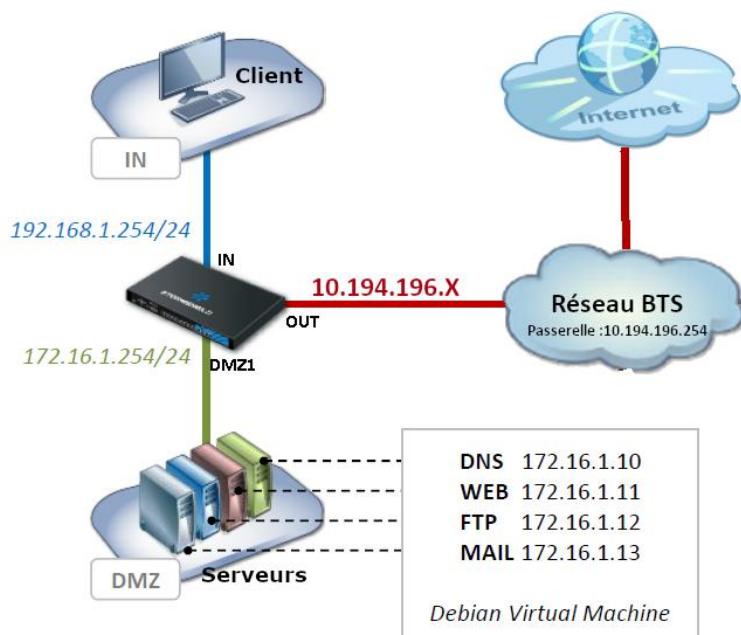


Activité 5 - Stormshield Filtrage

Lors de l'activité 4 vous avez configuré la translation d'adresse NAT.
Maintenant, vous allez mettre en œuvre le filtrage du trafic depuis le pare-feu Stormshield.

1 – Rappel - Infrastructure virtuelle



Lors de l'activité 4 vous avez configuré la translation d'adresse NAT.

Maintenant, vous allez mettre en œuvre le filtrage du trafic.

Etudiant	Adresse IP interface OUT	srv_ftp_pub	srv_mail_pub
1	10.194.196.30	10.194.196.31	10.194.196.32
2	10.194.196.33	10.194.196.34	10.194.196.35
3	10.194.196.36	10.194.196.37	10.194.196.38
4	10.194.196.39	10.194.196.40	10.194.196.41
5	10.194.196.42	10.194.196.43	10.194.196.44
6	10.194.196.45	10.194.196.46	10.194.196.47
7	10.194.196.48	10.194.196.49	10.194.196.50
8	10.194.196.51	10.194.196.52	10.194.196.53
9	10.194.196.54	10.194.196.55	10.194.196.56
10	10.194.196.57	10.194.196.58	10.194.196.59
11	10.194.196.60	10.194.196.61	10.194.196.62

Votre objectif

Grâce à la politique de filtrage, l'administrateur est capable de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers du Pare-feu. Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise. Par exemple, dans notre cas :

- Le PC Administrateur doit pouvoir accéder au Pare-feu.
- Le réseau interne **IN** doit pouvoir accéder aux serveurs de votre **DMZ**.
- Vous pouvez accéder à Internet en http ou https.
- Vous ne pouvez pas accéder sur les sites de l'Iran (test avec www.visitiran.ir).
- L'accès au site <https://www.cnn.com> est bloqué depuis le réseau interne.
- Vous pouvez émettre un ping vers l'extérieur de votre réseau depuis le réseau interne.
- Les réseaux externes peuvent joindre vos serveurs Web et FTP.
- Les réseaux externes sont autorisés à pinguer l'interface « out » de votre firewall.

Lors de l'activité 6 "Filtrage de contenu", vous complèterez le filtrage par des inspections de sécurité (IPS) : analyse antivirus, analyse antispam, filtrage URL, ...

Ceci permettra d'avoir une politique de filtrage efficace.

Configuration de la politique de filtrage

Une règle de filtrage se base sur de nombreux critères :

- ✓ L'adresse IP source et/ou destination,
- ✓ La réputation et la géolocalisation de l'adresse IP source et/ou destination,
- ✓ L'interface d'entrée et/ou sortie,
- ✓ L'adresse réseau source et/ou destination,
- ✓ Le FQDN source et/ou destination,
- ✓ Le service TCP/UDP,
- ✓ Le protocole IP
- ✓ ...

Il est recommandé d'ordonner au mieux les règles de la plus **restrictive** à la plus **généraliste**.
Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué.

Technologie SPI (Stateful Packet Inspection)

Le firewall peut garder en mémoire l'état des connexions TCP, UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. On parle de suivi "Stateful" qui implique que les réponses faisant partie de la même connexion sont implicitement autorisées.

- ⇒ Nul besoin d'une règle de filtrage supplémentaire pour autoriser (dans le sens entrant) les paquets réponse d'une connexion établie au travers du firewall.

Les types de filtrage

Le filtrage implicite

Regroupe les règles de filtrage préconfigurées ou ajoutées dynamiquement par le firewall pour autoriser ou bloquer certains flux après l'activation d'un service.

Les règles implicites sont accessibles depuis le menu **CONFIGURATION** ⇒ **POLITIQUE DE SÉCURITÉ** ⇒ **Règles implicites**. Chaque règle peut être activée/désactivée.

- 👉 1 – Observez les règles de filtrage active sur votre firewall.

Vous ne modifierez pas ces règles lors de cette activité.

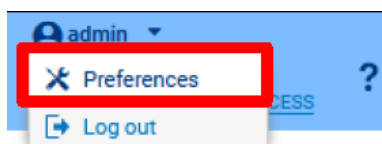
Le filtrage global

Regroupe les règles de filtrage injectées au firewall depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales. Permet la gestion du filtrage sur un réseaux multisites : réseau constitué de plusieurs réseaux et pare-feux Stormshield.

Vous ne modifierez pas ces règles lors de cette activité.

Le filtrage local : Représente les règles de filtrage ajoutées par l'administrateur (donc vous) depuis l'interface d'administration. C'est ce type de règles que vous allez mettre en œuvre sur le firewall.

- 👉 2 – Affichez les règles globales



Pour afficher les règles globales, il faut cocher l'option **Afficher les politiques globales (Filtrage, NAT, VPN IPsec et Objets)** dans le menu **Préférences** --> Onglet **affichage**.

✖ PRÉFÉRENCES

↶ Restaurer les paramètres par défaut

PARAMÈTRES

AFFICHAGE

LIENS

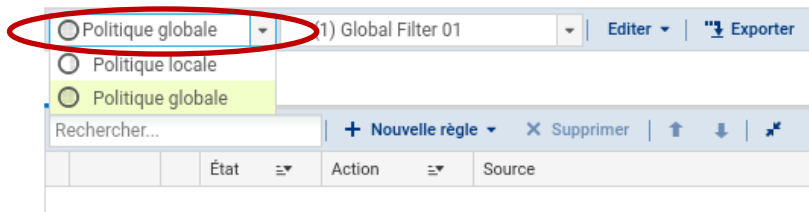
Paramètres de l'application

- ☐ Toujours afficher les éléments de configuration avancée
- ☐ Afficher le bouton d'enregistrement des commandes
- ☐ Afficher les utilisateurs dès l'accès au module
- ☒ Afficher les objets réseau dès le lancement du module
- ☒ Afficher les politiques globales (Objets réseau, Certificats, Filtrage, NAT et VPN IPsec)
- ☒ Appliquer un commentaire par défaut aux règles (Filtrage, NAT et IPsec)

Nombre de règles par page (Filtrage, NAT et IPsec)

Automatique

✚ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT



Cette option fait apparaître dans l'en-tête du menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Filtrage et NAT** une liste déroulante qui permet de sélectionner les politiques globales ou locales. Par défaut, aucune règle de filtrage et NAT n'est présente dans les slots globaux.



3 – Votre ami : l'analyseur de cohérence et de conformité. Analysez cette configuration.

✚ SECURITY POLICY / FILTER - NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_in	srv_mail	smtp	udp	IPS
2	on	pass	Network_in	srv_dns	dns		IPS
3	on	pass	Network_in	Internet	https, http		IPS
4	on	block	Network_in	Internet Geolocation Iran	https, http		IPS
5	on	pass	Internet interface: out	Network_in	http		IPS

CONFIGURATION VALIDATOR (2 ⚠ / 1 ✖)

- ⚠ The active policy is not up to date. We recommend that you activate the policy.
- ✖ [Rule 1] The destination port 'smtp' uses an IP that is incompatible with the value of the protocol column
- ⚠ [Rule 4] This rule will never be applied as it is covered by the rule 3.

Les firewalls Stormshield Network embarquent un moteur de vérification qui permet de détecter d'éventuelles situations de recouvrement ou d'incohérence créées dans la politique de filtrage. Ce type de situation est signalé par un message d'avertissement en bas du menu.

Trois exemples sont illustrés dans la figure ci-dessus :

- ✓ Dans la règle n°1, le port destination HTTPS est incompatible avec le protocole UDP parce que le protocole applicatif HTTPS utilise le protocole de transport TCP,
- ✓ La règle n°4 ne sera jamais utilisée parce qu'elle est recouverte par la règle n°3.

NOTE : Les messages signalés avec une croix rouge bloquent l'activation de la politique.

4 – Copiez la politique de filtrage/NAT **(4) Activite_4** vers la politique numéro 5. Renommez la politique "**Activite_5**", puis activez cette politique (bouton "**Appliquer**" en bas de la page).

5 – Dans l'onglet **Filtrage**, supprimez la règle **Pass any any any** proposée par défaut.

Remarque : Pour les prochaines règles de filtrage vous afficherez la colonne "nom" (elle est cachée par défaut). Pourquoi nomme-t-on les règles ?

Dans les journaux d'audit, la recherche s'effectue sur le nom de la règle. Cela permet de retrouver très facilement dans les logs tous les paquets qui ont été filtrés par la règle de filtrage.

Filtrage du trafic interne

Règle à configurer

Le PC Administrateur doit pouvoir accéder au Pare-feu.

6 – Créer un séparateur pour cette règle. Vous le nommerez "**Administration depuis PC Admin**".

7 – Complétez le tableau suivant pour configurer la règle :

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Admin_vers_Parefeu	passer	Pc_admin	Firewall_in	https	-----	IPS

Solution

FILTRAGE		NAT	
Rechercher...	+ Nouvelle règle	X Supprimer	↑ ↓ ↶ ↷
	Couper	Copier	Coller
	Chercher dans les logs	Chercher dans l	
	État	Nom	Action
	Source	Destination	Port dest.
	Protocole	Inspection de sécurité	
1	on	Admin_vers_parefeu	passer
	pc_admin	Firewall_in	https
			IPS

Règles à configurer

Votre réseau interne (IN : 192.168.1.0/24) doit pouvoir accéder aux serveurs de votre DMZ : DNS, WEB (ports 80 et 808 pour le Webmail), FTP et SMTP.

Il faudra faire une règle par type de serveur.

8 – Créer un séparateur pour cette règle. Vous le nommerez "**Trafic IN vers DMZ**".

9 – Complétez le tableau dans le cas où l'on souhaite accéder au serveur DNS.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_DNS	pass	network_in	srv_dns	dns	-----	IPS

10 – Complétez le tableau dans le cas où l'on souhaite accéder au serveur WEB.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_WEB	pass	network_in	srv_web	http	-----	IPS

11 – Complétez le tableau dans le cas où l'on souhaite accéder au serveur WEB pour faire du webmail.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_WEBMAIL	pass	network_in	srv_web	webmail	HTTP	IPS

✂ 12 – Complétez le tableau dans le cas où l'on souhaite accéder au serveur FTP.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_FTP	pass	network_in	srv_ftp	ftp	-----	IPS

✂ 13 – Complétez le tableau dans le cas où l'on souhaite accéder au serveur SMTP.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_SMTP	pass	network_in	srv_mail	smtp	-----	IPS

Règle à configurer

Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine (pc_stagiaire) est 192.168.1.200.

👉 14 – Créez un objet "pc_stagiaire" qui vous associerez à l'adresse 192.16.1.200.

✂ 15 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Block_ftp_stagiaire	block	pc_stagiaire	any	ftp	-----	IPS

✂ 16 – Pour que cette dernière règle soit exécutée correctement comment la positionnée par rapport aux autres règles ?

Pour que l'on puisse bloquer le PC du stagiaire s'il génère une requête FTP il faut mettre cette règle avant la règle générale qui autorise l'accès au serveur FTP à tous les éléments du réseau IN ou en première position.

Solution

FILTRAGE		NAT	
Rechercher...	+ Nouvelle règle	X Supprimer	↑ ↓ ↺ ↻
État	Nom	Action	Source
ADMINISTRATION DEPUIS PC_admin (contient 1 règles, de 1 à 1)			
1	Admin_vers_parefeu	passer	pc_admin
BLOCAJE FTP STAGIAIRE (contient 1 règles, de 2 à 2)			
2	BLOCK_FTP_STAGIAIRE	bloquer	pc_stagiaire
TRAFFIC IN VERS DMZ (contient 5 règles, de 3 à 7)			
3	IN_VERS_DNS	passer	Network_in
4	IN_VERS_WEB	passer	Network_in
5	IN_VERS_WEBMAIL	passer	Network_in
6	IN_VERS_FTP	passer	Network_in
7	IN_VERS_SMTP	passer	Network_in

Filtrage des trafics sortants

Règle à configurer

Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en http et HTTPS, sauf sur les sites de l'Iran (test avec www.visitiran.ir).

👉 17 – Créer un séparateur pour cette règle. Vous le nommerez "Trafic_sortant".

✂ 18 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Autoriser_http	Pass	Network_in	Internet	http	-----	IPS
ON	Autoriser_https	pass	Network_in	Internet	https	-----	IPS
ON	Bloquer_Iran	block	Network_in	Internet geolocalisation Iran	http https	-----	IPS

✂ 19 – Dans quel ordre faut-il classer ces règles ?

On commence toujours par la plus restrictive puis après les moins restrictives. Donc filtrage de l'internet Iranien en premier.

Règle à configurer

L'accès au site <https://www.cnn.com> doit être bloqué depuis le réseau interne.
Pour cela utilisez un objet FQDN (Fully Qualifie Domain Name).

C'est quoi un objet FQDN ?

Un objet FQDN est utilisé pour identifier un hôte ou un service sur Internet par son nom de domaine complet plutôt que par son adresse IP. Cela permet de créer des règles de filtrage basées sur des noms de domaine plutôt que sur des adresses IP statiques, ce qui peut être utile pour gérer l'accès à des services dont les adresses IP peuvent changer dynamiquement.

NB : L'objet FQDN peut mettre un certain temps (plus de 5 minutes) à être totalement opérationnel.

✂ 20 – Complétez le tableau suivant pour configurer la règle.

CRÉER UN OBJET

Créez un FQDN (Menu Objet)

Ecrire www.cnn.com dans le nom de l'objet puis effectuer une recherche pour obtenir l'adresse IP.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Bloquer_CNN	block	Network_in	FQDN www.cnn.com	http https	-----	IPS

Règle à configurer

Votre réseau interne doit pouvoir joindre les serveurs FTP d'Internet.
Votre réseau interne doit pouvoir émettre un ping (protocole icmp) vers n'importe quelle destination.

✂ 21 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	IN_vers_ftp_internet	pass	Network_in	Internet	ftp	-----	IPS
ON	Autoriser_ping	pass	Network_in	any	any	icmp	IPS

Règle à configurer

L'accès à ChatGPT doit être interdit depuis le réseau interne. Pour cela, utilisez un service Web.

✂ 22 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Blocage_ChatGPT	block	Network_in	Web services and IP ChatGPT	http https	-----	IPS

Règle à configurer

Seul votre serveur DNS interne (172.16.1.10) peut envoyer des requêtes DNS vers l'extérieur.

Votre serveur de messagerie peut envoyer des mails en SMTP vers n'importe quel serveur de mail externe.

✂ 23 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	dns_vers_internet	pass	srv_dns	Internet	dns	-----	IPS
ON	Smtp_vers_Internet	pass	srv_mail	Internet	smtp	-----	IPS

Solution

FILTRAGE

NAT

Rechercher...

+ Nouvelle règle

X Supprimer

↑

↓

↕

↕

Couper

Copier

Coller

Chercher dans les logs

Chercher

		État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection
TRAFIC SORTANT (contient 9 règles, de 8 à 16)									
8		on	Bloquer_Iran	bloquer	Network_in	Internet Géolocalisation Iran	http https		IPS
9		on	Blocage_ChatGPT	bloquer	Network_in	Any Services Web et réputations ChatGPT	http https		IPS
10		on	19d67eee1dc_14	bloquer	Any	www.cnn.com	http https		IPS
11		on	Autoriser_http	passer	Network_in	Internet	http		IPS
12		on	Autoriser_https	passer	Network_in	Internet	https		IPS
13		on	IN_vers_FTP_internet	passer	Network_in	Internet	ftp		IPS
14		on	Autoriser_ping	passer	Network_in	Any	Any icmp (requête Echo (Ping))		IPS
15		on	dns_vers_internet	passer	srv_dns	Internet	dns		IPS
16		on	SMTP_vers_Internet	passer	srv_mail	Internet	smtp		IPS

Page

1

sur 1

Filtrage des trafics entrants

✂ 24 – Créer un séparateur pour cette règle. Vous le nommerez "Trafic_entrant".

Règle à configurer

Les réseaux externes peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés (trace dans le journal).

✂ 25 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Internet_vers_web	pass	Internet	Firewall_out	http	-----	IPS

ON	Internet_vers_ftp	pass	Internet	srv_ftp_pub	ftp	-----	IPS
----	-------------------	------	----------	-------------	-----	-------	-----

26 – Pourquoi la destination est "Firewall_out" ?

Le serveur web possède une adresse privée, on ne peut pas le joindre directement. Le seul hôte que l'on peut joindre depuis Internet est le port OUT du firewall. Ce sont les règles NAT de l'activité 4 qui permettront de traduire la trame vers le serveur WEB.

Règle à configurer

Les serveurs mail externes sont autorisés à transmettre des e-mails à votre serveur de messagerie.

27 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Internet_vers_smtp	pass	Internet	srv_mail_pub	smtp	-----	IPS

Règle à configurer

Les réseaux externes sont autorisés à ping l'interface « out » de votre firewall ; ce type d'événement doit lever une alarme mineure.

28 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	ping_depuis_Internet	pass	Internet	Firewall_out	any	icmp	IPS

Règle à configurer

Les réseaux externes peuvent se connecter à votre firewall : via l'interface web et en SSH. Ce type d'événement doit lever une alarme majeure.

29 – Complétez le tableau suivant pour configurer la règle.

Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	ssh_depuis_Internet	pass	Internet	Firewall_out	https ssh	-----	IPS

Solution

FILTRAGE

NAT

Rechercher...

+ Nouvelle règle

X Supprimer

↑ ↓ ↶ ↷

Couper

Copier

Coller

Chercher dans les logs

Chercher da

		État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection de :
TRAFIC ENTRANT (contient 5 règles, de 17 à 21)									
17		on	INTERNET_VERS_WEB	passer	Internet	Firewall_out	http		IPS
18		on	INTERNET_VERS_FTP	passer	Internet	srv_ftp_pub	ftp		IPS
19		on	INTERNET_VERS_SMTP	passer	Internet	srv_mail_pub	smtp		IPS
20		on	PING_DEPUIS_INTERN...	passer	Internet	Firewall_out	Any	icmp (requête Echo (Ping))	IPS
21		on	SSH_DEPUIS_INTERNET	passer	Internet	Firewall_out	https ssh		IPS

Test de votre politique de filtrage

Testez les règles concernant le trafic interne

- Vous devez pouvoir consulter le site web situé dans la DMZ depuis le réseau interne.
- Vous devez pouvoir consulter votre Webmail situé dans la DMZ depuis le réseau interne.
 - Serveur SMTP : **mail.a.net**
 - Accès au webmail : **http://172.16.1.11:808**
 - Utilisateur : **user**
 - Mot de passe : **user**
 - Adresses email : user@a.net
- Vous ne testerez pas le PC du stagiaire.
- Retrouvez les traces de votre navigation et les règles qui ont été activées dans l'onglet "Monitoring".

Testez les règles concernant le trafic sortant

- Vérifiez que vous pouvez accéder à Internet en http ou https.
- Vérifiez que vous ne pouvez pas accéder sur les sites de l'Iran (test avec www.visitiran.ir).
- Vérifiez que l'accès au site <https://www.cnn.com> est bloqué depuis le réseau interne.
- Vérifiez que vous ne pouvez pas accéder au service web ChatGPT.
- Vérifiez que vous pouvez émettre un ping vers l'extérieur de votre réseau depuis le réseau interne.
- Retrouvez les traces de votre navigation et les règles qui ont été activées dans l'onglet "Monitoring".

Testez les règles concernant le trafic entrant

- Les réseaux externes peuvent joindre votre serveur Web.
- Connectez-vous au Webmail et envoyez-vous un mail sur votre messagerie (GMAIL, Outlook, ...)
- Les réseaux externes sont autorisés à pinguer l'interface « out » de votre firewall
- Les réseaux externes peuvent se connecter à votre firewall : via l'interface web et en SSH. Pour autoriser un hôte à se connecter à votre firewall via l'interface web, il faut ajouter son adresse IP publique dans "**Accès aux pages d'administration du firewall** du menu **Système => Configuration => onglet Administration du firewall** (pas d'alarme pour ce flux spécifique, donc).
- Retrouvez les traces de votre navigation et les règles qui ont été activées dans l'onglet "Monitoring".