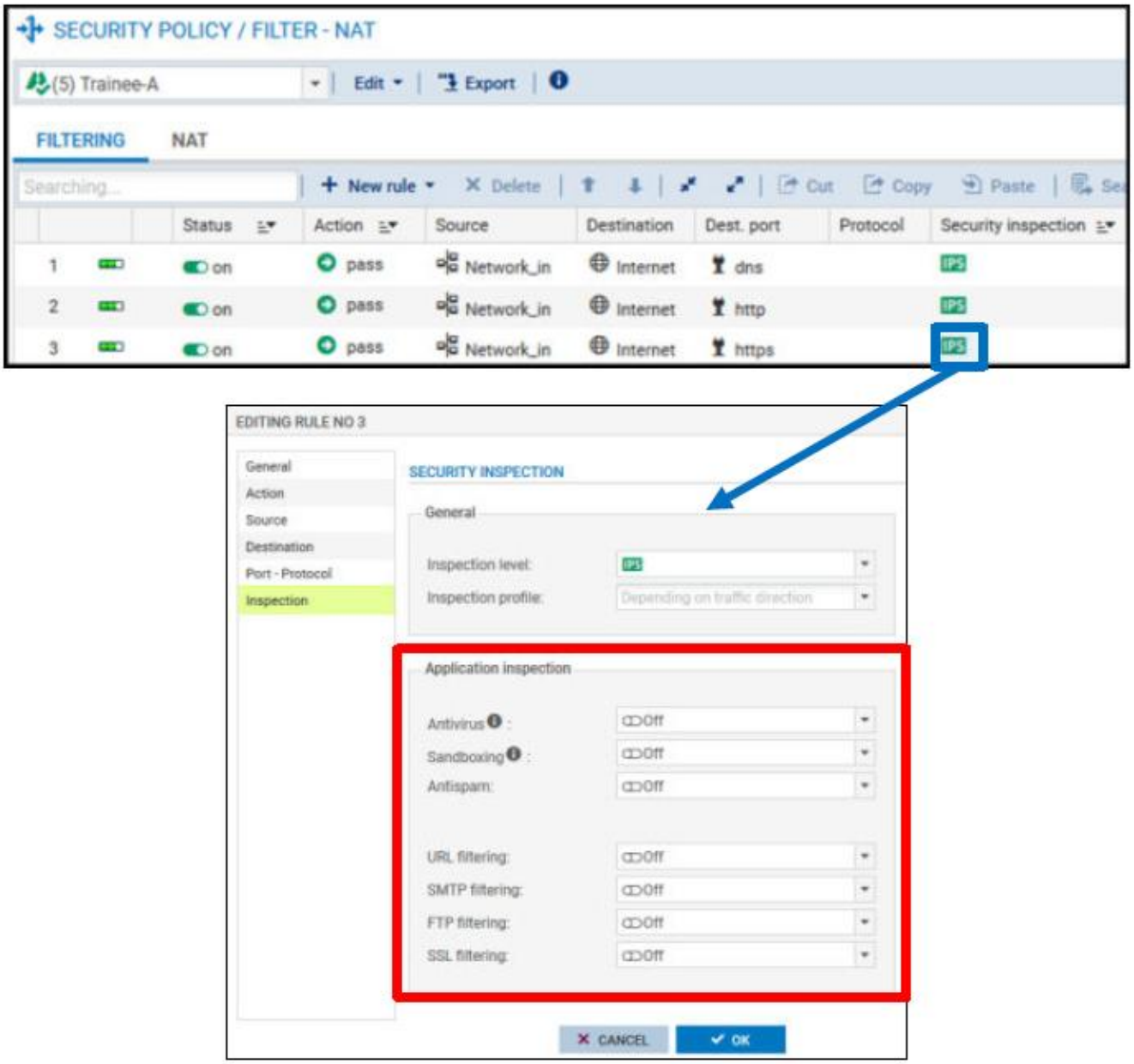
Activité 6 - Stormshield
Filtrage de contenu (http – https)

Votre objectif

Les objectifs de l'activité :

- Contrôler les accès aux sites web d'Internet (filtrage d'URL et filtrage SSL).
- Effectuer une analyse antivirale sur les flux DATA (HTTP, SMTP, FTP, POP3, …)

Notion de "proxy transparent"



Le filtrage de contenu (antivirus, antispam, filtrage d'URL, …) nécessite l'activation d'une inspection applicative (encadré rouge) sur une règle de filtrage du pare-feu (encadré bleu).
Cela provoque le passage en mode "proxy transparent".

Proxy transparent :

- Le firewall se fait passer pour le client auprès du serveur.
- Le firewall se fait passer pour le serveur auprès du client.
- La configuration du poste client n'est pas modifiée (c'est le principe du mode transparent), par exemple, le port d'écoute et l'adresse IP du Proxy n'ont pas à être configurés sur son navigateur Internet.

Contrôler les accès aux sites web d'Internet en http

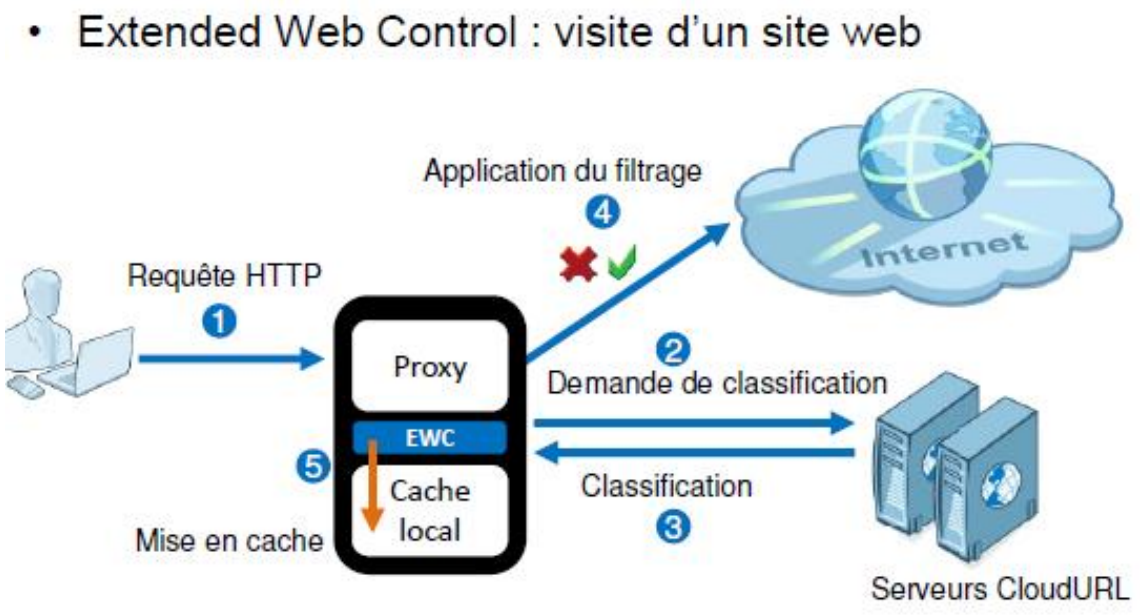
La fonction de filtrage des URL permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Elle est basée sur la consultation d'une "**base URL**" organisée en catégories ou en mot clés personnalisés.

Deux solutions possibles :

- 1 - Base URL embarquée composée de 16 catégories. Cette base est sauvegardée sur le firewall. Cette solution est comprise dans le prix de votre licence.

- 2 - Base Extended Web Control (EWC) constituée de 78 catégories, toutes hébergées dans le Cloud. L'avantage majeur est que la base de données n'est pas téléchargée, ce qui permet d'éviter la saturation de l'espace disque alloué au stockage de la base.
Il s'agit d'une option payante, elle n'est pas intégrée par défaut sur le firewall.

Principe de la solution EWC (Extended Web Control)



1 --> Un utilisateur envoie une requête http (URL) à destination d'un site web sur Internet. Le proxy transparent intercepte la requête.

2 --> Le firewall envoie une requête vers un serveur Extended Web Control (EWC) afin de recenser les catégories auxquelles appartient l'URL visitée.

3 --> Le serveur EWC peut renvoyer jusqu'à 5 catégories par URL.

4 --> Par conséquent, une URL peut se trouver simultanément dans une catégorie bloquée et une catégorie autorisée. Dans ce cas, c'est l'ordre des règles de filtrage URL qui prime. Il est très important de bien ordonnancer les règles de filtrage URL.

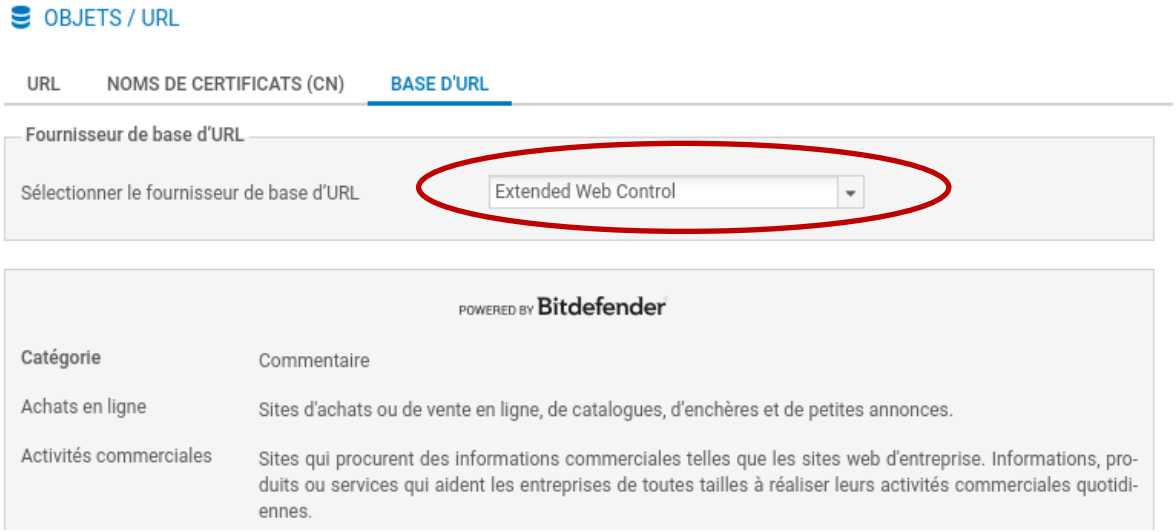
5 --> Afin d'optimiser le fonctionnement et éviter l'envoi de plusieurs requêtes vers le serveur EWC, le firewall utilise un cache. Lorsqu'une requête HTTP est interceptée, le proxy interroge tout d'abord le cache local. Si l'URL n'est pas présente, une requête est alors envoyée au serveur EWC pour connaître les catégories incluant cette URL.
Le cache est mis à jour pour conserver la décision appliquée à l'URL. La taille du cache est dimensionnée pour conserver 1 jour de navigation.

Cette solution payante est incluse (gratuitement) dans la licence du pare-feu virtuel que vous utilisez. Dans ce cas, nous utiliserons la base EWC pour la suite du TP.

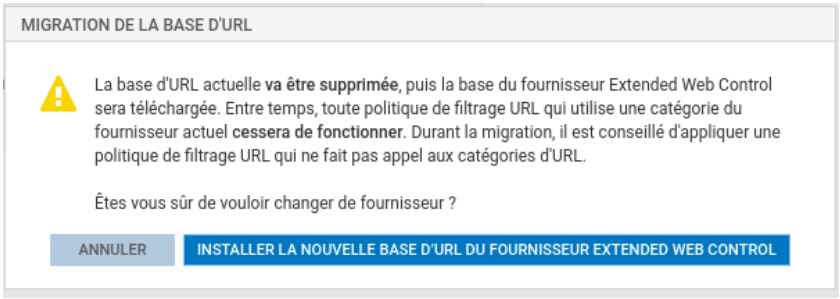
Mise en place de la solution "Base EWC"

☞ 1 – Copiez la politique de filtrage/NAT **(5) Activite_5** vers la politique numéro 6. Renommez la politique "**Activite_6**", puis activez cette politique (bouton "**Appliquer**" en bas de la page).

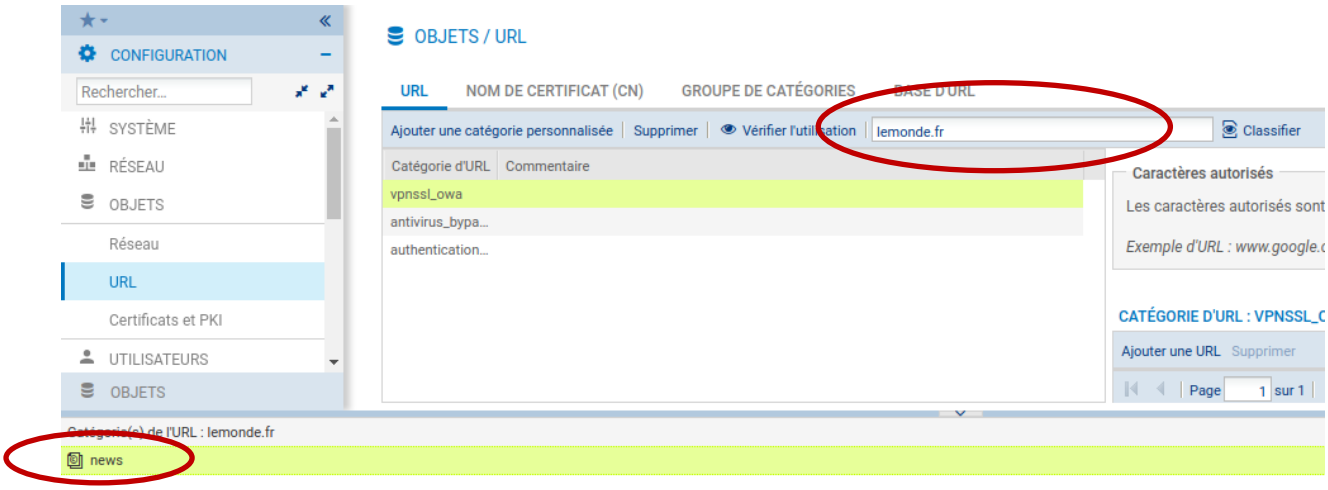
☞ 2 – Vérifiez que vous avez bien sélectionné la "Base Extended Web Control". Le choix de la base s'effectue depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **BASE D'URL**.



Le passage de la base d'URL embarquée à EWC entraîne la suppression des catégories embarquées ; cela vous est notifié par un message d'avertissement. Validez l'installation de la nouvelle base.



✍ 3 – Trouvez les catégories dans lesquelles sont classées les URL : lemonde.fr, mozilla.org, github.com, youtube.com et mes-cours.fr.
Pour déterminer les catégories dans lesquelles les URL sont classées, rendez-vous dans le menu **URL** puis entrez ces valeurs dans le champ « **Vérifier la classification d'une URL** ».



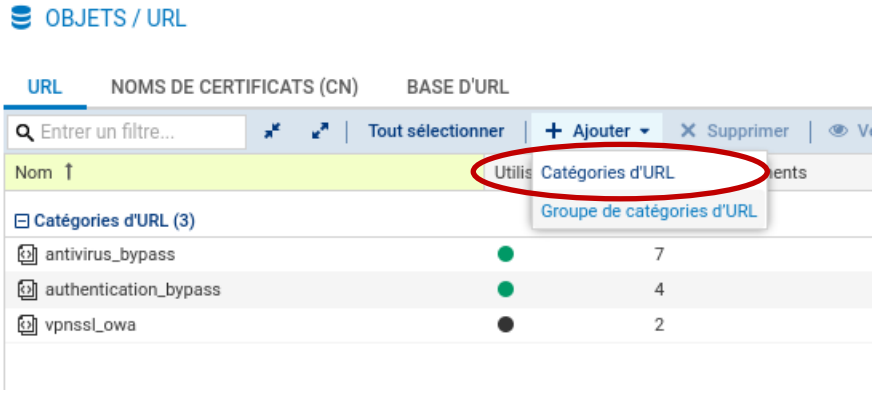
Depuis la dernière version, ce module de vérification ne fonctionne pas correctement. Testez-le et essayez de compléter le tableau suivant.

URL	Catégorie
lemonde.fr	news
mozilla.org	IT
github.com	IT
youtube.com	
mes-cours.fr	Pas référencée

Votre objectif (Questions 4 à 9)
Création d'une catégorie "blacklist" et ajout d'une liste de site à bloquer. On bloquera les sites appartenant aux catégorie "News" et "onlineshop". Faites une exception afin que le site lemonde.fr et ses sous-domaines restent joignables.

Il est possible d'ajouter d'autres catégories. Depuis le menu **CONFIGURATION** ⇒ **OBJETS** ⇒ **URL**, dans l'onglet **URL**, vous pouvez créer vos propres catégories. Par définition, une catégorie contient une liste d'URL.

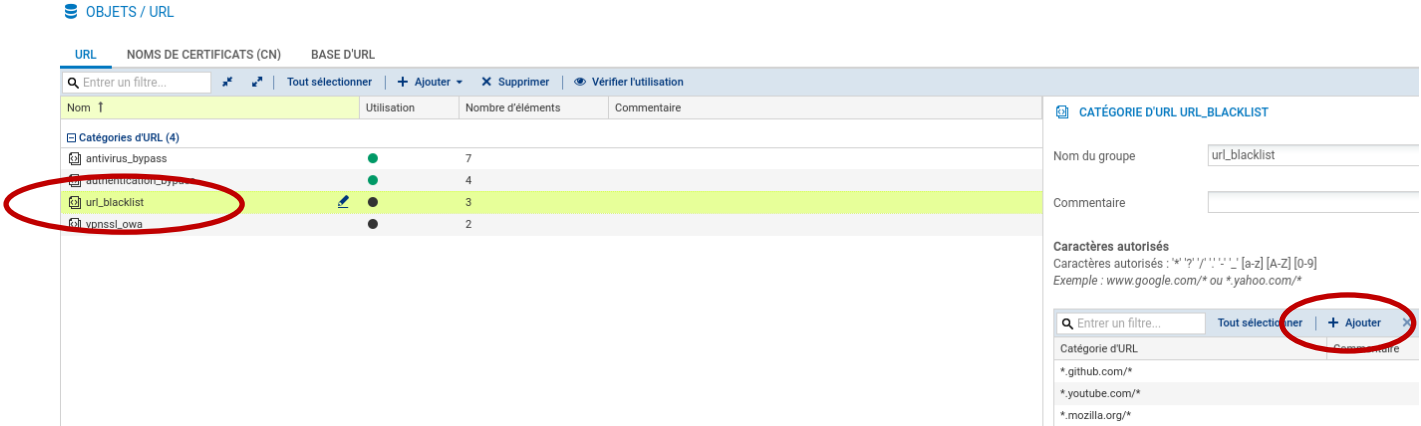
☞ 4 – Commencez par réer une catégorie personnalisée nommée "**url_blacklist**"



✍ 5 – Avant d'ajouter des URL à cette liste, il faut vérifier si elle n'est pas inscrite dans une autre catégorie. Vérifiez pour : github.com, youtube.com et mozilla.org. Que constatez-vous ?

> **A actualiser** L'url netbsd.org est déjà présente dans la liste "IT". Si on l'ajoute à "blacklist" il faudra faire attention à l'ordre des règles. Une url peut être présente dans 5 catégories au maximum. Au-delà, le firewall n'affiche pas les autres catégories.

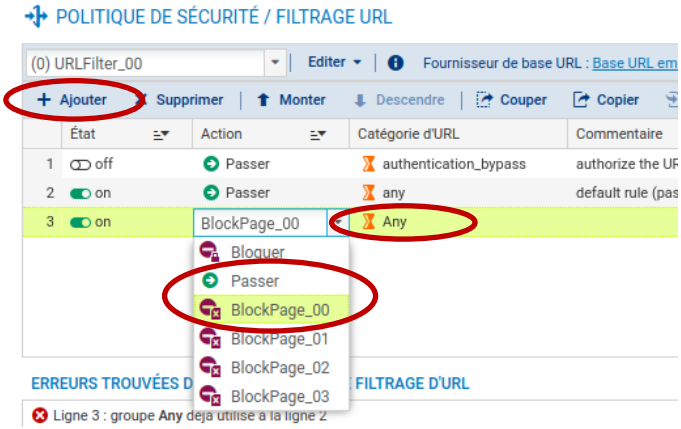
☞ 6 – Ajoutez à la liste "url_blacklist" : *.github.com/*, *.youtube.com/* et *.mozilla.org.org/*.
Pour agir sur toutes les url des domaines " github.com " on ajoute un * qui remplace toutes les chaines de caractère existantes.
Pour ajouter une url, sélectionnez la catégorie puis cliquez sur "**Ajouter une URL**".



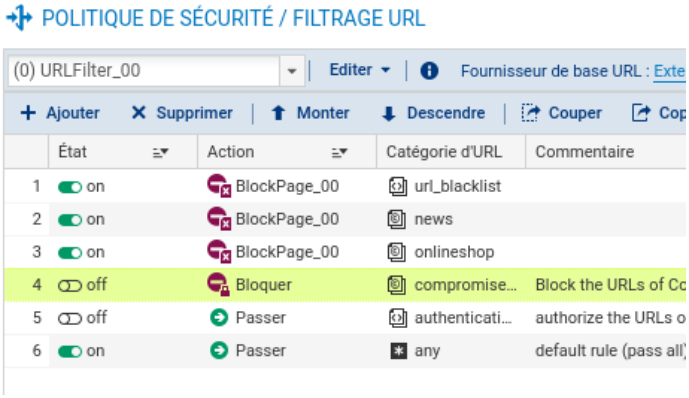
☞ 7 – Vous venez de définir une catégorie avec des url associées mais il faut maintenant préciser au firewall si vous souhaitez interdire ou autoriser cette catégorie. On appelle cela le filtrage d'URL.
Rendez-vous dans le menu **Configuration** => **Politique de sécurité** => **Filtrage URL** => **slot URLFilter_00**.

☞ 8 – Ajoutez les règles nécessaires pour autoriser (**passer**) toutes les catégories sauf "url_blacklist", "news" et "onlineshop". Attention à l'ordre des règles, n'oubliez pas que "github.com" doit être bloqué alors qu'il se trouve à la fois dans une catégorie autorisée et une interdite.

Pour ajouter une règle, cliquez sur ajouter puis sélectionnez "**Passer**" ou "**BlockPage_00**". Choisissez ensuite la catégorie à filtrer dans la colonne "**catégorie d'URL**".



Solution :

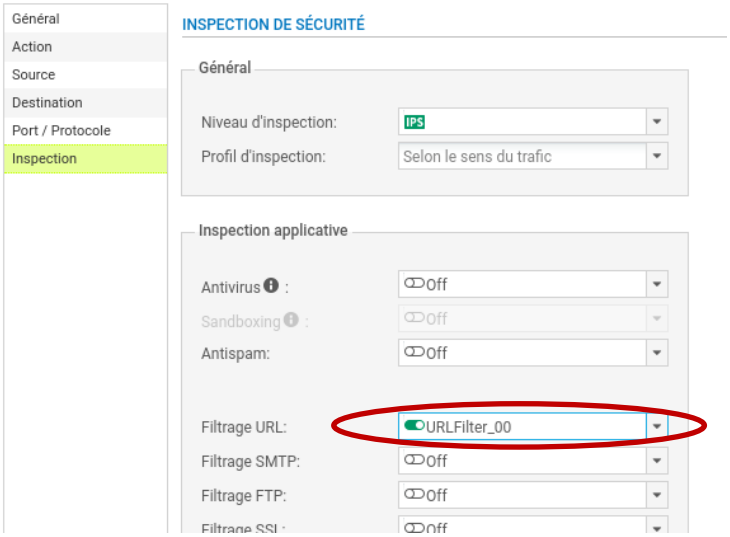


☞ 9 – Lors de l'activité 5 (Filtrage) question 18, vous avez mis en place cette règle :

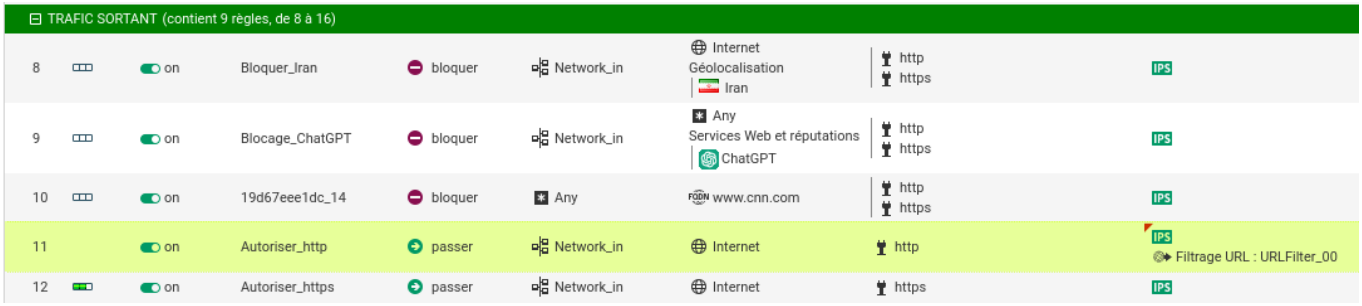
Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Autoriser_htttp	Pass	Network_in	Internet	http	----------	IPS

Elle autorise le trafic web http du réseau interne vers Internet. Or on souhaite bloquer certaines catégories : news, onlineshop et blacklist.

Vous allez devoir modifier le champ sécurité "IPS". Pour modifier ce champ, retournez dans le menu **configuration** => **politique de sécurité** => **filtrage et NA**T et double cliquez sur "IPS" de la règle "Autoriser_http".
Sélectionnez la politique de sécurité "**URLFilter_00**" pour le filtrage URL.



Solution



Bilan

Vous venez de mettre en place une politique de sécurité pour les sites web en http :

- Blocage des sites web de la catégorie "**news**".
- Blocage des sites web de la catégorie "**onlineshop**".
- Blocage des sites web de la catégorie "**blacklist**".
- Tous les autres sites web http sont autorisés.

Dans le chapitre suivant, vous aller devoir mettre en place la politique de sécurité pour les sites en https.

Contrôler les accès aux sites web d'Internet en https

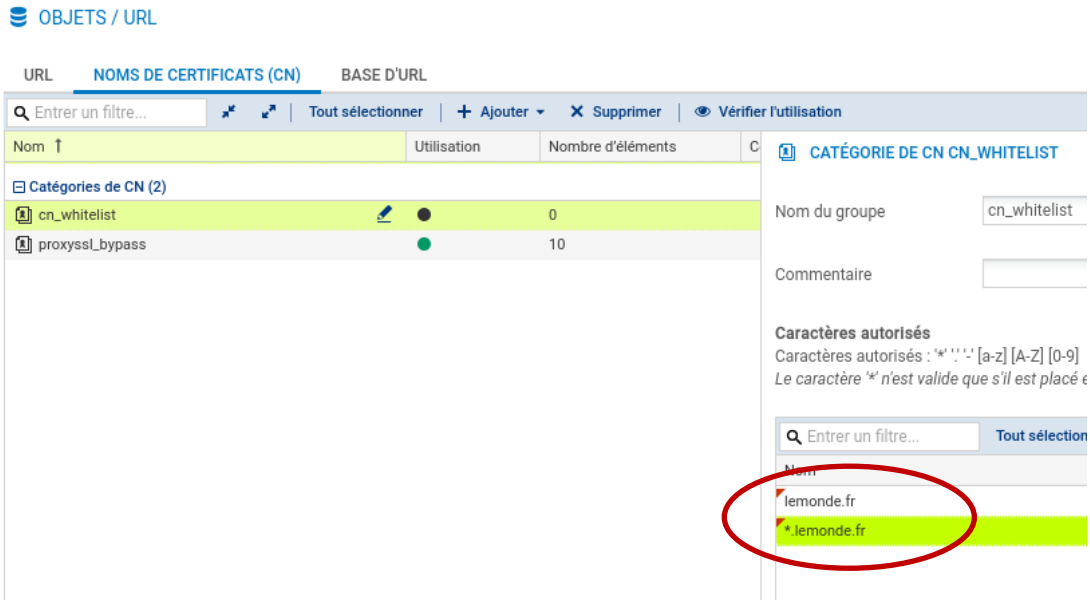
Pour les sites en https, il faut gérer les Certificats Numériques (protocole SSL).

Travail à faire (Q10 à Q16)

Configurez une politique de filtrage SSL, permettant l'accès à tous les sites Web (https) sauf les sites des catégories "onlineshop" et "news".
Cependant, assurez-vous que le site **lemonde.fr** (catégorie **news**) reste joignable et que les sites ***.mozilla.org, github.com** et***.youtube.com** soient bloqués.

☞ 10 – Commencez par créer une catégorie personnalisée de CN (Nom de Certificat) appelée "**cn_whitelist**" dans le menu **Configuration** => **Objets** => **URL** => onglet **Nom de certificat (CN)**.

☞ 11 – Ajouter dans " **cn_whitelist** " les certificats numériques des sites du "le monde" : lemonde.fr et *.lemonde.fr.



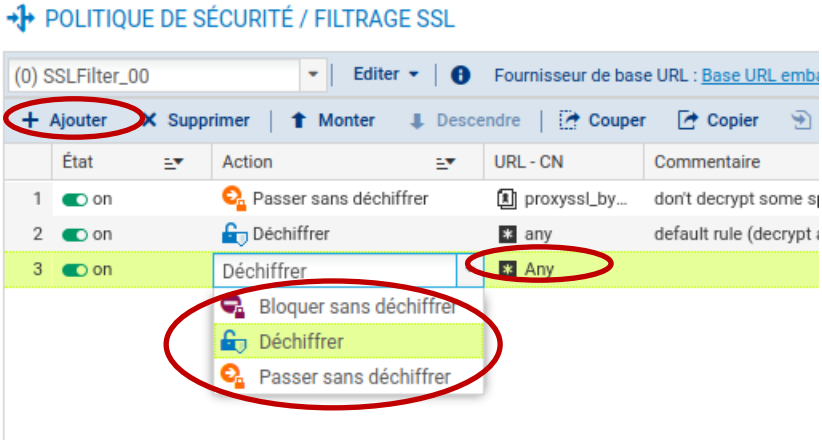
☞ 12 –Créez une autre catégorie personnalisée de CN (Nom de Certificat) appelée "**cn_blacklist**" dans le menu **Configuration** => **Objets** => **URL** => onglet **Nom de certificat (CN)**.

☞ 13 – Ajouter dans " **cn_blacklist** " les certificats numériques des sites : mozilla.org, *.mozilla.org, youtube.com, *.youtube.com, github.com et *.github.com.

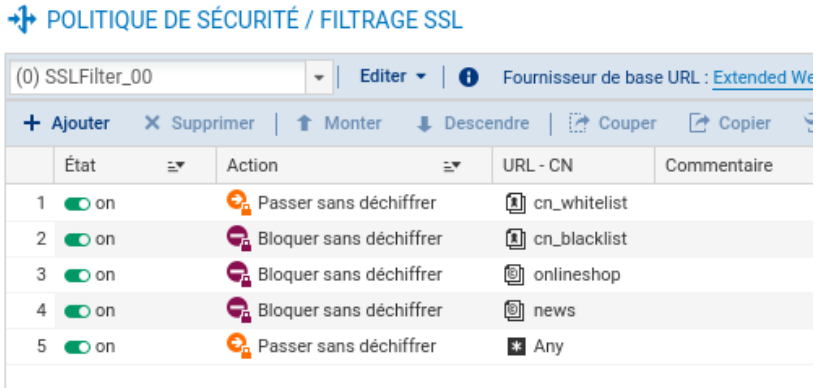
☞ 14 – Vous venez de définir une catégorie avec des CN (Certificats Numériques) associées mais il faut maintenant préciser au firewall si vous souhaitez interdire ou autoriser cette catégorie.
Rendez-vous dans le menu **Configuration** => **Politique de sécurité** => **Filtrage SSL** => **slot SSLFilter_00**.

☞ 15 – Ajoutez les règles nécessaires pour autoriser (**passer**) toutes les catégories sauf " **cn_blacklist** ", "news" et "onlineshop". Attention à l'ordre des règles, positionner correctement la catégorie " **cn_whitelist** ".

Pour ajouter une règle, cliquez sur ajouter puis sélectionnez "**Passer sans déchiffer**" ou "**Bloquer sans déchiffrer**". Choisissez ensuite la catégorie à filtrer dans la colonne "**URL - CN**".



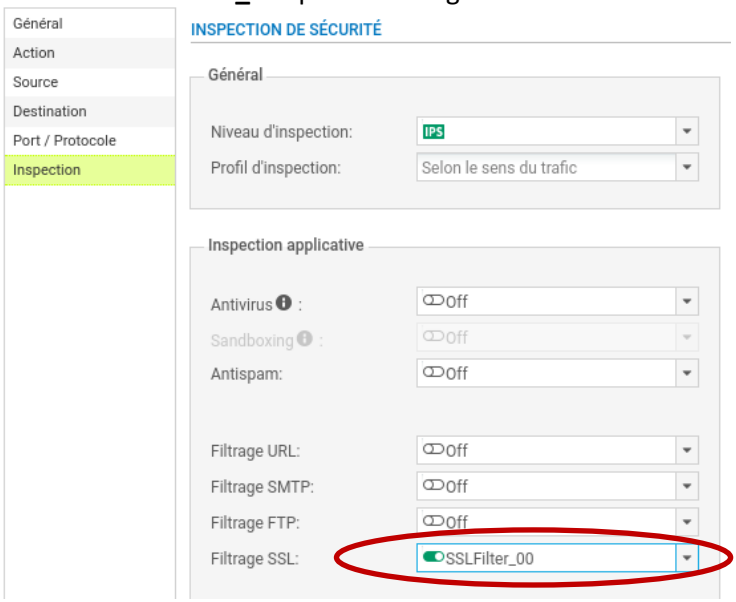
Solution

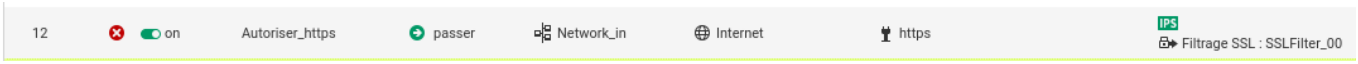


☞ 16 – Lors de l'activité 5 (Filtrage) question 18, vous avez mis en place cette règle :

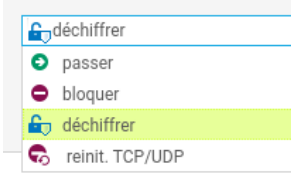
Status	Nom	Action	Source	Destination	Port dest.	Protocole	Sécurité
ON	Autoriser_htttps	Pass	Network_in	Internet	https	----------	IPS

Elle autorise le trafic web **https** du réseau interne vers Internet. Or on souhaite bloquer certaines catégories (news, onlineshop et cn_blacklist).
Vous allez devoir modifier le champ sécurité "IPS" dans le menu **configuration** => **politique de sécurité** => **filtrage et NA**T et double cliquez sur "IPS" de la règle "Autoriser_https".
Sélectionnez la politique de sécurité "**SSLFilter_00**" pour le filtrage SSL.

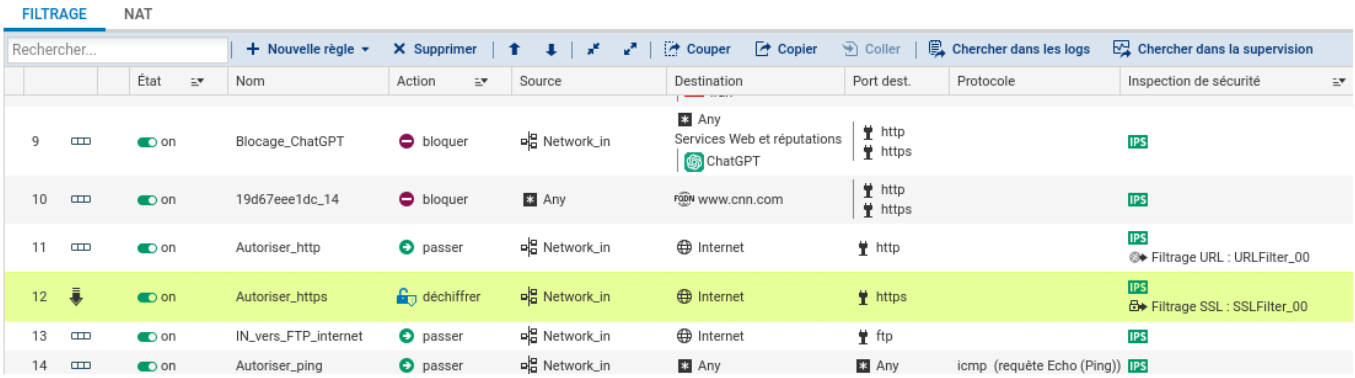




Attention : Cette règle ne peut pas être utilisée si l'option "passer" est activée. Il faut la remplacer par "Déchiffrer".



Solution



Bilan

Vous venez de mettre en place une politique de sécurité pour les sites web en **https** :

- Blocage des sites web de la catégorie "**news**".
- Blocage des sites web de la catégorie "**shopping**".
- Blocage des sites web de la catégorie "**cnblacklist**".
- Autorisation des sites web de la catégorie "**cnwhitelist**".
- Tous les autres sites web **https** sont autoriser.

Testez le firewall

Pour les tests suivants vous vous connecterez en http puis après en https.

18 – Tentez d'accéder au site **cnn.com**. Que constatez-vous ? Est-ce correct ?

Le site est bloqué en http et en https. Cela correspond à une des règles mise en place lors de l'activité 5. Fonctionnement correct du firewall. Cette règle n'est plus nécessaire car le site est aussi filtré par la catégorie new.

19 – Tentez d'accéder au site **euronews.com**. Que constatez-vous ? Est-ce correct ?

Le site est bloqué en http et en https. Cela correspond à la politique de sécurité mise en place pour filtrer la catégorie "news" en http et en https.
Fonctionnement correct du firewall.

20 – Tentez d'accéder au site **lemonde.fr**. Que constatez-vous ? Est-ce correct ?

Le site n'est pas bloqué en http et en https. Cela correspond à la politique de sécurité mise en place pour filtrer la catégorie "cn_whitelist" et aussi "news" en http et en https. "cn_whitelist" autorise le site mais "news" le bloque. Comme la règle sur "cn_whitelist" apparait en premier alors le site sera autorisé.
Fonctionnement correct du firewall.

21 – Tentez d'accéder au site **youtube.com**. Que constatez-vous ? Est-ce correct ?

Le site est bloqué en http et en https. Cela correspond à la politique de sécurité mise en place pour filtrer les catégories "cn_blacklist" et "news" en http et en https. La règle " cn_blacklist " arrivant en premier, c'est elle qui validera le blocage.
Fonctionnement correct du firewall.

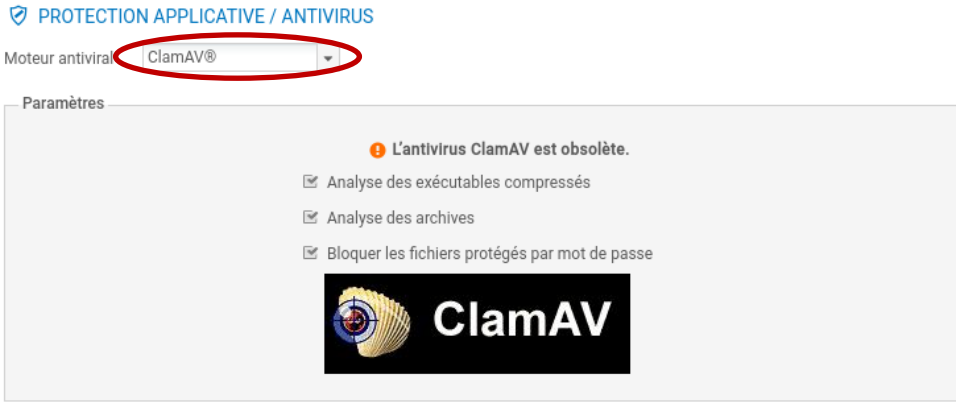
22 – Cliquez sur l'onglet "monitoring" et observez les différents journaux. Vous devriez retrouver les alarmes par rapport aux sites bloqués.

Analyse antivirale

L'analyse antivirale des fichiers n'est possible que sur les protocoles suivants : http, https, smtp, ftp ou pop3.
Vous disposez de deux solutions antivirales :

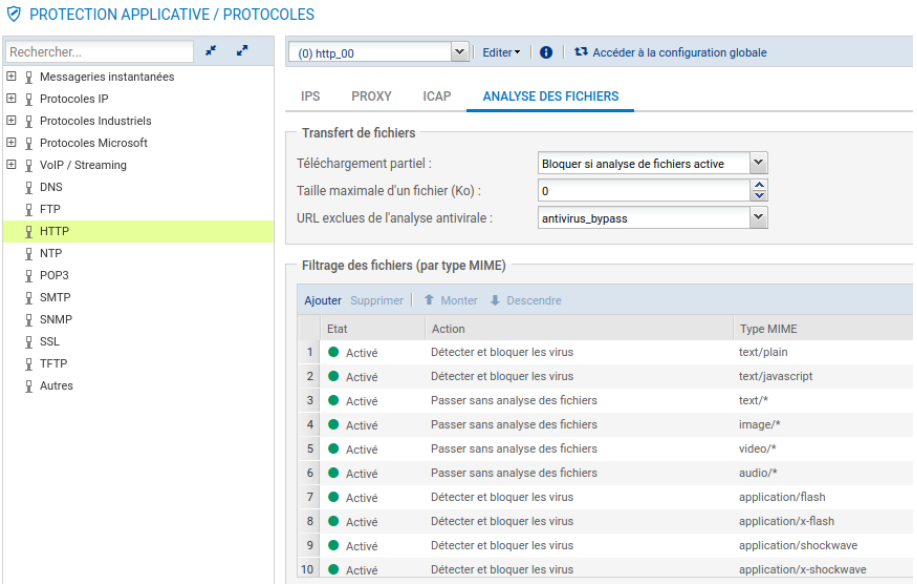
- ClamAV : Ce moteur antiviral est intégré gratuitement et par défaut.
- Antivirus avancé (payant) : Il est nécessaire de souscrire à un pack de sécurité incluant cette option.

☞ 23 – Depuis le menu **CONFIGURATION** ⇒**PROTECTION APPLICATIVE** ⇒ **Antivirus** vous sélectionnerez la solution antivirale gratuite **"ClamAV"**.

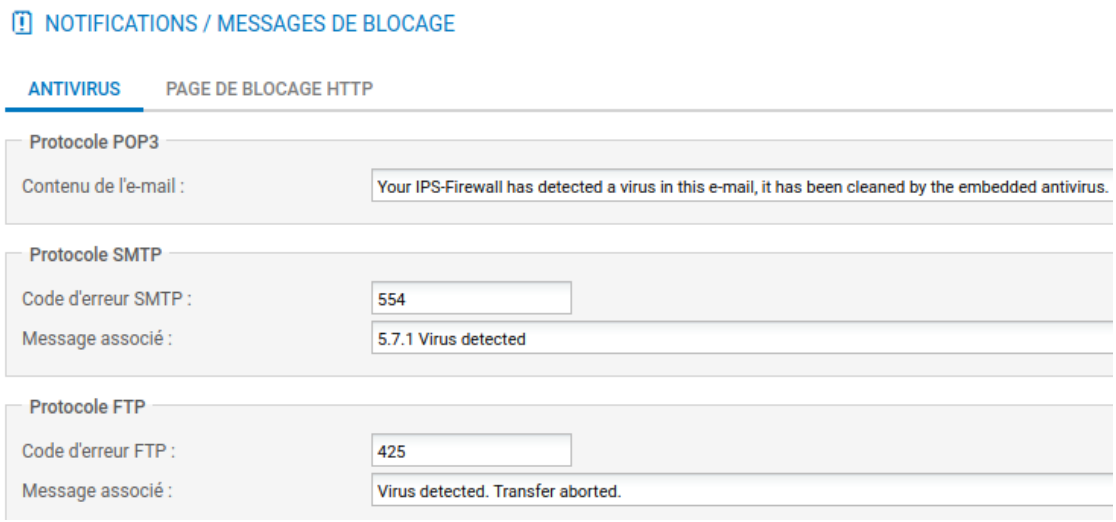


Vous pouvez constater que cette version est obsolète donc revenez sur la version antivirus avancée.

☞ 24 – Vous trouverez des paramètres additionnels à appliquer aux protocoles pouvant être soumis à une analyse antivirale (voir le menu **CONFIGURATION** ⇒ **PROTECTION APPLICATIVE** ⇒ **Protocoles** ⇒ **HTTP, SMTP, FTP** ou **POP3** ⇒ **ANALYSE DES FICHIERS**). Ce menu contient la taille maximale pour l'analyse antivirale, les actions sur les messages. Vous laisserez les paramètres par défaut.



☞ 25 – Depuis le menu **CONFIGURATION** ⇒ **NOTIFICATIONS** ⇒ **Messages de blocage**, il est possible de modifier les notifications envoyées aux utilisateurs lorsqu'un mail ou un fichier téléchargé par FTP contient un virus. Mettez les messages en français.



☞ 26 – Activation de l'analyse antivirale

Les flux pouvant être analysés par le moteur antiviral sont :

- HTTP et HTTPS,
- FTP,
- SMTP et SMTPS,
- POP3 et POP3S.

Pour mettre en œuvre cette analyse, il suffit de sélectionner l'inspection applicative Antivirus dans la colonne inspection de sécurité (IPS) de la règle de filtrage concernée.

NOTE : Pour être soumis à une analyse antivirale les flux HTTPS, SMTPS et POP3S doivent au préalable être déchiffrés par une règle d'inspection SSL.