Fiche savoirs technologiques 4 : Configuration du NAT/PAT

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de NAT qui vont permettre d'accéder aux serveurs en DMZ de l'autre agence à travers des IP **publiques**.

Dans la fiche 2 vous avez mis en place une règle de NAT pour permettre l'accès à Internet à vos réseaux internes via la passerelle de l'enseignant.

Vous allez maintenant configurer des règles de NAT et des règles de redirections de ports afin de rendre accessible vos services hébergés par le serveur Debian de la DMZ.

Mise en oeuvre de la NAT statique

Vous disposez de 2 adresses IP publiques **192.36.253.x2** et **192.36.253.x3** réservées respectivement à vos serveurs FTP et MAIL (au besoin ajoutez ces 2 objets créés cf Partie 3).

Étape 1 : Vous allez ajouter les règles de NAT qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.

- Dans votre politique AgenceX, sélectionnez l'onglet NAT puis Nouvelle règle/ règle de NAT statique (bimap) ; un assistant s'ouvre :
 - Machine(s) privée(s) : L'adresse IP privée du serveur en interne
 - Machine(s) virtuelle(s) : L'adresse IP publique virtuelle dédiée au serveur interne
 - Uniquement sur l'interface : L'interface externe depuis laquelle le serveur est accessible avec son adresse IP publique virtuelle.
 - Uniquement pour les ports : La règle de NAT statique permet de translater tous les ports. Cependant, il est possible de la restreindre en spécifiant un ou une plage de ports au niveau de ce paramètre. Il est conseillé de laisser cette valeur à Any et de restreindre le port directement dans les règles de filtrage.
 - publication ARP : cochez Activer la publication ARP pour l'adresse IP publique.

jectif: Associer une adres:	se IP privée et une adresse IP publique	e (virtuel	le).			
Général	in separation of the serve of serve	a reed	er anen Providure			
					-	
A	DRESSE IP PRIVEE		ADRESSE IP	VIRTUELLE (PUBLIQU	E)	_
wachine(s) privee(s):	srv_rtp_priv	- =	machine(s) virtuelle(s):	siv_ttp_pub	•	-
			Uniquement sur l'interface:	out		
Configuration avancée						
	s: Any	* ≡				
Jniquement pour les port						

- Dans Adresse IP Privée, Machine(s) privée(s), choisissez l'adresse privée de la machine FTP : objet srvftppriv.
- Dans Adresse IP Virtuelle, Machine(s) virtuelle (s), choisissez l'adresse publique de la machine FTP : objet srvftppub.

Choisissez out dans Uniquement sur l'interface et laissez Any dans Uniquement pour les ports et cochez Publication ARP

 et cliquez Terminer.

L'assistant ajoute deux règles NATs :

- La première règle pour la translation du flux sortant du serveur interne vers le réseau public
- et la deuxième pour le flux entrant à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être modifiées par la suite indépendamment l'une de l'autre.

2		💽 on	srv_ftp_priv	Any interface: out	🐮 Any	→ LEP 🖪 srv_ftp_pub	
3		🔹 on 📊	Any I Interface: out	RE Srv_ftp_pub	Any Any	→	I srv_ftp_priv
 Proc 	édez de ma	nière ide	ntique pour le	e serveur mail : ol	bjet srv<i>ma</i>	ilpriv et objet srv<i>mail</i>pub	
	4	🔍 on	Srv_mail_pr	iv Any interface: out	× An	y → MRP 🖪 srv_mail_pub	
	5	🔹 on	Any interface: out	REP (srv_mail_	pub 💌 Ang	· •	🛙 srv_mail_priv

Étape 2 : Testez l'application de la première règle de NAT, en envoyant un ping vers la passerelle par défaut.

- Envoyez un ping vers la passerelle par défaut de **l'autre agence** depuis la machine serveur debian du réseau de votre agence (AgenceX) ;
- Ouvrez Configuration / Politique de sécurité / Filtrage et NAT onglet NAT sur le firewall de votre agence (AgenceX). Dans la liste des règles la barre devient verte quand les règles s'appliquent et une info-bulle indique le nombre de fois où la règle a été appliquée :

(5) Agence	eA	▼ Editer ▼	Exporter								
FILTRAGE	NAT										
Rechercher		+ Nouvelle	règle 🔹 🗙 Supprimer	+ + +	2	Couper	Copier 🐑 Coller	🛛 🗒 Chercher	dans les log		
	. E T	Ti	afic original (avant transla	riginal (avant translation)			Trafic après translation				
	Etat	Source	Destination	Port dest.	S	ource	Port src.	Destination	Port dest		
1 🚥	ඟ on	Po Network_interna	Internet interface: out	* Any	→ (Firewall_out	I ephemeral_fw	Any Any			
2 Cette règle a été utilisée 856 fois			Any interface: out	🐮 Any	➡ IRF II srv_ftp_pub						
ns le bande gles pour r	eau d'affic remettre le	hage des règles es compteurs à z	, dépliez le menu (éro.	3 traits horizor	ntaux) et cliquez su	r Réinitialiser l	es statistiq	ues des		
		Copier 🐑	Coller 🗒 Ch	ercher dans le	s log	5	=				
		Protocole Inspectio		11001000000000	Chercher dan						
		Protocole	Inspectio	n de sécurité	24	Chercher da	ris la supervision				
		Protocole	Inspectio	n de sécurité es des règles	=	Chercher da	ns la supervision				

Mise en oeuvre de la redirection de ports

Étape 3 : Vous allez ajouter une règle de NAT afin que votre serveur WEB (objet srvwebpub, protocole http) soit joignable grâce à une redirection de port via l'adresse IP publique OUT de votre firewall : 192.36.253.x0.

 Dans votre politique AgenceX, sélectionnez l'onglet NAT puis Nouvelle règle / règle simple et modifiez avec les paramètres suivants :

T http

- Source originale = Internet,
- Interface d'entrée = out,
- Destination originale = FirewallOut, * Port dest= http, * Source translatée = Any, * Destination translatée = srvwebpriv, * Port destination translaté = ephemeralfw.

🖸 Any

6	n 💽	Internet	Firewall_out
		interface, out	

===== Traçage des règles de NAT =====

🖪 srv_web_priv 🎽 ephemeral

Étape 4 : Vous allez activez le traçage des règles de NAT pour les flux entrants, ceci permet d'avoir les informations visibles dans les Journaux d'audit (logs).

* Double-cliquez une règle (par ex la règle n°3), et choisissez l'onglet Options, et dans niveau de trace tracer* puis OK. * Répétez l'opération pour les autres règles entrantes.

EDITION DE LA RÈGLE	l° 3				
Général	OPTIONS				
Source originale					
Destination originale					
Source translatée	Niveau de trace:	📄 tracer			
Destination translatée		VAT dans le tunnel IPSec (avant chiffrement, après déchiffrement)			
Options					

Vous pouvez tester l'accès à l'ensemble de vos ressources et vérifiez le traçage des règles demandées (flux entrants) dans les logs du firewall. Vous pouvez par exemple tenter d'accéder via des ping d'une machine debian à l'autre. * Cliquez l'onglet **Monitoring** puis **LOGS - Journaux d'audit / Vues / Trafic réseau** : vous devriez voir apparaître les ping vers la passerelle du Siège effectués précédemment.

LOG / TRAFIC RÉSEAU

Dernière heure	- 💼	C Actualiser R	echercher.						
RECHERCHE DU - 08	/09/2020 01:	26:08 - AU - 08/09/	2020 02:2	6:08					
Enregistré à	Action Utilisateur Pa			Nom de la source	Nom de destination	N			
08/09/2020 02:26:04	Autoriser			Anonymized		FW_Siege	^		
08/09/2020 02:26:03	Autoriser			Anonymized		FW_Siege			
08/09/2020 02:26:02	 Autoriser 			Anonymized		FW_Siege			
08/09/2020 02:26:02	 Autoriser 			Anonymized		dns2.google.com			
08/09/2020 02:26:02	O Autoriser			Anonymized		dns1.google.com			
08/09/2020 02:25:26	 Autoriser 			Anonymized Firewall_dr		Firewall_dmz2	all_dmz2		
08/09/2020 02:25:26	• Autoriser			Anonymized		srv_dns_priv			
08/09/2020 02:24:59				Anonymized		srv_dns_pub			

From: / - Les cours du BTS SIO

Permanent link: /doku.php/reseau/stormshield/fiche4?rev=1632085124

Last update: 2021/09/19 22:58

