### Fiche 6 – Configuration du NAT/PAT

# **Table des matières**

I Mise en œuvre du NAT dynamique	.1
Il Mise en œuvre du NAT statique par port (redirection de port)	.4

Dans les pare-feu SNS, les règles de filtrage et 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 l'icône :

## I Mise en œuvre du NAT dynamique

La règle de NAT dynamique NAPT permet aux machines du réseau interne (Network\_internals) d'accéder au réseau externe (Network\_Out) et à Internet

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 prédéfinie **ephemeral\_fw** [20000-59999] au niveau du port source dans le trafic après traduction. Par défaut, les ports sont choisis séquentiellement dans cette plage, cependant une option est disponible pour permettre un choix aléatoire du numéro de port pour chaque nouvelle connexion et le rendre ainsi moins prédictible.

#### Dans votre politique (10), sélectionner l'onglet NAT puis Nouvelle règle / règle de partage d'adresse source (masquerading)

FILTRAGE NAT

Rechercher			+ Nouv	elle règle 👻	× Supprimer	Ŧ	$ \mathbf{x}  \neq \mathbf{z}$	🖉   🕃 Coupe	er 🔄 Copier	🕑 Coll	er   🗒 Cherch	er dans les logs	
			E.	Trafic original (avant translation)		Trafic après translation			Dretocolo	Ontingo			
		Etat		Source	Destinat	Port dest.		Source	Port arc.	Destination	Port d	Protocole	Options
	1	Ð	off	🗖 Any	🖪 Any	Any	+	🖪 Any	T 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 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 permet de définir l'adresse IP d'un hôte ou du réseau source ;
- Destination 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 définit l'adresse IP ou le réseau source et le port source vus de l'extérieur.
- **Destination** définit l'adresse IP ou le réseau destination et **Port destination** translatée le port de destination.

#### Pour configurer un NAT/PAT pour permettre la sortie sur Internet

- Double-cliquer sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée « Edition de la règle N°1 ».
- Cliquer l'onglet du menu de gauche **Général**, dans la zone **Commentaire**, saisir un commentaire, par exemple « Configuration de la règle de NAT/PAT pour la sortie internet ».
- Cliquer sur l'onglet du menu de gauche **Source Originale**.
- Double-cliquer sur Any et avec la flèche choisir **Network\_internals** (qui renvoie à tous les réseaux internes protégés), dans l'onglet Configuration avancée, laissez **Any** pour le port de destination.

Général	SOURCE AVANT TRANSLAT	TION (ORIGINALE)	
Source originale			
Destination originale	GÉNÉRAL CONFIGU	IRATION AVANCEE	
Source translatée	Général		
Destination translatée	- Ociciai		
			-
Protocole	I Itilisateur:	Hereit Hereit Hechercher	
Protocole Options	Utilisateur:	Rechercher	

- Cliquer sur l'onglet du menu de gauche **Destination originale**.
- Double-cliquer sur **Any** et avec la flèche choisir **Internet**, laissez **Any** pour le port de destination.

General     DESTINATION AVANT TRANSLATION (ORIGINALE)       Source originale     GENERAL     CONFIGURATION AVANCEE       Source translatée     Général     Général       Destination translatée     Général     Général       Options     Machines destinations:     + Ajouter × Supprimer       Port destination:     + Ajouter × Supprimer     •	EDITION DE LA RÉGLE N	I' 1						
Source originale           Source originale         GENERAL         CONFIGURATION AVANCEE           Source translatée         Général         Général           Destination translatée         Machines destinations:         + Ajouter × Supprimer         • •           Options         Port destination:         + Ajouter × Supprimer         • •	Général	DESTINATION AVANT TRANS	LATION (ORIGINALE)					
Destination originale       GENERAL       CONFIGURATION AVANCEE         Source translatée       Destination translatée         Protocole       Machines destinations:       + Ajouter         Options       Port destination:       + Ajouter         Port destination:       + Ajouter       Supprimer         Any       Any	Source originale							
Source translatée Destination translatée Protocole Options  Port destination:  + Ajouter × Supprimer  - Internet  Port destination:  + Ajouter × Supprimer	Destination originale	GÉNÉRAL CONFIGUR	ATION AVANCÉE					
Destination translatée Protocole Options Machines destinations: + Ajouter X Supprimer Internet  Port destination: + Ajouter X Supprimer  T	Source translatée	Général						
Protocole     Machines destinations:     + Ajouter × Supprimer       Options     Port destination:     + Ajouter × Supprimer       Port destination:     + Ajouter × Supprimer       Any	Destination translatée	General						
Options Options Port destination: + Ajouter × Supprimer  Any	Protocole	Machines destinations:	A tinutar Y Cumpings	0				
Port destination: + Ajouter × Supprimer • •	Options	100000000000000000000000000000000000000	T Noulei A supplime					
Port destination: + Ajouter × Supprimer • •			Internet					
Port destination: + Ajouter × Supprimer • ·								
Port destination: + Ajouter × Supprimer • •								
Any		Port destination:	+ Ajouter X Supprimer	Θ.+				
			Any					



Attention : si dans la zone destination originale, 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 subiront également une traduction NAT vers l'interface **OUT** qui l'interprétera comme une tentative d'intrusion et les bloquera.

Vous pouvez rendre cette règle plus restrictive en choisissant explicitement l'interface de sortie.

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

EDITION DE LA RÈGLE N	1			
Général	DESTINATION A	VANT TRAP	ISLATION (ORIGINALE)	
Source originale				
Destination originale	GÉNÉRAL	CONFIGU	RATION AVANCÉE	
Source translatée	Configuration	a avancéa		
Destination translatée	comguration	avancee		
Protocole	Interface de sortie:		out	
Options				
			Publication ARP sur la destination externe (publique)	

- Cliquer sur l'onglet Source translatée et sélectionner Firewall\_Out dans Machine source translatée.
- Dans Port source translaté, laisser ephemeral\_fw et cocher choisir aléatoirement le port source translaté.

Cette option **choisit aléatoirement le port source translaté**, ce qui permet d'éviter les attaques utilisant la prédictibilité des ports utilisés. Ainsi si le premier port est 10000, le suivant ne sera pas 10001. Cette précaution n'empêche pas les attaques, elle permet de les rendre plus complexes.

Général	SOURCE APRÈS TRANSLATION			
Source originale				
Destination originale	GÉNÉRAL CONFIGURAT	TION AVANCÉE		
Source translatée	Général			
Destination translatée	General			
Protocole	Machine source translatée:	Firewall_out		<b>-</b> ≡
Options	Barton and a fait			
	Port source translate:	epnemera_tw	* =	
		🔽 abaiair aléatairement la part source trapalaté		

Cliquer 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		
Général	PROTOCOLE		
Source originale			
Destination originale	Protocole		
Source translatée			
Destination translatée	Type de protocole:	Détection automatique du protocole (par défaut)	*
Protocole	Protocole applicatif:	Détection automatique du protocole (par défaut)	\$0
Options	Protocole IP:	Protocole applicatif	
options		Protocole IP	
		Protocole Ethernet	

Cliquer 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, choisir tracer.

Général	OPTIONS		
Source originale			
Destination originale			
Source translatée	Niveau de trace:	🖹 standard (journal de connexions)	P
Destination translatée		standard (journal de connexions)	
Protocole		🗎 tracer	
Options		alarme mineure	
		🗶 alarme majeure	

NB : Le NAT ne laisse jamais de traces dans le journal de connexions. Pour tracer une règle de NAT, il faut choisir l'option « tracer », sinon, aucune journalisation de NAT ne sera effectuée.

Cliquer sur **OK** pour sauvegarder les modifications de la règle de NAT dynamique que vous venez de créer.

État

Dans la colonne État, sélectionner avec la flèche Définir l'état on

La règle passe à **1 Ton** 

Cliquer sur **Appliquer** puis **Oui, Activer la politique** puis confirmer.

Définir l'état on

Définir l'état off

Dans la nombre	a liste e de f	e des règ ois où la	gles la barre d règle a été ap	evient ver pliquée :	te quand	es règle	es s'appliqu	ent et une info	o-bulle indic	que le
FILTRAG	E N		regio a oto ap	piiquoo .						
Recherche	c		🕂 🕂 Nouvelle règle 👻	× Supprimer	114	210	Couper 🛛 🔄 Copie	r 👻 Coller   🗒 Cl	vercher dans les logs	E
		6 LT	Tra	fic original (avant	translation)			Trafic après t	ranslation	
		Etat	Source	Destination	Port des	L.	Source	Port src.	Destination	Port dest.
1 <b>-</b>	•	🔹 on	🖶 Network_internals	Internet interface: out	Any	-	. 🕻 FirewalLout	< 🍷 ephemeral_fw	Any	
	Cette	règle a été util	isée 12 fois							
Da Da	Dans le bandeau d'affichage des règles, déplier le menu et cliquer sur Réinitialiser les statistiques des règles pour remettre les compteurs à zéro.									
Copier	9	) Coller	🗒 Chercher d	ans les logs			=			
Prot	ocole		Inspection de séc	curité 🛂	Chercher da	ns la sup	ervision			
<b>1</b>	Réiniti	aliser les :	statistiques des rè	ègles ≡						
<b>1</b>	Réiniti	aliser l'affi	chage des colonn	es						

### II Mise en œuvre du NAT statique par port (redirection de port)

Pour faire une redirection NAT « classique », il faut sélectionner l'onglet NAT puis Nouvelle règle / règle simple.

**Exemple** avec une règle de NAT afin qu'unserveur WEB (objet srv\_web\_priv, protocole http) soit joignable grâce à une redirection de port via l'adresse IP publique OUT d'un pare-feu: « 192.36.253.70 ». Source originale = Internet, Interface d'entrée = out Destination originale = Firewall\_Out, Port dest= http

t	ranslaté = none	Any (ou pas de	source), Destination	TTANSIALEE	- srv_web_priv,	Port destination
	6 💽 on	Internet interface: out	Firewall_out	🖞 http	➡ 🗷 Any	srv_web_priv

Cliquer Appliquer puis Oui, Activer la politique puis confirmer.

Le détail ci-dessous :



latán — amu urah mulu. Dant dantinatian

#### Dans l'onglet Destination de la règle de filtrage, choisissez l'onglet Configuration avancée, puis dans NAT sur la destination, sélectionner l'objet correspondant à votre serveur web privé :

Destination:	srv_web_priv	-	≡
	Publication ARP sur la destination externe (publique)		

Puis dans l'onglet Port/Protocole, choisir http dans la zone Port destination translaté.

Port destination translaté: http	<ul> <li>Translation de port</li> </ul>		
Port destination translaté: http			
Port destination translaté: http			
	Port destination translaté:	http	- ≡

#### Traçage des règles de NAT

NAT sur la destination

Activer le traçage des règles de NAT permet d'avoir les informations visibles dans les Journaux d'audit (logs).

Double-cliquer sur la règle que vous voulez tracer et choisissez l'onglet **Options**, et dans niveau de tracer puis **OK**.

Général	OPTIONS	
Source originale		
Destination originale		
Source translatée	Niveau de trace:	🖹 tracer 💌
Destination translatée		NAT dans le tunnel IPSec (avant chiffrement, après déchiffrement)
Protocole		

Vous pouvez tester l'accès à l'ensemble de vos ressources et vérifier le traçage des règles demandées dans les logs du pare-feu (journal **standard** et journal **Filtrage**).

Cliquer sur l'onglet **Monitoring** puis **LOGS - Journaux d'audit / Vues / Trafic réseau** : vous devriez voir apparaître les traces :

LOG / TRAFIC RÉSEAU										
- 💼 <	C Actualiser	Re	chercher			» Red	cherche avancée			
RECHERCHE DU - 11/12/2021 17:51:52 - AU - 11/12/2021 18:51:52										
Action	Utilisateur	Ρ	Nom de la source	P	Nom de destination		Nom du port dest.			
Autoriser			Anonymized		www.a.net		http			
			Anonymized	55	www.google.fr		https			
<ol> <li>Autoriser</li> </ol>			Anonymized	598	www.google.fr		https			
<ol> <li>Autoriser</li> </ol>			Anonymized		3.debian.pool.ntp.org	<b>j</b>	ntp			
<ol> <li>Autoriser</li> </ol>			Anonymized		0.debian.pool.ntp.org	)	ntp			
<ol> <li>Autoriser</li> </ol>			Anonymized		www.b.net		http			
			Anonymized		webmail.b.net		http			
			Anonymized		www.b.net		http			
Autoriser			Anonymized		www.b.net		http			
			Anonymized	-	FW_B					
			Anonymized	н.	1.1.1.1					
			Anonymized	-	gw_default					
	EÉSEAU	RÉSEAU	RÉSEAU	Action Utilisateur   Action Utilisateur   Action Utilisateur   Autoriser Anonymized   Autoriser Anonymized	Action Utilisateur P.   Action Utilisateur P.   Action Utilisateur P.   Action Utilisateur P.   Autoriser Anonymized   Autoriser Anonymized	Image: Second state sta	Action Utilisateur P. Nom de la source P. Nom de destination   Action Utilisateur P. Nom de la source P. Nom de destination   Action Utilisateur P. Nom de la source P. Nom de destination   Action Utilisateur P. Nom de la source P. Nom de destination   Action Utilisateur P. Nom de la source P. Nom de destination   Actioniser Anonymized Monymized Www.google.fr Monymized   Autoriser Anonymized Monymized Monymized Monymized   Autoriser Anonymized Www.b.net Monymized Monymized   Autoriser Anonymized Www.b.net Monymized Monymized   Autoriser Anonymized Www.b.net Monymized Monymized   Autoriser Anonymized FW_B Monymized Monymized			



Il est également possible de réaliser une redirection de ports directement lors de la création d'une règle de filtrage (voir fiche 6). L'intérêt d'intégrer le filtrage et la redirection dans une règle unique est d'optimiser les performances puisque le pare-feu réalise un seul traitement au lieu de deux. Voici un exemple ci-dessous équivalent à la règle précédente :

4	_	•	€
1	On	passer	-

Internet interface: out Firewall\_out 

🖞 http