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 GÉNÉRALE	CONFIGURATION AVANCÉE	
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	
Adresse IPv4:	 IP dynamique (obtenue par IP fixe (statique) 	
 Confiduration DHCP avancée 		
interface était membre d'un bric	dge, la configuration est légèrement différente pour la zone Plan d'adressag	ge :
lan d'adressage		
dressage:	Ilan d'adressage hérité du bridge O Dynamique / Statique	
dressage: ridge:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge 	
dressage: ridge: cas échéant, cliquez dans la zone	Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique	
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique) , un table	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît : 	
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique) , un table Plan d'adressage	Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît :	
dressage: ridge: cas échéant, cliquez dans la zone quez Ip fixe (statique) , un table Plan d'adressage Adressage:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît : Plan d'adressage hérité du bridge O Dynamique / Statique 	
dressage: ridge: cas échéant, cliquez dans la zone uez Ip fixe (statique) , un table Plan d'adressage Adressage: Adresse IPv4:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît : O Plan d'adressage hérité du bridge O Dynamique / Statique O Plan d'adressage hérité du bridge O Dynamique / Statique O Plan d'adressage hérité du bridge O Dynamique / Statique O Plan d'adressage hérité du bridge O Dynamique / Statique O IP dynamique (obtenue par O IP fixe (statique) DHCP) 	
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique) , un table Plan d'adressage Adressage: Adresse IPv4: + Ajouter × Supprimer	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît : Plan d'adressage hérité du bridge Dynamique / Statique IP dynamique (obtenue par DHCP) IP fixe (statique) 	
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique) , un table Plan d'adressage Adressage: Adresse IPv4: Adresse / Masque	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique au apparaît : Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique (obtenue par O IP fixe (statique) DHCP) Commentaire 	
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique), un table Plan d'adressage Adressage: Adresse IPv4:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique eau apparaît : Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique (obtenue par O IP fixe (statique) DHCP) Commentaire 	puis le masqu
dressage: ridge: cas échéant, cliquez dans la zone juez Ip fixe (statique) , un table Plan d'adressage Adressage: Adresse iPv4:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique e Plan d'adressage hérité du bridge O Dynamique / Statique Plan d'adressage hérité du bridge Pire (statique) DHCP Commentaire Adresse / Masque saisissez l'adresse IP de l'interface IN 192.168.x.254 plan d'adressage hérité du bridge Pire Pire (statique) 	puis le masqu
dressage: ridge: cas échéant, cliquez dans la zone quez Ip fixe (statique) , un table Plan d'adressage Adressage: Adresse IPv4: + Ajouter × Supprimer Adresse / Masque quez sur +Ajouter et dans la zon R /24 ou en notation décimale por Plan d'adressage Adressage: Adressage:	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique (obtenue par O IP fixe (statique) DHCP) Commentaire commentaire Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique saisissez l'adresse IP de l'interface IN 192.168.x.254 Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique (obtenue par O IP fixe (statique) 	puis le masqu
dressage: ridge: cas échéant, cliquez dans la zone quez Ip fixe (statique), un table Plan d'adressage Adressage: Adresse IPv4: + Ajouter × Supprimer Adresse / Masque quez sur +Ajouter et dans la zon R /24 ou en notation décimale por Plan d'adressage Adressage: Adressage: Adresse IPv4: + Ajouter × Supprimer	 Plan d'adressage hérité du bridge O Dynamique / Statique bridge Plan d'adressage sur Dynamique/Statique Plan d'adressage hérité du bridge O Dynamique / Statique IP dynamique (obtenue par O IP fixe (statique) DHCP) Nasque saisissez l'adresse IP de l'interface IN 192.168.x.254 prive (statique) Plan d'adressage hérité du bridge O Dynamique / Statique DHCP 	puis le masqu

- 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 :

RECENCY ROUTHOE			
ROUTES STATIQUES IPV4	ROUTAGE DYNAMIQUE	ROUTES DE RETOUR IPV4	
Configuration générale			

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 ON OBJET		
Achine		
FORN Nom DNS (FODN)	Nom de l'objet:	FWOUT_Siege Q
¤¦⊟ Réseau	Adresse IPv4:	192.36.253.1
aa Plage d'adresses IP	Adresse MAC:	01:23:45:67:89:ab (Facultatif)
🐸 Routeur	Résolution	
Groupe	 Aucune (IP statique) 	O Automatique
Protocole IP		
1 Port	Commentaire	
🚧 Groupe de ports	control citere.	

===== 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 / TIERRAG	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.

* Dans la liste déroulante des politiques de sécurité, choisissez (10) Pass all. Cette politique laisse explicitement passer tous les flux.

FILTRAGE	NAT								
Rechercher		+ Nouvelle règi	e • X Supprimer	t = t *	🖌 🔄 Couper	Copier	D Coller	🛱 Chercher dans	les logs
	État ≞•	Action =•	Source	Destination	Port dest.	Protocole	Inspec	tion de sécurité <u>≞</u> ▼	Commentai
1	💿 on	passer	* Any	Any	* Апу		IPS		
APPLIQU	ER ET COP	IER LE PROF	ΠL		(pur exemple				
	ER ET COP	IER LE PROF	TL ons seront sa	uvegardées	puis copiées	de(10) Pa	ss all \	nvers (5) Filt	er 05.

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

