NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

VMWARE NSX : FIREWALL SNS DANS LE RÔLE D'UN ROUTEUR PÉRIPHÉRIQUE

Produits concernés : SNS 1 et versions supérieures

Date : 06 Février 2019

Référence : sns-fr_VMWare-NSX-SNS-routeur-périphérique_note-technique

Table des matières

Avant de commencer 3
Topologie 4
Intégrer un firewall SNS comme routeur périphérique 5
Créer les objets réseau 5
Définir les routes statiques sur le firewall 6
Paramétrer les règles de filtrage sur le firewall 7
Autoriser l'accès des réseaux virtuels à Internet 7
Autoriser l'accès des réseaux externes au serveur Web 7
Interdire tous les autres flux 8
Paramétrer les règles de NAT sur le firewall 8
Masquer les réseaux virtuels lors de leur accès à Internet 8
Rediriger les requêtes HTTP/HTTPS externes vers le serveur Web 9
Tester la configuration 9

Avant de commencer

VMware NSX Data Center est une plate-forme de virtualisation de réseau destinée au Software-Defined Data Center (SDDC) qui fournit l'intégralité des fonctions réseau et de sécurité sous forme logicielle, et qui est isolée de l'infrastructure physique sous-jacente.

NSX Data Center permet ainsi la mise en œuvre d'un réseau Cloud virtuel en assurant une connectivité de bout en bout avec les applications et les données, où qu'elles se trouvent.

L'intégration d'un firewall SNS dans une architecture NSX peut alors apporter des fonctionnalités avancées de filtrage et de sécurité pour protéger ces données et applications.

Pour rappel, les différentes briques d'un environnement vSphere sont les suivantes :

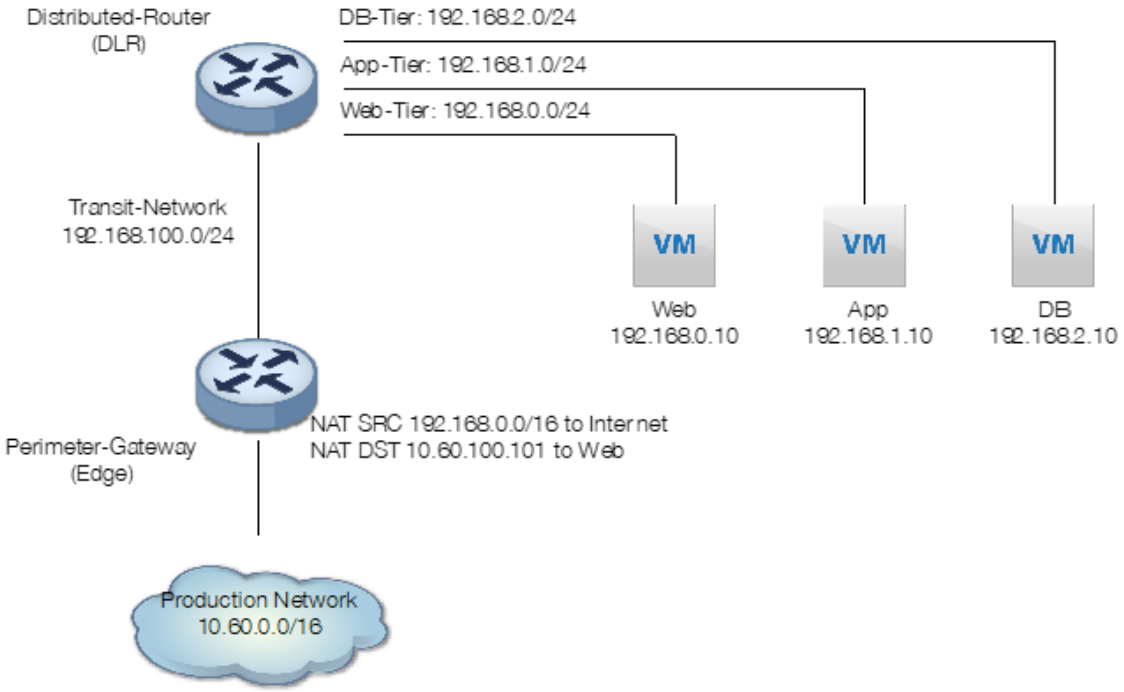
- ESXi : hyperviseur sur plate-forme matérielle (bare metal),
- vCenter : gestionnaire centralisé de machines virtuelles,
- vSphere : connexion vCenter - hyperviseur ESXi,
- vSphere Enterprise : version de vSphere incluant les Distributed Virtual Switches (DVS) et le Distributed Resource Scheduler (DRS).

Notez que ce document n'aborde pas l'installation de firewall à partir du fichier OVA téléchargeable depuis votre **espace client**. Vous pouvez consulter la procédure d'installation dans le document *Stormshield Network Virtual Firewalls - Guide d'installation*.

Topologie

L'application Web de cet exemple repose sur trois serveurs virtuels :

- Un serveur Web,
- Un serveur applicatif,
- Un serveur de base de données.



Chaque serveur est connecté à son propre réseau virtuel.

Le Distributed Logical Router (Distributed-Router) connecte ces trois réseaux virtuels entre eux, et le routeur périmétrique (Perimeter-Gateway) connecte le réseau physique à ces trois réseaux virtuels par le biais d'un réseau virtuel de transit (Transit-Network).

Le routeur périmétrique réalise également de la translation d'adresses :

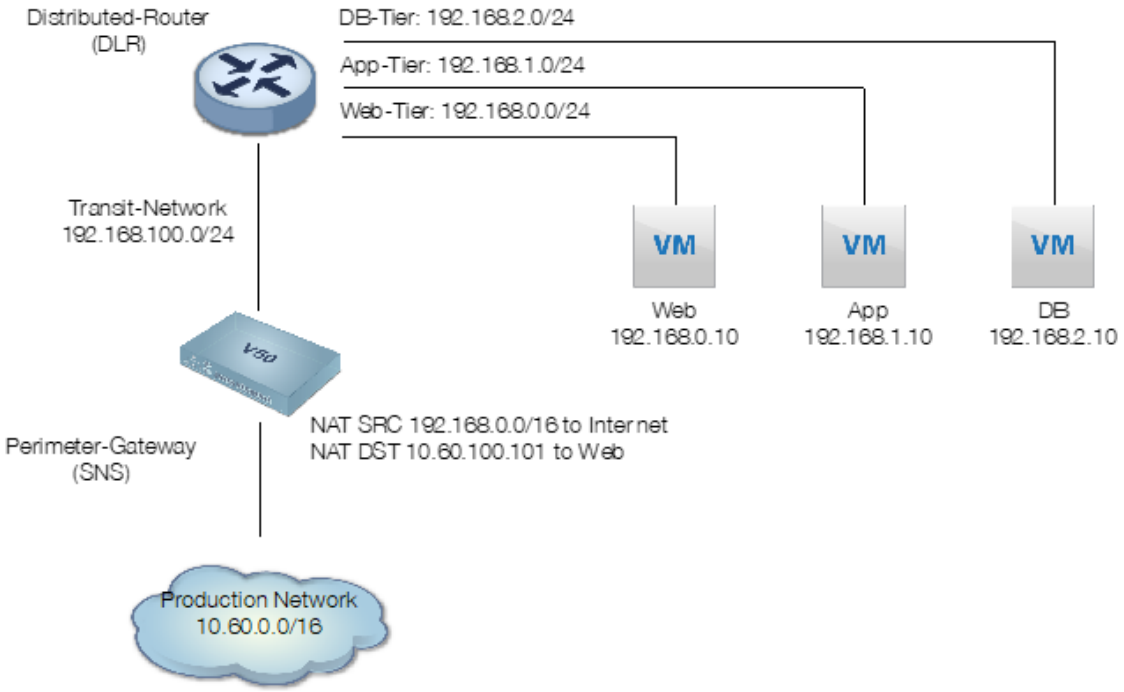
- NAT source pour autoriser les serveurs à communiquer avec Internet,
- NAT destination pour rediriger les requêtes à destination d'une adresse publique vers le serveur Web.

Dans cette architecture, les règles du firewall distribué intégré à NSX (routeur périmétrique) prennent la forme suivante :

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
▼	Web Application (Rule 1 - 2)						
1	web src NAT ip	1006	any	Web NAT	HTTP HTTPS	Allow	Distributed Firewall
2	Web Tier to App & DB Tier	1005	Web-Tier	App-Tier DB-Tier	any	Allow	Distributed Firewall

Intégrer un firewall SNS comme routeur périphérique

Le firewall SNS peut jouer avantageusement le rôle du routeur périphérique en offrant des fonctionnalités avancées de filtrage :



La mise en place de cette architecture nécessite un firewall Virtuel SNS déployé sur la plate-forme avec deux interfaces sorties du bridge créé par défaut :

- Une interface protégée avec une adresse dans le réseau **Transit-Network** (interface *in* renommée en **transit** et portant l'adresse 192.168.100.1 dans ce document),
- Une interface non protégée avec une adresse dans le réseau nommé **Production Network** (interface *out* portant l'adresse 10.60.100.100 dans ce document).

Les opérations de paramétrage du firewall détaillées dans cette note technique sont les suivantes :

- Créer les objets réseau nécessaires sur le firewall,
- Définir les routes statiques sur le firewall,
- Paramétrer les règles de filtrage sur le firewall,
- Paramétrer les règles de NAT sur le firewall.

Créer les objets réseau

Vous devez créer les objets suivants :

Nom de l'objet	Adresse IPv4 dans cet exemple	Rôle
Transit-Router	192.168.100.2	Routeur distribué (DLR)

Nom de l'objet	Adresse IPv4 dans cet exemple	Rôle
Web-NAT	10.60.100.101	Adresse IP du serveur Web visible depuis les réseaux externes
Web-Srv	192.168.0.10	Adresse IP réelle du serveur Web
Web-Tier	192.168.0.0/24	Réseau dédié aux serveurs Web
App-Tier	192.168.1.0/24	Réseau dédié aux serveurs d'application
DB-Tier	192.168.2.0/24	Réseau dédié aux serveurs de bases de données

Objets **Transit-Router**, **Web-NAT** et **Web-Srv**

1. Connectez-vous à l'interface Web d'administration du firewall en tant qu'administrateur.
2. Dans le menu **Objets** > **Objets réseau**, cliquez sur **Ajouter**.
3. Dans la colonne de gauche, sélectionnez **Machine** et renseignez les champs obligatoires pour l'objet **Transit-Router** en prenant exemple sur le tableau ci-dessus :
   - **Nom de l'objet**,
   - **Adresse IPv4**.
4. Cliquez sur **Créer et dupliquer**.
5. Répétez les étapes 3 et 4 pour l'objet **Web-NAT**.
6. Répétez l'étape 3 pour l'objet **Web-Srv**.
7. Cliquez sur **Créer**.

Objets **Web-Tier**, **App-Tier** et **DB-Tier**

1. Dans le menu **Objets** > **Objets réseau**, cliquez sur **Ajouter**.
2. Dans la colonne de gauche, sélectionnez **Réseau** et renseignez les champs obligatoires pour l'objet **Web-Tier** en prenant exemple sur le tableau ci-dessus :
   - **Nom de l'objet**,
   - **Adresse IPv4**.
3. Cliquez sur **Créer et dupliquer**.
4. Répétez les étapes 3 et 4 pour l'objet **App-Tier**.
5. Répétez l'étape 3 pour l'objet **DB-Tier**.
6. Cliquez sur **Créer**.

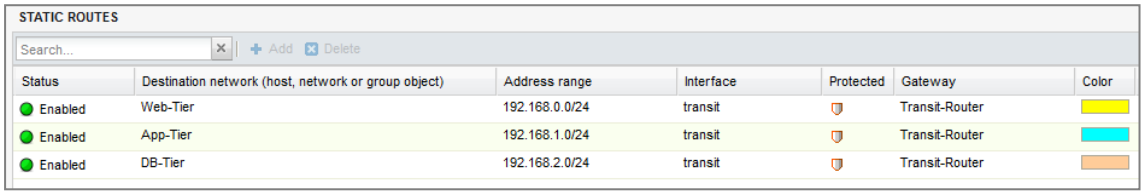
Définir les routes statiques sur le firewall

Dans le menu **Réseau** > **Routage** > onglet **Routes statiques** :

1. Cliquez sur **Ajouter**.
2. Cliquez dans la colonne **Réseau de destination (objet machine, réseau ou groupe)** de la nouvelle ligne.
3. Sélectionnez l'objet **Web-Tier**.
4. Cliquez dans la colonne **Interface.**
5. Sélectionnez l'interface **transit**.
6. Cliquez dans la colonne **Passerelle**.
7. Sélectionnez l'objet **Transit-Router**.

8. Double-cliquez sur la colonne **État** pour activer la route.
9. Renouvelez les étapes 1 à 8 pour créer la route vers le réseau **App-Tier**.
10. Renouvelez les étapes 1 à 8 pour créer la route vers le réseau **DB-Tier**.
11. Cliquez sur **Appliquer** pour valider la configuration.

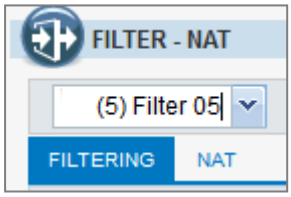
Les routes statiques du firewall prennent donc la forme suivante :



Paramétrer les règles de filtrage sur le firewall

Pour définir les différentes règles de filtrage nécessaires :

1. Placez-vous dans le menu **Politique de sécurité** > **Filtrage et NAT** > onglet **Filtrage.**
2. Sélectionnez la politique de sécurité souhaitée à l'aide de la liste déroulante :



Autoriser l'accès des réseaux virtuels à Internet

1. Cliquez sur **Nouvelle règle**.
2. Sélectionnez **Règle simple**.
3. Double cliquez sur la règle nouvellement ajoutée.
4. Dans le menu **Général**, positionnez l'**État** à *On*.
5. Dans le menu **Action** > onglet **Général**, positionnez l'**Action** à *passer*.
   Vous pouvez également choisir la valeur *tracer (journal de filtrage)* pour le champ **Niveau de trace**.
6. Dans le menu **Source** > onglet **Général** cliquez sur **Ajouter** et sélectionnez l'objet réseau *App-Tier*.
7. Renouvelez l'opération pour ajouter les objets **Web-Tier** et **DB-Tier**.
8. Pour le champ **Interface d'entrée**, sélectionnez l'interface transit.
9. Dans le menu **Destination** > onglet **Configuration avancée** sélectionnez l'interface *out* comme **Interface de sortie**.
10. Validez la règle en cliquant sur le bouton **OK**.

Autoriser l'accès des réseaux externes au serveur Web

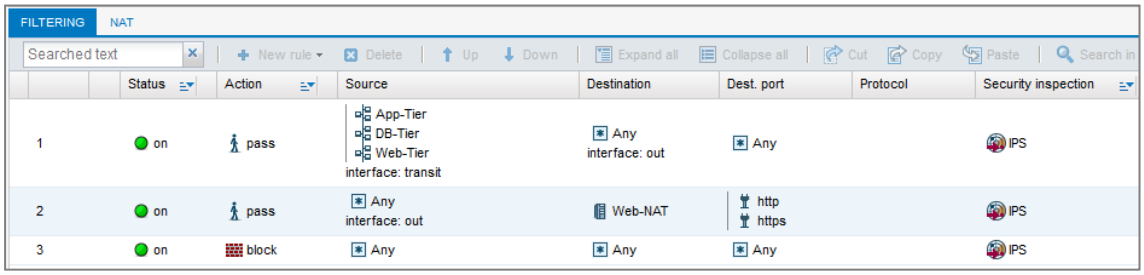
1. Cliquez sur **Nouvelle règle**.
2. Sélectionnez **Règle simple**.

3. Double cliquez sur la règle nouvellement ajoutée.
4. Dans le menu **Général**, positionnez l'**État** à *On*.
5. Dans le menu **Action** > onglet **Général**, positionnez l'**Action** à *passer*.
   Vous pouvez également choisir la valeur *tracer (journal de filtrage)* pour le champ **Niveau de trace**.
6. Dans le menu **Source** > onglet **Général**, sélectionnez l'interface *out* comme **Interface d'entrée**.
7. Dans le menu **Destination** > onglet **Général**, cliquez sur **Ajouter** et sélectionnez l'objet réseau *Web-NAT*.
8. Dans le menu **Port / Protocole** > partie **Port**, cliquez sur **Ajouter** et sélectionnez l'objet *http*.
9. Renouvelez l'opération pour ajouter l'objet *https*.
10. Validez la règle en cliquant sur le bouton **OK**.

Interdire tous les autres flux

1. Cliquez sur **Nouvelle règle**.
2. Sélectionnez **Règle simple**.
3. Double cliquez sur la règle nouvellement ajoutée.
4. Dans le menu **Général**, positionnez l'**État** à *On*.
5. Validez la règle en cliquant sur le bouton **OK**.
   La règle ainsi ajoutée bloque tous les autres flux.
   Assurez-vous que cette règle est bien en dernière position de votre politique de filtrage (au besoin vous pouvez la sélectionner et la déplacer à l'aide des boutons **Monter** et **Descendre**).

La politique de filtrage sur le firewall périphérique prend donc la forme suivante :



Paramétrer les règles de NAT sur le firewall

Pour définir les différentes règles de NAT :

1. Placez-vous dans le menu **Politique de sécurité** > **Filtrage et NAT.**
2. Sélectionnez la politique de sécurité contenant les règles de filtrage précédemment ajoutées.
3. Cliquez sur l'onglet **NAT.**

Masquer les réseaux virtuels lors de leur accès à Internet

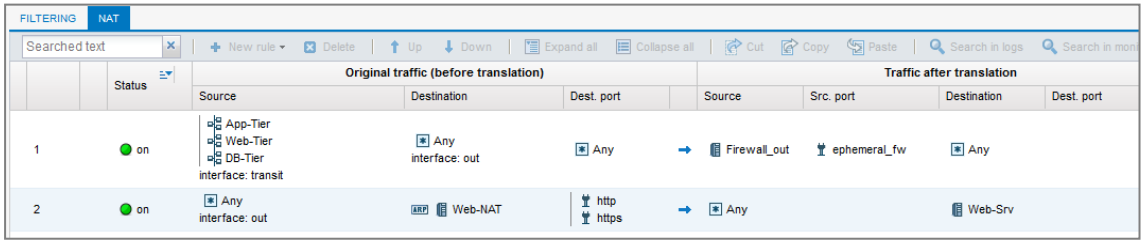
1. Cliquez sur **Nouvelle règle**.
2. Sélectionnez **Règle de partage d'adresse source (masquerading)**.
3. Double cliquez sur la règle nouvellement ajoutée.

4. Dans le menu **Général**, positionnez l'**État** à *On*.
5. Dans le menu **Source originale** > onglet **Général**, cliquez sur **Ajouter** et sélectionnez l'objet réseau **App-Tier**.
6. Renouvelez l'opération pour ajouter les objets **Web-Tier** et **DB-Tier**.
7. Pour le champ **Interface d'entrée**, sélectionnez l'interface **transit**.
8. Dans le menu **Destination originale** > onglet **Configuration avancée**, sélectionnez l'interface **out** comme **Interface de sortie**.
9. Dans le menu **Source translatée** > onglet **Général**, sélectionnez l'objet réseau **Firewall_out** pour le champ **Machine source translatée**.
10. Validez la règle en cliquant sur le bouton **OK**.

Rediriger les requêtes HTTP/HTTPS externes vers le serveur Web

1. Cliquez sur **Nouvelle règle**.
2. Sélectionnez **Règle simple**.
3. Double cliquez sur la règle nouvellement ajoutée.
4. Dans le menu **Général**, positionnez l'**État** à *On*.
5. Dans le menu **Source originale** > onglet **Général** > champ **Interface d'entrée**, sélectionnez l'interface **out**.
6. Dans le menu **Destination originale** > onglet **Général** > partie **Machines destinations**, cliquez sur **Ajouter** et sélectionnez l'objet réseau **Web-NAT**.
7. Dans la partie **Port destination**, cliquez sur **Ajouter** et sélectionnez l'objet **http**.
8. Renouvelez l'opération pour ajouter l'objet **https**.
9. Dans l'onglet **Configuration avancée**, cochez la case **Publication ARP**.
10. Dans le menu **Destination translatée** > onglet **Général** > champ **Machine destination translatée**, cliquez sur **Ajouter** et sélectionnez l'objet **Web-Srv**.
11. Validez la règle en cliquant sur le bouton **OK**.

La politique de NAT sur le firewall périphérique prend donc la forme suivante :



Activez la politique de filtrage et NAT en cliquant sur le bouton **Sauvegarder et activer**.

Tester la configuration

Depuis une machine située sur le réseau de production, établissez une connexion Web vers la page d'accueil de l'application.

Lorsque la connexion est établie, les traces correspondantes ainsi que les opérations de NAT peuvent être visualisées au sein de l'interface Web d'administration du firewall (module **Logs -**

Journaux d'Audit > **Vues** > **Trafic réseau** et module **Logs - Journaux d'Audit** > **Logs - Journaux** > **Connexions réseaux**).

documentation@stormshield.eu