

Fiche savoirs technologiques : Mise en place du plan d'adressage réseau du Lab

Configuration des interfaces réseau

Dans une configuration usine :

- la **première interface** du pare-feu SNS est nommée **OUT** ou **WAN**,
- la seconde **IN**
- et le reste des interfaces **DMZx**.

L'interface « OUT » est une **interface externe** utilisée pour connecter le pare-feu SNS à internet (WAN) et le reste des interfaces sont internes et servent principalement à connecter le pare-feu SNS à des réseaux locaux.

La distinction interface interne/externe permet de se protéger contre les attaques d'usurpation d'adresse IP.

Pour accéder à l'interface d'administration du pare-feu SNS, il faut connecter votre machine sur une interface interne sous peine d'être détecté comme tentative d'intrusion qui nécessite le redémarrage du firewall.

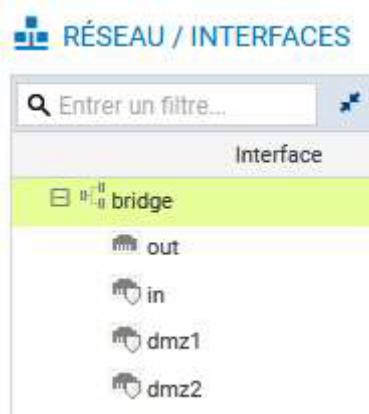
Vous allez configurer votre pare-feu SNS selon les paramètres de l'architecture globale présentée dans l'activité précédente (interfaces IN, OUT et DMZ1) en utilisant le pare-feu SNS en mode **routeur**.

- @Interface **OUT** 192.36.253.x0 /24 qui correspond au premier port (WAN) ;
- @Interface **IN** 192.168.x.254 /24 qui correspond au deuxième port (port LAN N°1) ;
- @Interface **DMZ1** 172.16.x.254 /24 qui correspond au port DMZ.

La passerelle par défaut de votre pare-feu SNS est la passerelle du réseau NatNetwork de VirtualBox @192.36.253.1.

La configuration du SNS se fera depuis le client Linux Graphique connecté à l'interface **IN**.

[La configuration des interfaces](#) s'effectue dans le menu **Configuration / Réseau / Interfaces** en faisant sortir les interfaces Ethernet de l'interface bridge.



- Choisir une première interface (par exemple **IN**) pour la sortir du bridge ou la configurer avec une IP fixe ou dynamique (les manipulations sont identiques).

CONFIGURATION DE IN

CONFIGURATION GÉNÉRALE **CONFIGURATION AVANCÉE**

État

Paramètres généraux

Nom:	in
Commentaire:	
Cette interface est:	<input checked="" type="radio"/> Interne (protégée) <input type="radio"/> Externe (publique)

Plan d'adressage

Adressage:	<input type="radio"/> Plan d'adressage hérité du bridge <input checked="" type="radio"/> Dynamique / Statique
Adresse IPv4:	<input type="radio"/> IP dynamique (obtenue par DHCP) <input type="radio"/> IP fixe (statique)

▼ Configuration DHCP avancée

Si l'interface était membre d'un bridge, la configuration est légèrement différente pour la zone **Plan d'adressage** :

Plan d'adressage

Adressage:	<input checked="" type="radio"/> Plan d'adressage hérité du bridge <input type="radio"/> Dynamique / Statique
Bridge:	bridge

- Le cas échéant, cliquez dans la zone **Plan d'adressage** sur **Dynamique/Statique**
- Cliquez **Ip fixe (statique)**, un tableau apparaît :

Plan d'adressage

Adressage:	<input type="radio"/> Plan d'adressage hérité du bridge <input checked="" type="radio"/> Dynamique / Statique
Adresse IPv4:	<input type="radio"/> IP dynamique (obtenue par DHCP) <input checked="" type="radio"/> IP fixe (statique)

+ Ajouter	X Supprimer
Adresse / Masque	Commentaire

• Cliquez sur **+Ajouter** et dans la zone Adresse / Masque saisissez **l'adresse IP de l'interface IN** 192.168.x.254 puis le masque en CIDR /24 ou en notation décimale pointée : 255.255.255.0

Plan d'adressage

Adressage:	<input type="radio"/> Plan d'adressage hérité du bridge <input checked="" type="radio"/> Dynamique / Statique
Adresse IPv4:	<input type="radio"/> IP dynamique (obtenue par DHCP) <input checked="" type="radio"/> IP fixe (statique)

+ Ajouter	X Supprimer
Adresse / Masque	Commentaire

192.168.1.254/24	
------------------	--

- Cliquez le bouton **Appliquer** puis **Sauvegarder** et à nouveau **Sauvegarder**. Un message de reconnexion peut s'afficher, le cas échéant reconnectez-vous.
- Procédez de manière identique pour les deux autres interfaces à configurer.

Route par défaut

La configuration de la passerelle par défaut de votre pare-feu SNS doit pointer la passerelle du réseau NatNetwork de VirtualBox :

192.36.253.1

- Cliquez sur **Configuration / Réseau / Routage** onglet **Routes statiques IPv4** :

Passerelle par défaut (routeur):

CRÉER UN OBJET

<input checked="" type="checkbox"/> Machine	Nom de l'objet: <input type="text" value="FWOUT_Siege"/>
<input type="checkbox"/> FQDN Nom DNS (FQDN)	Adresse IPv4: <input type="text" value="192.36.253.1"/>
<input type="checkbox"/> Réseau	Adresse MAC: <input type="text" value="01:23:45:67:89:ab (Facultatif)"/>
<input type="checkbox"/> Plage d'adresses IP	
<input checked="" type="checkbox"/> Routeur	Résolution
<input type="checkbox"/> Groupe	<input checked="" type="radio"/> Aucune (IP statique) <input type="radio"/> Automatique
<input type="checkbox"/> Protocole IP	Commentaire:
<input type="checkbox"/> Port	
<input type="checkbox"/> Groupe de ports	

===== Mise en oeuvre de la traduction d'adresses pour l'accès à Internet (NAT/PAT) ===== Pour le LAB, nous considérons le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n'est tolérée. De plus, la passerelle du réseau NatNetWork est connecté à internet via une interface autre que celles utilisées dans l'architecture du LAB. * Ouvrez le menu **Configuration / Politique de sécurité / Filtrage et NAT** :

Rechercher...	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
Remote Management: Go to System - Configuration to setup the web administration application access (contient 2 règles, de 1 à 2)	on	passer	Any	firewall_all	firewall_srv	IPS		Admin from everywhere
Default policy (contient 1 règles, de 3 à 3)	on	passer	Any	firewall_all	Any	icmp (requête Ech)	IPS	Allow Ping from everywhere
	on	bloquer	Any	Any	Any	IPS		Block all

Dans les pare-feux SNS, les règles de filtrage et de NAT (traduction d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par une icône. La politique de sécurité active en configuration usine est **(1) Block all** : elle n'autorise que le ping des interfaces du firewall et l'accès en https à l'administration du boîtier. Une politique implicite **Block all** est également configurée sur le pare-feu SNS.

Pour réaliser les activités, vous allez choisir une politique plus permissive que vous durcirez progressivement.

Étape 1 : Copiez la politique de filtrage/NAT (10) Pass all vers une autre politique vide en la renommant AgenceX (remplacez X par la lettre de votre entreprise). Ensuite, activez cette politique. La démarche est présentée ci-après. </WRAP> * Dans la liste déroulante des politiques de sécurité, choisissez (10) Pass all. Cette politique laisse explicitement passer tous les flux.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(10) Pass all | Editer | Exporter |

Filtrage NAT

Rechercher...	+ Nouvelle règle	Supprimer	↑ ↓ ↗ ↘	Couper	Copier	Coller	Chercher dans les logs
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
1	on	passer	Any	Any	Any	IPS	

* Cliquez sur **Editer** puis **copier vers** et choisir une politique vide (par exemple **Filter 05**).

APPLIQUER ET COPIER LE PROFIL

Toutes vos modifications seront sauvegardées puis copiées de(10) Pass all \vers (5) Filter 05.

ANNULER SAUVEGARDER LES MODIFICATIONS ET COPIER VERS (5) FILTER 05

* Cliquez **Sauvegarder les modifications...** * Dans la liste déroulante des politiques de sécurité, choisissez la politique **(05) Pass all**. * Cliquez **Éditer** puis **Renommer** et renommez-là en **AgenceX**, puis **Mettre à jour**. * Cliquez le bouton **Appliquer** puis **Activer la politique AgenceX**.

ACTIVER LA POLITIQUE SÉLECTIONNÉE?

Souhaitez-vous activer la politique sélectionnée ?
Attention, cette activation recharge les configurations locales et globales.

ANNULER ACTIVER LA POLITIQUE ENTREPRISE

La politique **AgenceX** est activée :

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(5) AgenceA | Editer | Exporter |

Filtrage NAT

Rechercher...	+ Nouvelle règle	Supprimer	↑ ↓ ↗ ↘	Couper	Copier	Coller	Chercher dans les logs
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
1	on	passer	Any	Any	Any	IPS	

Étape 2 : Ajoutez une règle de NAT afin que les machines de votre réseau interne (**Networkin**) puissent accéder au réseau externe (**FirewallOut**) sans que leur IP ne soit visible (DNAT).

Testez l'accès au réseau externe et l'accès à Internet depuis votre poste sur le réseau interne **IN** de votre agence.

La démarche est présentée ci-après.

La règle de **NAT dynamique** est créée avec le bouton **Nouvelle règle / règle de partage d'adresse source (masquerading)** qui ajoute automatiquement la plage de ports ephemeralfw au niveau du port source dans le trafic après traduction ce qui génère aléatoirement un numéro de port pour chaque nouvelle connexion et la rend moins prédictible. * Dans votre politique (5) AgenceX, sélectionnez l'onglet **NAT** puis **Nouvelle règle / règle de partage d'adresse source (masquerading)**

Filtrage NAT

Rechercher...	+ Nouvelle règle	Supprimer	↑ ↓ ↗ ↘	Couper	Copier	Coller	Chercher dans les logs			
	État	Trafic original (avant translation)	Trafic après translation							
		Source	Destinat...	Port dest.	Source	Port src.	Destination	Port d...	Protocole	Options
1	off	Any	Any	Any	Any	ephemeral_fw	Any	Any		

Une nouvelle règle non activée apparaît avec des valeurs par défaut any, any. Dans la section **Traffic après translation**, le port source sera traduit par un numéro de port choisi aléatoirement dans la plage **ephemeral_fw**. La configuration du **Traffic original (avant translation)** permet de renseigner les valeurs des paramètres avant traduction (par défaut any, any) : * **Source Originale** permet de définir l'adresse IP d'un hôte ou du réseau source. * **Destination Originale** permet de définir l'adresse IP d'un hôte ou du réseau destination. La configuration du **Traffic après translation** permet de renseigner les nouvelles valeurs des paramètres après traduction (par défaut any, any) : * **Source translatée** définit

l'adresse IP ou le réseau source et le port source vus de l'extérieur. * **Destination traduite** définit l'adresse IP ou le réseau destination et Port destination traduite le port de destination. Voici le détail de chaque élément de la configuration de la règle. * Double-cliquez sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée. * Cliquez l'onglet à gauche **Source Originale**.

EDITION DE LA RÈGLE N° 1

Général
Source originale
Destination originale
Source traduite
Destination traduite
Protocole
Options

SOURCE AVANT TRANSLATION (ORIGINALE)

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Utilisateur: Rechercher...
 Machines sources: Ajouter Supprimer
 Network_internals

* Cliquez sur Any et avec la flèche choisir Networkinternals ; dans l'onglet Configuration avancée, laissez Any pour le port de destination. * Cliquez l'onglet du menu de gauche Destination Originale. * Cliquez sur Any et avec la flèche choisir Internet ; laissez Any pour le port de destination.

EDITION DE LA RÈGLE N° 1

Général
Source originale
Destination originale
Source traduite
Destination traduite
Protocole
Options

DESTINATION AVANT TRANSLATION (ORIGINALE)

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Machines destinations: Ajouter Supprimer
 Internet

Port destination: Ajouter Supprimer
 Any

Attention : si vous laissez Any, plutôt qu'Internet qui désigne tous les réseaux sauf ceux internes au pare-feu SNS, le pare-feu SNS bloquera les flux d'administration (en ssh et en https).

En effet, les flux d'administration seront de fait également natés vers l'interface OUT qui l'interprétera comme une tentative d'intrusion et les bloquera.

Vous pouvez sécuriser davantage cette règle en choisissant l'interface de sortie.

* Cliquez l'onglet Configuration avancée et sélectionnez out dans Interface de sortie.

EDITION DE LA RÈGLE N° 1

Général
Source originale
Destination originale
Source traduite
Destination traduite
Protocole
Options

DESTINATION AVANT TRANSLATION (ORIGINALE)

GÉNÉRAL CONFIGURATION AVANCÉE

Configuration avancée

Interface de sortie:
 Publication ARP sur la destination externe (publique)

* Cliquez l'onglet Source traduite et sélectionnez FirewallOut dans Machine source traduite. * Dans Port source traduit, laissez ephemeralfw et cochez choisir aléatoirement le port source traduit.

EDITION DE LA RÈGLE N° 1

SOURCE APRÈS TRANSLATION

GÉNÉRAL **CONFIGURATION AVANCÉE**

Général

Machine source traduite: Firewall_out
 ephemeral_fw
 choisir aléatoirement le port source traduit

* Cliquez l'onglet du menu de gauche **Protocole**, cela permet de définir le type de protocole : applicatif, IP ou Ethernet, laisser **Détection automatique du protocole (par défaut)**

EDITION DE LA RÈGLE N° 1

PROTOCOLE

Protocole

Type de protocole:

 Détection automatique du protocole (par défaut)
 Protocole applicatif
 Protocole IP
 Protocole Ethernet

* Cliquez sur l'onglet du menu de gauche **Options** ; cela permet de tracer le trafic qui correspond à la règle de traduction dans le journal de connexions. Laissez **standard**.

EDITION DE LA RÈGLE N° 1

OPTIONS

Niveau de trace:

 standard (journal de connexions)
 tracer
 alarme mineure
 alarme majeure

===== Retour Accueil Stormshield ===== * **Stormshield**

From:
 / - **Les cours du BTS SIO**

Permanent link:
</doku.php/reseau/stormshield/fiche2?rev=1631566546>

Last update: **2021/09/13 22:55**

