

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 antivirus sur les flux DATA (HTTP, SMTP, FTP, POP3, ...)

Notion de "proxy transparent"

SECURITY POLICY / FILTER - NAT

(5) Trainee-A | Edit | Export

FILTERING NAT

Searching...

+ New rule | X Delete | [Icons]

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Network_In	Internet	dns		IPS
2	on	pass	Network_In	Internet	http		IPS
3	on	pass	Network_In	Internet	https		IPS

EDITING RULE NO 3

General | Action | Source | Destination | Port - Protocol | Inspection

SECURITY INSPECTION

General

Inspection level: IPS

Inspection profile: Depending on traffic direction

Application inspection

Antivirus: Off

Sandboxing: Off

Antispam: Off

URL filtering: Off

SMTP filtering: Off

FTP filtering: Off

SSL filtering: Off

X CANCEL | OK

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

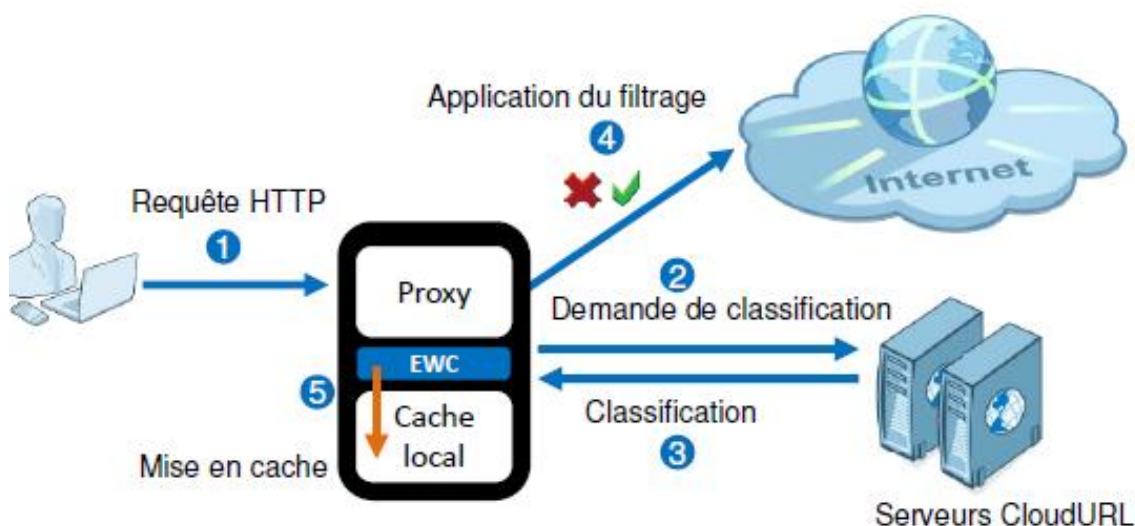
La fonction de filtrage des URL permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Elle est basée sur la consultation d'une "**base URL**" organisée en catégories ou en mots clés personnalisés.

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)

- Extended Web Control : visite d'un site web



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.

- 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**.

OBJETS / URL

URL
NOMS DE CERTIFICATS (CN)
BASE D'URL

Fournisseur de base d'URL

Sélectionner le fournisseur de base d'URL

Extended Web Control ▼

POWERED BY Bitdefender

Catégorie	Commentaire
Achats en ligne	Sites d'achats ou de vente en ligne, de catalogues, d'enchères et de petites annonces.
Activités commerciales	Sites qui procurent des informations commerciales telles que les sites web d'entreprise. Informations, produits ou services qui aident les entreprises de toutes tailles à réaliser leurs activités commerciales quotidiennes.

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.

MIGRATION DE LA BASE D'URL

La base d'URL actuelle va être supprimée, puis la base du fournisseur Extended Web Control sera téléchargée. Entre temps, toute politique de filtrage URL qui utilise une catégorie du fournisseur actuel cessera de fonctionner. Durant la migration, il est conseillé d'appliquer une politique de filtrage URL qui ne fait pas appel aux catégories d'URL.

Êtes vous sûr de vouloir changer de fournisseur ?

ANNULER
INSTALLER LA NOUVELLE BASE D'URL DU FOURNISSEUR EXTENDED WEB CONTROL

- 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** ».

CONFIGURATION

SYSTÈME

RÉSEAU

OBJETS

Réseau

URL

Certificats et PKI

UTILISATEURS

OBJETS

OBJETS / URL

URL
NOM DE CERTIFICAT (CN)
GROUPE DE CATÉGORIES
BASE D'URL

Ajouter une catégorie personnalisée
Supprimer
Vérifier l'utilisation

lemonde.fr

Classifier

Catégorie d'URL	Commentaire
vpnsLowa	
antivirus_bypa...	
authentication...	

Caractères autorisés

Les caractères autorisés sont

Exemple d'URL : www.google.c

CATÉGORIE D'URL : VPNSL_C

Ajouter une URL Supprimer

Page 1 sur 1

Catégorie(s) de l'URL : lemonde.fr

news

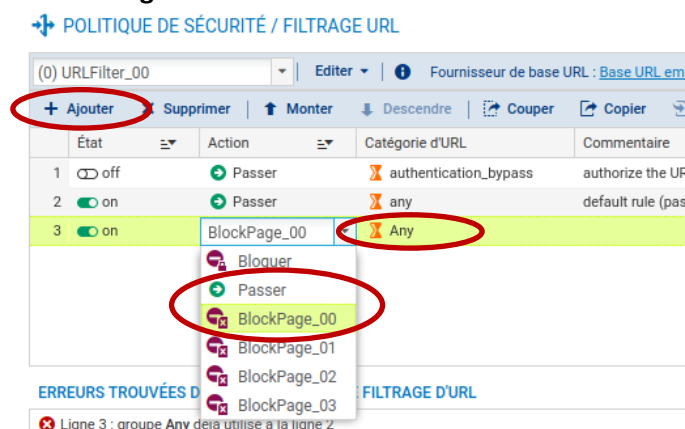
Depuis la dernière version, ce module de vérification ne fonctionne pas correctement. Testez-le et essayez de compléter le tableau suivant.

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 :

POLITIQUE DE SÉCURITÉ / FILTRAGE URL

État	Action	Catégorie d'URL	Commentaire
1 ☒ on	BlockPage_00	url_blacklist	
2 ☒ on	BlockPage_00	news	
3 ☒ on	BlockPage_00	onlineshop	
4 ☐ off	Bloquer	compromise...	Block the URLs of Co
5 ☐ off	Passer	authentificati...	authorize the URLs o
6 ☒ on	Passer	any	default rule (pass all,

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_http	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 NAT** et double cliquez sur "IPS" de la règle "Autoriser_http". Sélectionnez la politique de sécurité "**URLFilter_00**" pour le filtrage URL.

INSPECTION DE SÉCURITÉ

Général

Niveau d'inspection: **IPS**

Profil d'inspection: Selon le sens du trafic

Inspection applicative

Antivirus: Off

Sandboxing: Off

Antispam: Off

Filtrage URL: **URLFilter_00**

Filtrage SMTP: Off

Filtrage FTP: Off

Filtrage SSL: Off

Solution

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	Filtrage URL : URLFilter_00
12		on	Autoriser_https	passer	Network_in	Internet	https	IPS	

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 allez 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**.

URL **NOMS DE CERTIFICATS (CN)** BASE D'URL

Q Entrer un filtre... Tout sélectionner + Ajouter X Supprimer Vérifier l'utilisation

Nom ↑	Utilisation	Nombre d'éléments
Catégories de CN (2)		
cn_whitelist	●	0
proxysl_bypass	●	10

CATÉGORIE DE CN CN_WHITELIST

Nom du groupe: cn_whitelist

Commentaire:

Caractères autorisés
Caractères autorisés : '*' ':' '-' [a-z] [A-Z] [0-9]
Le caractère '*' n'est valide que s'il est placé en premier

Q Entrer un filtre... Tout sélectionner

Nom

lemonde.fr

*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 déchiffrer**" ou "**Bloquer sans déchiffrer**". Choisissez ensuite la catégorie à filtrer dans la colonne "**URL - CN**".

POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00 Editer Fournisseur de base URL : Base URL emb...

+ Ajouter X Supprimer Monter Descendre Couper Copier

	État	Action	URL - CN	Commentaire
1	on	Passer sans déchiffrer	proxysl_by...	don't decrypt some s
2	on	Déchiffrer	* any	default rule (decrypt
3	on	Déchiffrer	* Any	

Bloquer sans déchiffrer

Déchiffrer

Passer sans déchiffrer

Solution

(0) SSLFilter_00		Editer		Fournisseur de base URL : Extended We	
+ Ajouter ✕ Supprimer ↑ Monter ↓ Descendre ✂ Couper 📋 Copier					
	État	Action	URL - CN	Commentaire	
1	on	Passer sans déchiffrer	cn_whitelist		
2	on	Bloquer sans déchiffrer	cn_blacklist		
3	on	Bloquer sans déchiffrer	onlineshop		
4	on	Bloquer sans déchiffrer	news		
5	on	Passer sans déchiffrer	Any		

👉 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_https	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 NAT** et double cliquez sur "IPS" de la règle "Autoriser_https".

Sélectionnez la politique de sécurité "**SSLFilter_00**" pour le filtrage SSL.

Général
 Action
 Source
 Destination
 Port / Protocole
Inspection

INSPECTION DE SÉCURITÉ

Général

Niveau d'inspection: **IPS**

Profil d'inspection: Selon le sens du trafic

Inspection applicative

Antivirus : Off

Sandboxing : Off

Antispam: Off

Filtrage URL: Off

Filtrage SMTP: Off

Filtrage FTP: Off

Filtrage SSL: **SSLFilter_00**

12	✕ on	Autoriser_https	➡ passer	🌐 Network_in	🌐 Internet	🔒 https	IPS Filtrage SSL : SSLFilter_00
----	------	-----------------	----------	--------------	------------	---------	------------------------------------

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

- 🔒 déchiffrer
- ➡ passer
- 🚫 bloquer
- 🔒 déchiffrer
- 🔄 reinit. TCP/UDP

Solution

FILTAGE		NAT											
Rechercher...			+ Nouvelle règle ✕ Supprimer ↑ ↓ ↕ ↕ Couper Copier Coller Chercher dans les logs Chercher dans la supervision										
		État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité				
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 Filtrage URL : URLFilter_00				
12		on	Autoriser_https	déchiffrer	Network_in	Internet	https		IPS Filtrage SSL : SSLFilter_00				
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				

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.

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

- ClamAV : Ce moteur antivirus 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 antivirus gratuite "**ClamAV**".

PROTECTION APPLICATIVE / ANTIVIRUS

Moteur antivirus : ClamAV®

Paramètres

L'antivirus ClamAV est obsolète.

☒ Analyse des exécutables compressés

☒ Analyse des archives

☒ Bloquer les fichiers protégés par mot de passe



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 antivirus (voir le menu **CONFIGURATION** ⇒ **PROTECTION APPLICATIVE** ⇒ **Protocoles** ⇒ **HTTP, SMTP, FTP ou POP3** ⇒ **ANALYSE DES FICHIERS**). Ce menu contient la taille maximale pour l'analyse antivirus, les actions sur les messages. Vous laisserez les paramètres par défaut.

PROTECTION APPLICATIVE / PROTOCOLES

Rechercher...

(0) http_00

IPS PROXY ICAP **ANALYSE DES FICHIERS**

Transfert de fichiers

Téléchargement partiel : Bloquer si analyse de fichiers active

Taille maximale d'un fichier (Ko) : 0

URL exclues de l'analyse antivirus : antivirus_bypass

Filtrage des fichiers (par type MIME)

	Etat	Action	Type MIME
1	Activé	Détecter et bloquer les virus	text/plain
2	Activé	Détecter et bloquer les virus	text/javascript
3	Activé	Passer sans analyse des fichiers	text/*
4	Activé	Passer sans analyse des fichiers	image/*
5	Activé	Passer sans analyse des fichiers	video/*
6	Activé	Passer sans analyse des fichiers	audio/*
7	Activé	Détecter et bloquer les virus	application/flash
8	Activé	Détecter et bloquer les virus	application/x-flash
9	Activé	Détecter et bloquer les virus	application/shockwave
10	Activé	Détecter et bloquer les virus	application/x-shockwave

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.

ANTIVIRUS PAGE DE BLOCAGE HTTP	
Protocole POP3	
Contenu de l'e-mail :	Your IPS-Firewall has detected a virus in this e-mail, it has been cleaned by the embedded antivirus.
Protocole SMTP	
Code d'erreur SMTP :	554
Message associé :	5.7.1 Virus detected
Protocole FTP	
Code d'erreur FTP :	425
Message associé :	Virus detected. Transfer aborted.

26 – Activation de l'analyse antivirusale

Les flux pouvant être analysés par le moteur antivirus 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 antivirusale les flux HTTPS, SMTPS et POP3S doivent au préalable être déchiffrés par une règle d'inspection SSL.

INSPECTION DE SÉCURITÉ

Général	
Niveau d'inspection:	IPS
Profil d'inspection:	Selon le sens du trafic
Inspection applicative	
Antivirus :	On
Sandboxing :	Off
Antispam:	Off
Filtrage URL:	Off
Filtrage SMTP:	Off