt-get install apache2.`
2. Validez l'installation en tapant *y*.
Les paquets nécessaires au fonctionnement du serveur Apache sont installés.

Tester l'accès au serveur Web

Depuis un poste client :

1. Ouvrez une navigateur Internet.
2. Tapez l'URL `http://adresse_ip_publique_firewall`.
   La page d'accueil du serveur Web doit s'afficher.

Pour aller plus loin

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

STORMSHIELD

documentation@stormshield.eu