## 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).

Sector Designed Sector		
CONFIGURATION GÉNÉRALE	CONFIGURATION AVANCEE	
État		
ON		
Paramètres généraux		
Nom:	in	
Commentaire:		
Cette interface est:	Interne (protégée)     O Externe (publique)	
Plan d'adressage		
Adressage:	O Plan d'adressage hérité du bridge   Dynamique / Statique	
Adresse IPv4:	<ul> <li>IP dynamique (obtenue par</li> <li>IP fixe (statique)</li> <li>DHCP)</li> </ul>	
<ul> <li>Confiduration DHCP avance</li> </ul>	iée	
interface était membre d'un b	ridge, la configuration est légèrement différente pour la zone <b>Plan d'adressage</b> :	
Plan d'adressage		
Adressage:	Ilan d'adressage hérité du bridge O Dynamique / Statique	
Bridge:	bridge 💌	
quez <b>Ip fixe (statique)</b> , un tal	bleau apparaît :	
Plan d'adressage		
Adressano'	<ul> <li>Plan d'adressage bérité du bridge (         Dynamigue / Statigue     </li> </ul>	
Adresse IPv4	IP dynamique (obtenue par     IP fixe (statique)	
	DHCP)	
+ Ajouter × Supprimer		
Adresse / Masque	Commentaire	
quez sur <b>+Ajouter</b> et dans la z DR /24 ou en notation décimale	cone Adresse / Masque saisissez <b>l'adresse IP de l'interface IN</b> 192.168.x.254 puis le m e pointée : 255.255.255.0	asqu
Plan d'adressage		
Adressage:	○ Plan d'adressage hérité du bridge ⑧ Dynamique / Statique	
in coordige.	O IP dynamique (obtenue par <ul> <li>IP fixe (statique)</li> </ul>	
Adresse IPv4:	DHCP)	
Adresse IPv4: + Ajouter × Supprimer	DHCP)	
Adresse IPv4: + Ajouter × Supprimer Adresse / Masque	DHCP) Commentaire	

- 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 :

ROUTES STATIQUES IPV4	ROUTAGE DYNAMIQUE	ROUTES DE RETOUR IPV4
Configuration générale	6	

Cliquez sur l'icône tout à droite pour ajouter un objet réseau, choisissez Machine et renseignez les champs Nom (Ex : GWNatNetwork) et l'Adresse IPv4 de la passerelle du réseau NatNetwork : 192.36.253.1 puis cliquez le bouton Créer.

CREER UN OBJET		
Machine		
Nom DNS (FQDN)	Nom de l'objet:	FWOUT_Siege Q
e Réseau	Adresse IPv4:	192.36.253.1
	Adresse MAC:	01:23:45:67:89:ab (Facultatif)
🥶 Routeur	Résolution	
Groupe	<ul> <li>Aucune (IP statique)</li> </ul>	O Automatique
Protocole IP		
1 Port	Commentaire:	
🚧 Groupe de ports	oonmentane.	

===== 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.** :

Network Security	MONITORING	CONFIGURATION	EVA1 VMSNSX09	9K0639A9			⊖ admin ・ I écriture / ■ Acc	ÈS RESTREINT
*- «		E SÉCURITÉ / EUTRAG	E ET NAT					
CONFIGURATION	4 TOLINGOL DI	E GEOGRATE / TIERWRO	E E I IVII					
Rechercher	🥀(1) Block all	✓ Editer	▪   "≟ Exporter   0					
H SYSTÈME	FILTRAGE N/	AT						
	Rechercher	+ Nouvel	le règle 🔹 🗙 Supprim	er   🕇 🕹   🧩	🛃   🔄 Couper	🔄 Copier 🕥	Coller   🗒 Chercher dans	les logs 🛛 🗮
EE RESEAU		État 🚉 Action	ET Source	Destination	Port dest.	Protocole	Inspection de sécurité 🖃	Commentaire
OBJETS	∃ Remote Manag	ement: Go to System - Config	guration to setup the web a	dministration applicatio	on access (contient 2	règles, de 1 à 2)		
LUTILISATEURS	1 🚥	🔹 on 🔹 passer	Any	🛱 firewall_all	firewall_srv		IPS	Admin from every
POLITIQUE DE SECURITE	2	on O passer	Any Any	B firewall_all	Any	icmp (requête Ech	IPS	Allow Ping from e
Filtrage et NAT	∃ Default policy (	contient 1 règles, de 3 à 3)						-
Filtrage URL	3 🚥	🜑 on 🗢 bloquer	Any	Any	🛚 Any		IPS	Block all
Filtrage SSL								

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 boitier. 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.

PILTRAGE       NAT         Perchercher       Image: Action       Supporting       Image: Actin       Supporting       Im	(10) Pass all	1	Editer	Exporter						
Rechercher: + Nouvelle règle * X Supprimer * # # * * # Couper <th>FILTRAGE</th> <th>NAT</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	FILTRAGE	NAT								
Etter atton avoite Destination Por dest. Protocole Inspection de sécurité so Comme   1 Com © passer Any Any Any Editer   Inspection de sécurité so   Comme	Rechercher		+ Nouvelle règle	e 🔹 🗙 Supprimer	* *   *	🖌   🔄 Couper	Copier	D Coller	🐘 Chercher dan	s les logs
1       Con       Passer       Any       Any       Any       Edition         Iliquez sur Éditer puis copier vers et choisir une politique vide (par exemple Filter 05).         XPPLIQUER ET COPIER LE PROFIL         Image: Comment of the second se		État ≞•	Action =	Source	Destination	Port dest.	Protocole	Inspec	ction de sécurité 🚉	Commenta
Iiquez sur Editer puis copier vers et choisir une politique vide (par exemple Filter 05).         APPLIQUER ET COPIER LE PROFIL         Image: Comparison of the provide state of	1	C on	passer	* Any	Any	* Any		IPS		
ANNULER       SAUVEGARDER LES MODIFICATIONS ET COPIER VERS (5) FILTER 05         Inquez Sauvegarder les modifications * Dans la liste déroulante des politiques de sécurité, nisissez la politique (05) Pass all. * Cliquez Éditer puis Renommer et renommez-là en AgenceX, puttre à jour. * Cliquez le bouton Appliquer puis Activer la politique AgenceX.         ACTIVER LA POLITIQUE SÉLECTIONNÉE?         Ø         Souhaitez-vous activer la politique sélectionnée ? Attention, cette activation recharge les configurations locales et globales.         ANNULER       ACTIVER LA POLITIQUE ENTREPRISEA         politique AgenceX est activée :         POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT         (a) AgenceA       • Ester • * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Coller * Coller * Coller * Coller * Supprimer * 1 & * * * @ Couper * Coller * Supprimer * * Supprimer * * * * * * * * * * * * * * * * * * *	Cliquez sur	r <b>Editer</b> pi	uis <b>copier v</b>	ers et chois	ir une politic	que vide (pa	r exemp	le <b>Filte</b>	er 05).	
Toutes vos modifications seront sauvegardées puis copiées de(10) Pass all \nvers (5) Filter 05.         ANNULER       SAUVEGARDER LES MODIFICATIONS ET COPIER VERS (6) FILTER 05         Idquez Sauvegarder les modifications * Dans la liste déroulante des politiques de sécurité, bisissez la politique (05) Pass all. * Cliquez Éditer puis Renommer et renommez-là en AgenceX, pettre 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 ENTREPRISEA         politique AgenceX est activée :         POUTIQUE DE SÉCURITÉ / FILTRAGE ET NAT         (b) AgenceA <ul> <li>batter &lt; "3 Exporter (*)</li> <li>ta (*) (*) Couper (*) C</li></ul>	APPLIQUE	R ET COPI	ER LE PROF	IL						
ACTIVER LA POLITIQUE SÉLECTIONNÉE?	Cliquez <b>Sa</b>	ANNUL	ER SA	UVEGARDER I	LES MODIFIC	ATIONS ET C	opier vei	RS (5) FI	ILTER 05	
Souhaitez-vous activer la politique sélectionnée ? Attention, cette activation recharge les configurations locales et globales. ANNULER ACTIVER LA POLITIQUE ENTREPRISEA politique AgenceX est activée : POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT (5) AgenceA · Editer · * Exporter • ILTRAGE NAT Chercher. + Nouvelle règle · × Supprimer • • • • • • • • • • • • • • • • • • •	ioisissez la <b>ettre à io</b>	politique	(05) Pass a	all. * Cliquez	* <b>Éditer</b> puis	ste deroular 5 <b>Renomme</b> er la politic	ite des pi er et rend iue Agel	olitique ommez- <b>nceX</b> .	-là en <b>Agen</b>	é, <b>ceX</b> , pu
ANNULER ACTIVER LA POLITIQUE ENTREPRISEA  politique AgenceX est activée :  POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT  (5) AgenceA	oisissez la ettre à jo ACTI	politique ur. * Cliqu VER LA P	(05) Pass a lez le boutor OLITIQUE	all. * Cliquez n Appliquer SÉLECTION	* Dans la lis <b>Éditer</b> puis puis <b>Active</b> INÉE?	ste deroular 5 Renomme er la politic	ite des pr e <b>r</b> et rend <b>jue Age</b> i	olitique ommez- <b>nceX</b> .	-là en <b>Agen</b>	é, <b>ceX</b> , pu
politique AgenceX est activée : POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT (5) AgenceA     Editer   Exporter    Exporter    Coller   Coller	oisissez la ettre à jo ACTI	ver LA P Sout	(05) Pass a lez le boutor POLITIQUE haitez-vous ntion, cette	all. * Cliquez n Appliquer SÉLECTION activer la p activation	* Dans la lis : Éditer puis · puis Active INÉE? politique sé recharge le	er la politic	re des po r et reno jue Agen ? ations lo	nceX.	et globales	é, ceX, pu
POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT	oisissez la ettre à jo ACTI	ver LA P Sout Atter	(05) Pass a lez le boutor OLITIQUE haitez-vous ntion, cette ANNULE	all. * Cliquez n Appliquer SÉLECTION s activer la p activation ER AC	* Dans la lis • Éditer puis • puis Active INÉE? politique sé recharge le CTIVER LA P	er la politic	re des pi r et renc jue Ager ? ations lo	ontique ommez- nceX.	et globales	έ, <b>ceX</b> , ρι
(5) AgenceA	oisissez la ettre à jo ACTI E	ver LA P Sout Atter	(05) Pass a lez le boutor OLITIQUE : haitez-vous ntion, cette ANNULE est activée	all. * Cliquez n Appliquer SÉLECTION s activer la p activation ER AC	* Dans la lis <b>Éditer</b> puis • puis <b>Active</b> INÉE? politique sé recharge le CTIVER LA P	er la politic	re des pi ret renc jue Ager ? ations lo	ontique ommez: nceX.	et globales	é, ceX, pi
ILTRAGE     NAT       chercher     + Nouvelle règle ▼     X Supprimer     1 + 1 ≠ * * * 1 1 2 Couper     1 Copier     1 Cop	Disissez la ettre à jo ACTI ACTI Politique A	Politique ur. * Cliqu VER LA P Sout Atter AgenceX	(05) Pass a lez le boutor POLITIQUE : haitez-vous ntion, cette ANNULE est activée FILTRAGE ET NAT	all. * Cliquez n Appliquer SÉLECTION a activer la p activation ER AC	* Dans la lis : Éditer puis : puis Active INÉE? politique sé recharge le CTIVER LA P	er la politionée es configur	re des pir er et reno jue Ager ? ations lo	olitique ommez- nceX.	et globales	é, ceX, pi
chercher + Nouvelle règle - × Supprimer   1 ↓   * * *   2 Couper 2 Copier 2 Coller   , Chercher dans les logs 2 Cher	politique A POLITIQUE D (5) AgenceA	Politique ur. * Cliqu VER LA P Sout Atter AgenceX	(05) Pass a lez le boutor OLITIQUE : haitez-vous ntion, cette ANNULE est activée FILTRAGE ET NAT	All. * Cliquez Appliquer SÉLECTION a activer la p activation ER AC	* Dans la lis : Éditer puis : puis Active INÉE? politique sé recharge le	électionnée es configur	re des pir ret renc jue Ager ? ations lo	olitique ommez- nceX.	et globales	é, ceX, pu
État 🖅 Action 🖅 Source Destination Port dest. Protocole Inspection de sécurité	politique A politique A polit	AgenceX	(05) Pass a lez le boutor OLITIQUE : haitez-vous ntion, cette ANNULE est activée FILTRAGE ET NAT	all. * Cliquez Appliquer SÉLECTION activer la g activation ER AC Exporter 0	* Dans la lis : Éditer puis : puis Active INÉE? politique sé recharge le	er la politic	re des p r et renc jue Ager ? ations lo	ontique ommez- nceX.	et globales	é, ceX, pu
	Politique A Politique A Politique A Politique A Constant Politique A Politique A Politique A Politique A Politique A Politique A Politique A Politique A	AgenceX	(05) Pass a lez le boutor OLITIQUE : haitez-vous ntion, cette ANNULE est activée FILTRAGE ET NAT	Appliquer SÉLECTION Cactiver la p e activation ER AC	* Dans la lis <b>Éditer</b> puis puis <b>Active</b> INÉE? politique sé recharge le CTIVER LA P	Renomme er la politic électionnée es configur POLMQUE E	er et renc jue Agen ? ations lo NTREPR		et globales	é, ceX, pu

**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	Rechercher   + Nouvelle règle - × Supprimer   1						* 🛃   🔄 Coup	er 🖸 Copier	🐑 Coll	er   🖳 Cher	cher dans les logs
	E7	Tr	a <mark>fic original</mark> (a	avant translation)			Trafic après	translation			
	Etat	Source	Destinat	Port dest.		Source	Port src.	Destination	Port d	Protocole	Options
Т	CD off	🔲 Any	🔳 Any	🖾 Any	**	🖬 Any	# ephemeral_fw	🖬 Any			

Une nouvelle règle non activée apparaît avec des valeurs par défaut any, any. Dans la section **Trafic** après translation, le port source sera traduit par un numéro de port choisi aléatoirement dans la plage ephemeral\_fw. La configuration du **Trafic 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 **Trafic 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 translatée définit l'adresse IP ou le réseau destination et Port destination translatée 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 AVANT TRANSLATION (ORIGINALE) Source originale GÉNÉRAL CONFIGURATION AVANCÉE Destination originale Source translatée Général Destination translatée Protocole Utilisateur: 🖯 🔹 📵 🔹 Rechercher. ÷ Options Machines sources: × Supprimer . 9 + Ajouter 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 DESTINATION AVANT TRANSLATION (ORIGINALE) Source originale GÉNÉRAL CONFIGURATION AVANCÉE **Destination originale** Source translatée Général Destination translatée Protocole Machines destinations: + Ajouter × Supprimer ... Options Internet Port destination: 0. + Ajouter X Supprimer

Апу

From: / - Les cours du BTS SIO

Permanent link: /doku.php/reseau/stormshield/fiche2?rev=1631566080

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

Last update: 2021/09/13 22:48

