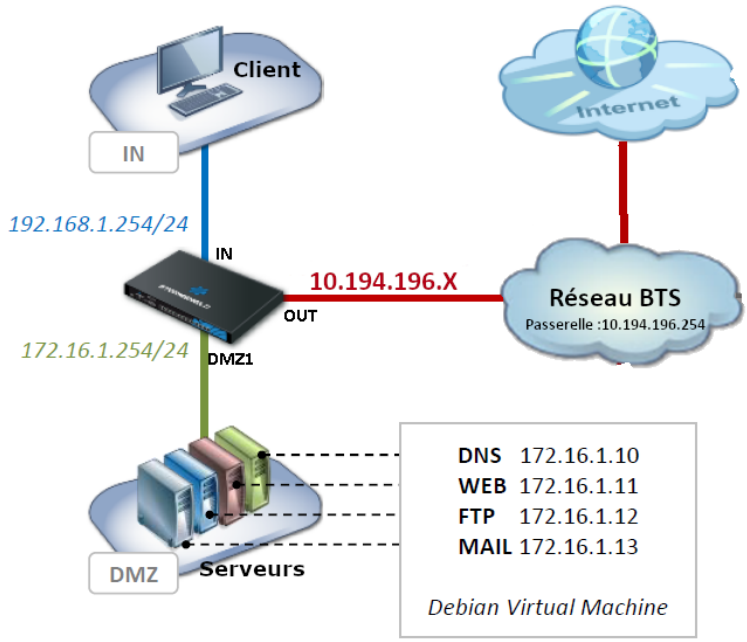
Activité 5 - Stormshield
Filtrage

Lors de l'activité 4 vous avez configurez 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 configurez 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 antivirale, 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

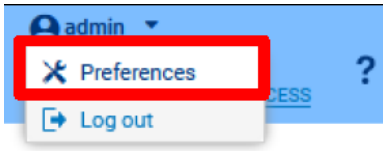
Le filtrage implicite
Regroupe les règles de filtrage préconfigurées ou ajoutées dynamiquement par le firewall pour autoriser ou bloquer certains flux après l'activation d'un service.
Les règles implicites sont accessibles depuis le menu **CONFIGURATION ⇒ POLITIQUE DE SÉCURITÉ ⇒ Règles implicites**. 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.

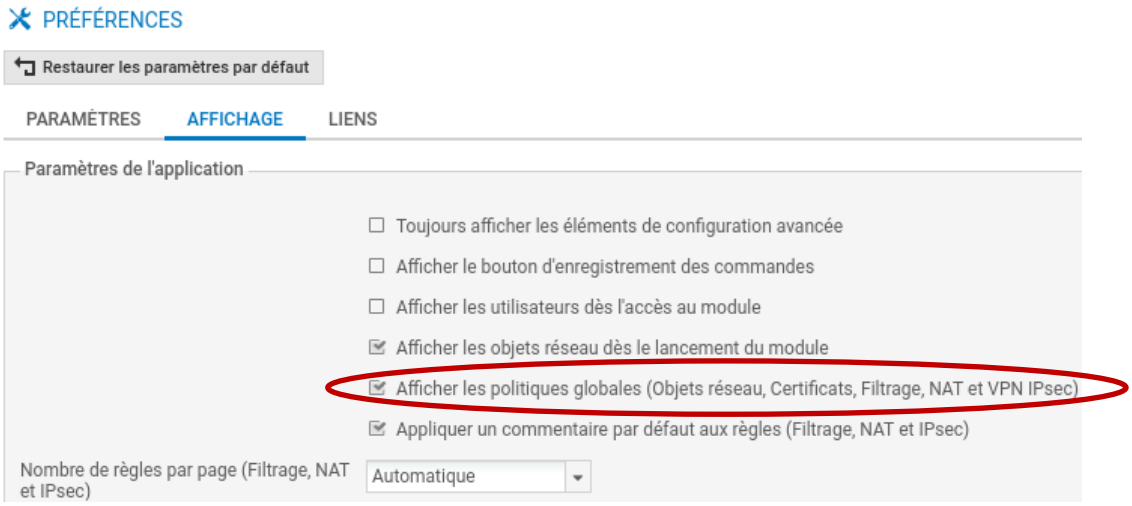
Le filtrage global
Regroupe les règles de filtrage injectées au firewall depuis l'outil d'administration « Stormshield Management Server » (SMC) ou après affichage des politiques globales. Permet la gestion du filtrage sur un réseaux multisites : réseau constitué de plusieurs réseaux et pares-feux Stormshield.
Vous ne modifierez pas ces règles lors de cette activité.

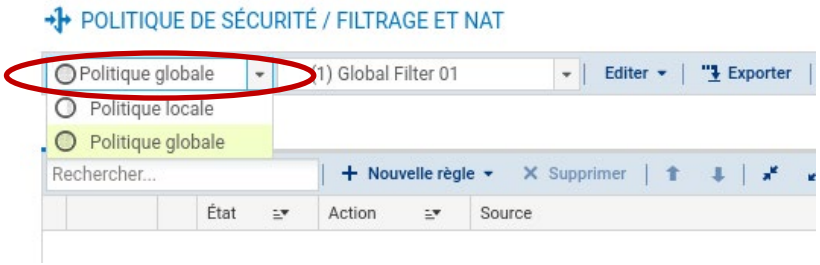
Le filtrage local : Représente les règles de filtrage ajoutées par l'administrateur (donc vous) depuis l'interface d'administration. C'est ce type de règles que vous allez mettre en œuvre sur le firewall.

☞ 2 – Affichez les règles globales



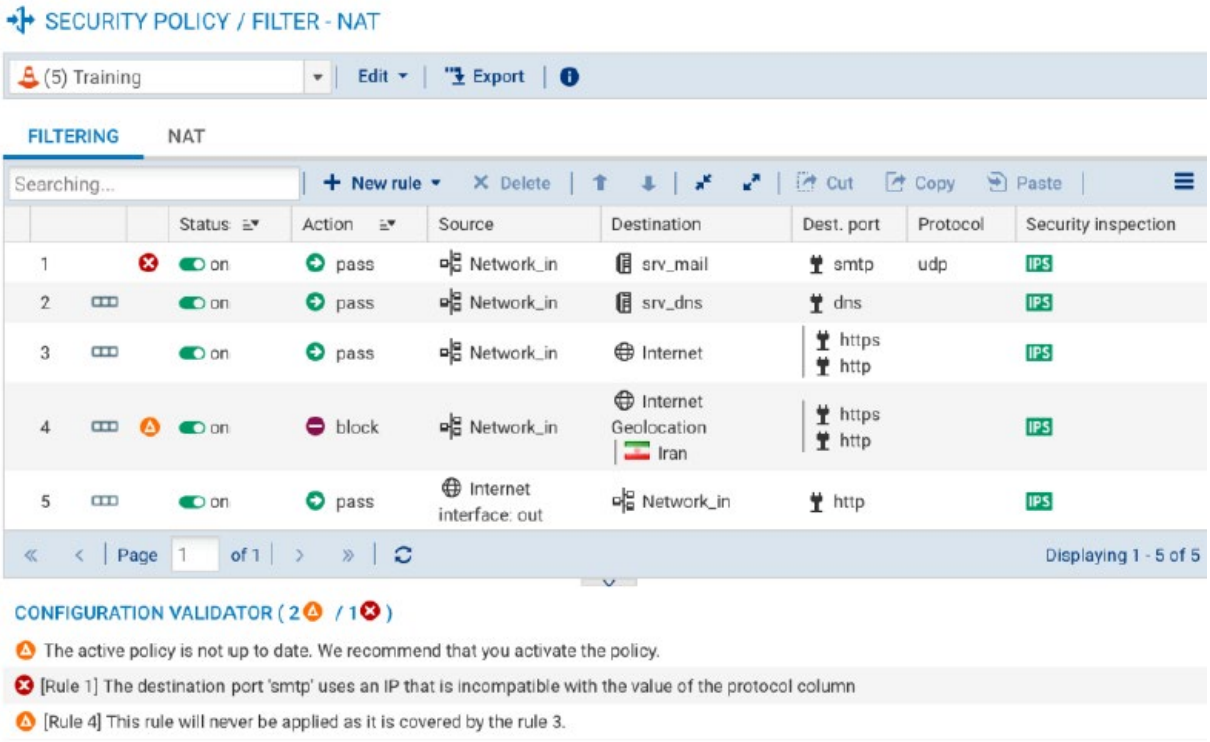
Pour afficher les règles globales, il faut cocher l'option **Afficher les politiques globales (Filtrage, NAT, VPN IPsec et Objets)** dans le menu **Préférences -->** Onglet **affichage.**





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.



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 defaut).
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 pas 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				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				dns	----------	

✍ 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				http	----------	

✍ 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				webmail	HTTP	

✍ 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				ftp	----------	

✍ 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				smtp	----------	

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				ftp	----------	

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

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_htttp					----------	
ON	Autoriser_htttps					----------	
ON	Bloquer_Iran					----------	

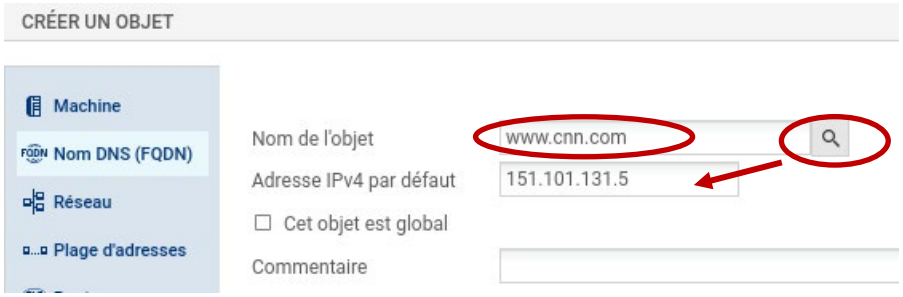
✍ 19 – Dans quel ordre faut-il classer ces règles ?

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 FDQN peut mettre un certain temps (plus de 5 minutes) à être totalement opérationnel.

20 – Complétez le tableau suivant pour configurer la règle.



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					----------	

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					----------	
ON	Autoriser_ping						

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					----------	

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					----------	
ON	Smtp_vers_Internet					----------	

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			**Firewall_out**		----------	
ON	Internet_vers_ftp			**srv_ftp_pub**		----------	

✍ 26 – Pourquoi la destination est "**Firewall_out**" ?

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			**srv_mail_pub**		----------	

Règle à configurer
Les réseaux externes sont autorisés à pinger 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					**icmp**	

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					----------	

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".