

FICHE SAVOIRS TECHNOLOGIQUE 6 :

CONFIGURER LE FILTRAGE APPLICATIF

Contenu

1. Présentation du moteur de prévention d'intrusion ASQ.....	2
2. Présentation des bases de catégories d'URL	4
3. Présentation des politiques de filtrage d'URL	7
4. Mise en place du Proxy SSL pour le filtrage des services sécurisés	9
5. Mise en place des règles de filtrage d'URL	13



Remarque :

Cette activité a été conçue dans le cadre du partenariat Stormshield Académie avec le réseau national Certa. Ce support se base sur la version 4.2 du firmware du pare-feu SNS et du support de formation officiel Stormshield. Il concerne l'utilisation de VM en autonomie, dans la même configuration que le Kit d'auto-formation CSNA de Stormshield.

Dans cette activité, vous allez reprendre l'architecture virtuelle présentée dans la fiche d'activité 1 et mettre en place des règles de filtrage au niveau applicatif afin de mieux sécuriser l'accès à votre réseau.

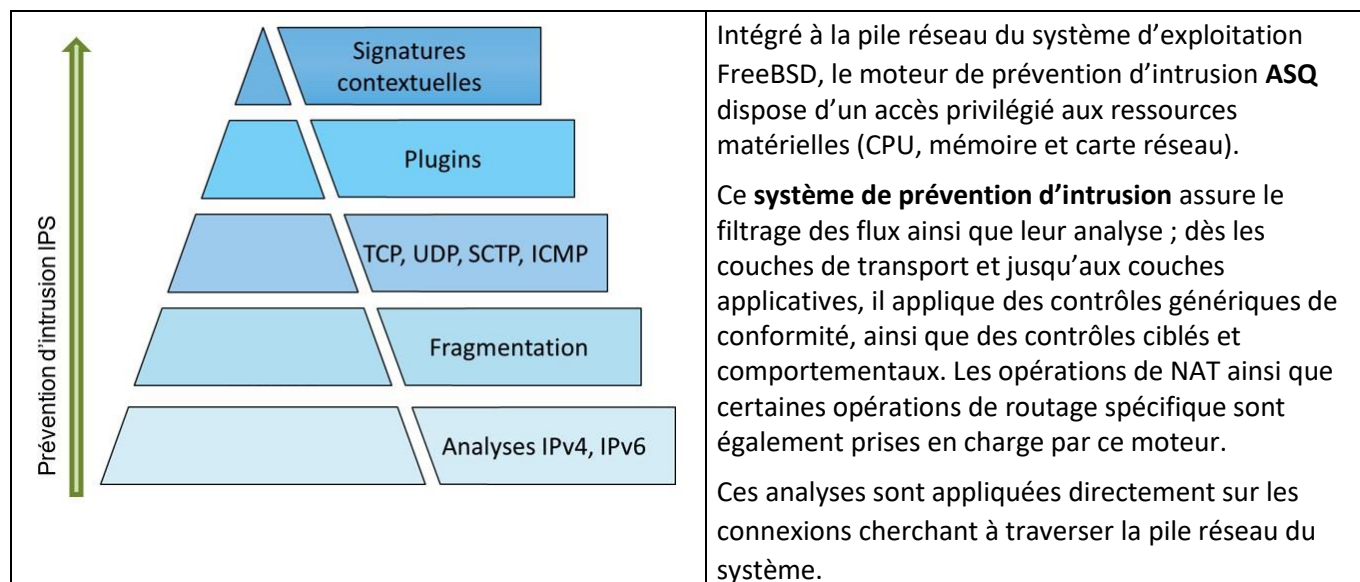
La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer des flux au travers du pare-feu SNS. Selon les flux, certaines inspections de sécurité (analyse antivirus, analyse antispam, filtrage URL, ...) peuvent être activées sur les pare-feu SNS afin de :

- Contrôler les accès à certains sites web d'Internet (filtrage d'URL et filtrage SSL).
- Créer une politique anti-relais et antispam (filtrage SMTP).
- Effectuer une analyse antivirus sur les flux DATA (HTTP, SMTP, FTP, POP3...).
- Bloquer les maliciels à l'aide d'une analyse comportementale sur des machines de détonation (sandboxing Breachfighter).

1. Présentation du moteur de prévention d'intrusion ASQ

1A. Présentation du moteur de prévention d'intrusion ASQ

Les équipements Stormshield Network Security sont équipés nativement d'un **module de prévention d'intrusion** nommé **ASQ (Active Security Qualification)**. Chaque paquet reçu par le pare-feu SNS sera soumis à un ensemble d'analyses à commencer par la vérification du protocole IP. Le rôle principal de l'ASQ est de s'assurer de la conformité du paquet par rapport aux protocoles utilisés de la couche IP jusqu'à la couche applicative (grâce aux plugins) et aux signatures contextuelles (ou Patterns). C'est également l'ASQ qui est en charge de filtrer les flux et d'appliquer une opération de NAT si nécessaire.



Le **système de prévention d'intrusion** ou **IPS** (Intrusion Prevention System) **détecte** et **bloque** les tentatives d'attaques des applicatifs grâce à des analyses contextuelles et comportementales complétées par une identification par signatures. Cette association présente deux bénéfices majeurs :

- il permet de réaliser un traitement préventif sur toutes les couches de communication (du réseau à l'application) fournissant ainsi une réelle protection 0-day ;
- l'usage des contextes applicatifs limite le nombre de signatures à examiner et réduit ainsi les risques de faux positifs tout en optimisant les temps de traitements pour procurer des performances optimales.

Les signatures utilisées par le moteur de prévention d'intrusion SNS sont construites pour détecter des attaques identifiables mais également leurs variantes potentielles. À titre d'exemple, la signature contextuelle sur une injection SQL par une commande SELECT ([http:url:decoded:95](http://url:decoded:95)) permet de contrer plus de 1 540 variantes d'attaques. En plus de maintenir un espace de stockage contenu, cette technique permet d'optimiser les temps de traitement et propose une protection contre de futures attaques basées sur les mêmes principes.

La **mise à jour des bases de signatures du moteur de prévention** Stormshield Network Security est assurée indépendamment de la mise à jour du firmware pour garantir une actualisation périodique et automatique afin de rester constamment protégé contre les nouvelles attaques.

Cette fonctionnalité de mise à jour automatique se nomme « Active Update » ; elle permet également d'ajouter de nouveaux contextes pour intégrer de nouvelles catégories de signatures contextuelles.

1B. Les différents types d'analyses

Au-delà du simple classement [niveau réseau][niveau applicatif], un firewall SNS protège le réseau selon trois familles d'analyses :

- **l'analyse protocolaire** : elle assure la conformité des flux réseau vis-à-vis des standards de communication (IP, TCP, UDP, ...) ainsi que la conformité aux protocoles applicatifs (HTTP, FTP, ...) grâce aux contrôles appliqués par les contextes applicatifs ;
- **l'analyse statistique** : basée sur des études statistiques du trafic transitant par le firewall, cette analyse détecte des comportements assimilables à du scan de ports, à du SYN flooding, ou encore à des tentatives de DoS (Denial of Service) par maintien de multiples connexions annonçant des petites fenêtres (SockStress) ;
- **l'analyse par signatures contextuelles** : elle vient compléter les contrôles de conformité sur le trafic. Cette analyse permet de se protéger de tentatives d'attaques visant spécifiquement un protocole et une implémentation cliente ou serveur, mais sans toutefois recourir à une inconformité au standard de communication. Elle s'appuie sur des bases de signatures construites par Stormshield, maintenues quotidiennement et mises à disposition sur les serveurs Active Update.

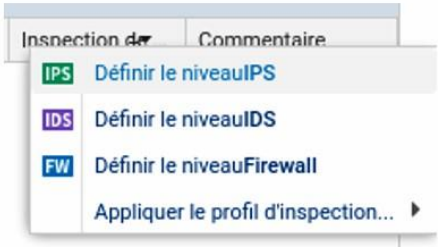
N.B. : le fonctionnement détaillé de l'ASQ ainsi que ses options sont abordés dans la formation Expert (CSNE).

1C. Les niveaux d'inspection de sécurité

Chaque paquet reçu par le pare-feu SNS est soumis à la politique de filtrage. Par défaut, l'analyse **IPS** (Intrusion Prevention System : système de prévention d'intrusion) est appliquée, ce qui signifie que le pare-feu SNS est capable de détecter une anomalie et de bloquer le paquet correspondant.

D'autres niveaux d'inspections peuvent être utilisés, à des fins de tests ou par nécessité ; par exemple si on contacte un serveur ne respectant pas la RFC des protocoles qu'il gère.

Ces niveaux sont à sélectionner dans la colonne **Inspection de sécurité** de la règle de filtrage concernée.

	<p>IPS : Détecter et bloquer (choix par défaut). L'ASQ va soumettre le paquet à l'ensemble des couches qu'il est capable d'analyser et le bloquer en cas d'anomalie.</p> <p>IDS : Détecter. L'ASQ effectue une analyse similaire à l'IPS sauf que le paquet est toujours autorisé. C'est un profil permettant de faire un audit rapide pour une règle de filtrage donnée.</p> <p>Firewall : Ne pas inspecter. L'ASQ ne va effectuer que très peu d'analyses sur le paquet reçu. Il se comporte comme un simple routeur filtrant.</p>
--	---

L'ASQ est composé de 10 configurations (également nommées **profils IPS**). Chacune de ces configurations peut être éditée en fonction des besoins de l'administrateur.

La configuration par défaut, comme indiqué dans le menu **Configuration** ⇒ **Protection applicative** ⇒ **Profils d'inspection**, applique les profils **IPS_00** et **IPS_01** respectivement aux connexions **entrantes** (paquet dont l'adresse IP source ne fait pas partie d'un réseau protégé) et aux connexions **sortantes** (paquet dont l'adresse IP source fait partie d'un réseau protégé).

Si des flux sains déclenchent des alarmes, il sera sûrement nécessaire de modifier les paramètres de l'ASQ pour ne pas bloquer la production. Dans ce cas, les modifications doivent être faites au plus spécifique. De préférence dans un profil dédié qui sera appliqué sur les règles identifiant précisément le trafic concerné.

Il est alors possible, dans la table de filtrage, de forcer l'utilisation d'un profil ASQ spécifique depuis la colonne **Inspection de sécurité**. Les profils sont ensuite configurables et administrables depuis les menus **Protocoles et Applications et protections** sous **Configuration** ⇒ **Protection applicative**.

Enfin, par défaut, l'IPS est actif sur toutes les règles de filtrage en mode de **détection automatique du protocole**. Afin de mieux inspecter les flux, il est recommandé de qualifier manuellement le type de protocole si le port utilisé n'est pas standard. L'IPS risquerait de ne pas détecter correctement l'application.

1D. Mode Proxy transparent du pare-feu

Selon les flux, certaines inspections de sécurité applicatives (analyse antivirus, analyse antispam, filtrage URL, ...) peuvent être activées. L'analyse applicative complète des flux, qu'ils soient initialement chiffrés ou pas, induit l'utilisation d'un mode Proxy sur les firewalls Stormshield. L'activation d'une inspection applicative sur une règle de filtrage du firewall entraîne ainsi le démarrage des analyses en mode Proxy transparent :

- Le firewall se fait passer pour le client auprès du serveur et 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.

N.B. : une analyse sur une règle de filtrage en mode **IPS** seulement n'utilise pas de mécanisme de type Proxy.

2. Présentation des bases de catégories d'URL

La fonction de filtrage des URL permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Pour contrôler ces accès, la politique de filtrage URL va se baser sur une liste d'URL classées en catégories ou de mots-clés personnalisés.

Deux fournisseurs de base URL sont disponibles sur les pare-feu SNS :

1) Base URL embarquée composée de 16 catégories téléchargées sur les serveurs de mise à jour, 2) Base Extended Web Control (EWC) constituée de 65 catégories, toutes hébergées dans le Cloud.

N.B. : la base étendue EWC est disponible en option payante, elle est néanmoins incluse dans les VM du partenariat Stormshield Academy.



- Ouvrez **Configuration / Objets / Objets Web** onglet **Base d'URL**. La base par défaut est la Base URL embarquée.

 **OBJETS / OBJETS WEB**

URL	NOM DE CERTIFICAT (CN)	GRUPE DE CATÉGORIES	BASE D'URL
Fournisseur de base d'URL :		Base URL embarquée	
Base URL embarquée			
Catégorie	Commentaire		
academic	Universities and Higher Education		
ads	Advertisement		
arts	Arts		
bank	Financial institutions		
business	Business		
employment	Employment		
entertainment	Entertainment		
illegal	Illegal Content		
it	Information Technology		
news	News		
online	Online Games, Gambling, Radios, Social Networking and File Sharing		
pornography	Pornography and Sexually-explicit Content		
proxy	Proxies and Anonymizers		

Les catégories prédéfinies pour la **Base URL embarquée** sont disponibles. Le contenu des catégories ne peut pas être consulté, cependant, l'appartenance d'une URL à un groupe peut être vérifiée par le biais des champs de classification. Ces champs sont disponibles depuis le menu Objets Web ou au sein d'une politique de filtrage URL. Nous allons vérifier l'appartenance de Stormshield à une des catégories de la base.

- Ouvrez **Configuration / Objets / Objets Web** onglet **URL**.
- Dans la zone **Vérifier l'utilisation** saisissez **stormshield.eu** et cliquez **Classifier**.

 **Vérifier l'utilisation** |  **Classifier**

Le résultat s'affiche dans la zone de commentaires, l'URL **stormshield.eu** fait partie de la catégorie **IT** :

Catégorie(s) de l'URL : stormshield.eu ↑
 it

- Au besoin, cliquez le symbole au bas de l'écran  pour déplier la zone de commentaires.



Si les catégories de sites web prédéfinies par votre base d'URL ne sont pas exactement adaptées à vos besoins, vous pouvez créer vos propres catégories pour y mettre les URL que vous souhaitez bloquer ou autoriser. Nous vous recommandons ainsi de prévoir une catégorie `white_list` et une catégorie `black_list`.

Étape 1 : nous allons créer une catégorie personnalisée `black_list` pour y mettre les URL à blacklister.

- Dans l'onglet **URL**, cliquez **Ajouter une catégorie personnalisée** puis donnez-lui le nom **black_list**.
- Dans la zone **Catégorie d'URL** cliquez **Ajouter une URL** saisir ***.badssl.com/***

Le site badssl.com permet d'effectuer de nombreux tests de configuration des navigateurs Internet. En particulier l'url [http.badssl.com](http://badssl.com) permet de tester l'affichage d'une page web en http.

Afin de bien comprendre les éléments nécessaires à ces analyses applicatives, nous créerons les règles de filtrage & NAT minimales pour tester les règles de filtrage d'URL.

Étape 2 : nous allons créer une nouvelle politique de filtrage basée sur (09) NAT Internet_Pass all et la renommer « Lab6_URL_NAT_Pass all ».

Nous allons créer une règle pour autoriser toutes les requêtes de résolution DNS, et une autre pour autoriser les requêtes http et https. Nous supprimerons ensuite la règle **Pass all** de cette politique.

- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**.
- Copiez la politique de filtrage/NAT **(09) NAT Internet_Pass all** vers la politique **(06)** et la renommer « **Lab6_URL_NAT_Pass all** ». Cliquez **Appliquer** pour activer la politique **(06)**. — Dans l'onglet Filtrage, cliquez Nouvelle règle / règle simple
 - Action : Passer
 - Source : Network_internals
 - Destination : Any
 - Protocole dest : Port destination, ici dns_udp.
- Cliquez Nouvelle règle / règle simple
 - Action : Passer
 - Source : Network_internals
 - Destination : Internet
 - Protocole dest : Port destination, ici http.
- Sélectionnez la règle précédente qui autorise l'accès à Internet avec le protocole http. Cliquez **Copier** puis **Coller** pour la dupliquer, modifiez **Port destination**, par **https**.
- Sélectionnez la règle **Pass all** puis cliquez sur **x Supprimer**. La règle implicite `Block_all` est réactivée.

Les règles suivantes doivent être créées :

	État	Action	Source	Destination	Port dest.
1	<input checked="" type="checkbox"/> on	→ passer	network_internals	* Any	dns_udp
2	<input checked="" type="checkbox"/> on	→ passer	Network_internals	Internet	http
3	<input checked="" type="checkbox"/> on	→ passer	Network_internals	Internet	https

À ce stade vous pouvez tester que vous pouvez accéder à n'importe quel site web depuis votre poste client configuré selon le plan d'adressage de l'agence **A** : Adresse IP : 192.168.1.100/24, Passerelle par défaut : 192.168.1.254, Serveurs DNS : 172.16.1.10.

- Ouvrez la page web [http.badssl.com](http://badssl.com) depuis le navigateur de votre poste client, elle doit s'afficher correctement.



3. Présentation des politiques de filtrage d'URL

Vous allez dans un premier temps découvrir à travers les règles déjà définies dans les politiques prédéfinies de filtrage, le fonctionnement des règles de filtrage sur un pare-feu Stormshield.

- Ouvrez le menu **Configuration / Politique de sécurité / Filtrage URL**
- Dans la liste déroulante des politiques de sécurité, choisissez **(0) URLFilter_00**.

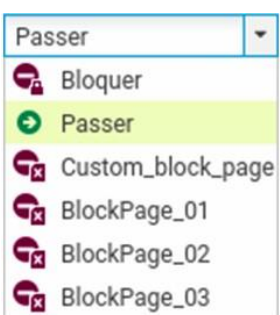
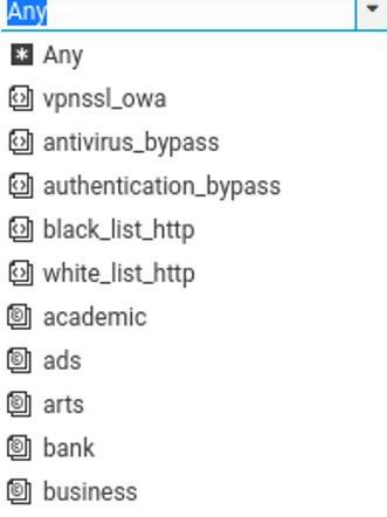
➤ POLITIQUE DE SÉCURITÉ / FILTRAGE URL

(0) URLFilter_00		Fournisseur de base URL : Base URL embarquée	
État	Action	Catégorie d'URL	Commentaire
1 <input type="checkbox"/> off	→ Passer	authenticati...	authorize the URLs of authentication_bypass group
2 <input checked="" type="checkbox"/> on	→ Passer	any	default rule (pass all)

La règle numéro 1 (non activée) autorise les URL qui font partie du groupe **authentication_bypass** qui peut être consulté dans le menu **Objets Web**, il s'agit des sites qui permettent les mises à jour Microsoft.

La règle numéro 2 laisse explicitement passer tous les flux.

Les règles de filtrage d'URL sont composées d'une colonne **Action** et d'une colonne **Catégorie d'URL**.

 <p>La colonne Action permet de Bloquer ou de Passer ou de rediriger vers l'une des 4 pages de blocage personnalisables.</p>	<p>La colonne Catégorie d'URL contient la liste des catégories prédéfinies de la base URL embarquée et les catégories personnalisées que vous avez créées.</p>	
---	--	---

Il convient ensuite de choisir les catégories de sites à autoriser, bloquer ou à rediriger vers l'une des 4 pages de blocage personnalisables. Le contrôle de cohérence en temps réel affiche les erreurs détectées dans votre politique.

Étape 3 : Nous allons créer une règle de blocage pour la catégorie personnalisée **black_list**.

- Dans la liste déroulante des politiques de sécurité, choisissez **(0) URLFilter_00**, cliquez **Éditer** puis **Renommer** « **Lab6_URL** » puis **Mettre à jour**.
- Positionnez-vous sur la règle 1 (désactivée) et cliquez + **Ajouter** pour ajouter une nouvelle règle de filtrage d'URL.

	État	≡	Action	≡	Catégorie d'URL	Commentaire
1	<input type="checkbox"/> off		Passer		authentificati...	authorize the URLs of authentication_bypass group
2	<input checked="" type="checkbox"/> on		BlockPage_00		Any	
3	<input checked="" type="checkbox"/> on		Passer		any	default rule (pass all)

- Dans la règle 2, dans **Action**, laissez **BlockPage_00**, dans la colonne **Catégorie d'URL**, choisissez **black_list**, cliquez **Appliquer** puis **Sauvegarder**.

Les pages de blocage par défaut, ici **BlockPage_00** peuvent être éditées depuis le menu **Configuration** ⇒ **Notifications** ⇒ **Messages de blocage** ⇒ Onglet **Page de blocage HTTP**. Les modifications peuvent s'effectuer grâce à l'éditeur HTML, cela permet de personnaliser la page.

- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.
- Dans l'onglet **Filtrage**, ouvrez la règle 2 qui autorise l'accès à Internet avec le protocole **http**. Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection applicative** choisir **LAB6_URL** dans la liste **Filtrage URL**.

Inspection applicative

Antivirus ⓘ :	<input type="checkbox"/> Off
Sandboxing ⓘ :	<input type="checkbox"/> Off
Antispam:	<input type="checkbox"/> Off
Filtrage URL:	<input checked="" type="checkbox"/> Lab6_URL
Filtrage SMTP:	<input type="checkbox"/> Off
Filtrage FTP:	<input type="checkbox"/> Off
Filtrage SSL:	<input type="checkbox"/> Off

Vous devez obtenir la règle suivante :

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
1	on	passer	network_internals	Any	dns_udp		IPS
2	on	passer	Network_in	Internet	http		IPS Filtrage URL : Lab6_URL

- Ouvrez la page web <http://badssl.com> depuis votre navigateur, elle ne doit pas s'afficher correctement. Vous devez voir le message de blocage ci-dessous :



If you believe it is an error, please contact your network administrator by clicking on the following link: [Request access to this website](#)

La règle de filtrage a été utilisée et la barre de comptage est passée en bleu pour indiquer que du filtrage applicatif a été appliqué.

1	on	passer	network_internals	Any	dns_udp	IPS
2	on	passer	Network_in	Internet	http	IPS Filtrage URL : LAB_6
3	on	passer	Network_internals	Internet	https	IPS

- Ouvrez la page web <https://badssl.com/> depuis votre navigateur, elle s'affiche correctement car l'url est en https et n'est donc pas déchiffrée par la règle précédente.

La majorité des url d'Internet étant en **https**, il faudra d'abord déchiffrer le flux pour pouvoir décider du blocage ou non, ce qui nécessite l'utilisation d'un proxy SSL.

4. Mise en place du Proxy SSL pour le filtrage des services sécurisés

De nombreux services réseau tels que le web, la messagerie, la messagerie instantanée etc. utilisent le protocole TLS (plus connu sous le nom de son prédécesseur SSL) pour authentifier les correspondants et chiffrer leurs communications.

Les firewalls SNS sont capables de filtrer et déchiffrer les connexions HTTPS, ce qui permet de :

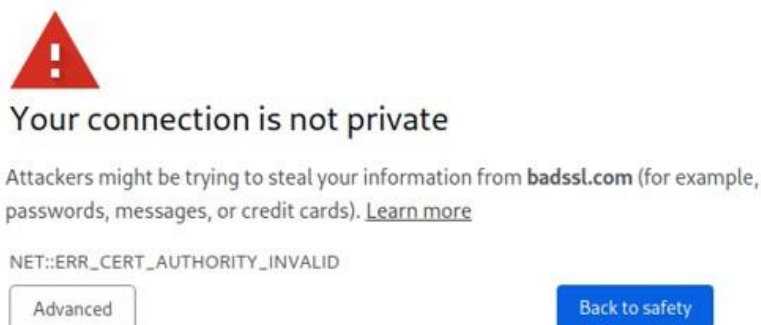
- Bloquer des sites web HTTPS ou des catégories de sites web HTTPS inappropriés.
- Analyser les flux HTTPS pour les fonctions de protection applicative (e.g., anti-virus, sandboxing, filtrage URL, Google SafeSearch, etc.).

Pour activer ces fonctionnalités sur votre pare-feu SNS, vous devez configurer le proxy SSL.

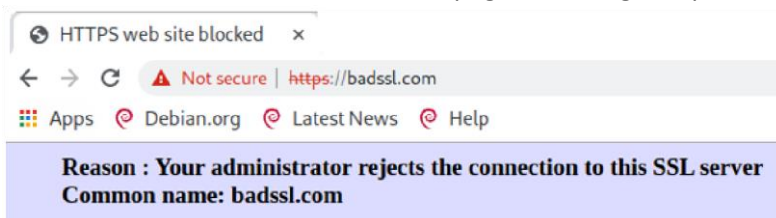
4A. Méthodes de filtrage pour HTTPS

Deux méthodes sont envisageables pour filtrer les connexions HTTPS : **avec** ou **sans** déchiffrement des flux SSL. Ces deux méthodes peuvent être combinées en fonction de différents critères, tels que l'authentification ou le réseau IP source. Nous étudierons ici uniquement le **Filtrage SANS déchiffrement des flux SSL**.

Cette méthode permet de bloquer les sites web HTTPS indésirables en vérifiant seulement leur certificat sans déchiffrer le flux. Ainsi, lorsqu'un client initie une connexion vers un site en HTTPS, il envoie en clair au serveur le nom de domaine du site demandé. Ce mécanisme appelé **Server Name Indication (SNI)** permet au serveur de sélectionner le bon certificat à présenter au client. Stormshield Network Security s'appuie sur ce système pour contrôler l'accès à ces sites web sans déchiffrer le flux. Avec ce type de filtrage, les pare-feu SNS sont compatibles avec les extensions SNI (Server Name Indication), permettant de décrire explicitement le nom de l'hôte avec lequel une session TLS est en négociation. Un message de certificat invalide apparaîtra en cas de blocage puis une page de blocage non personnalisable.



Si vous choisissez **Advanced** et **Proceed**, vous aurez accès à la page de blocage du pare-feu SNS :

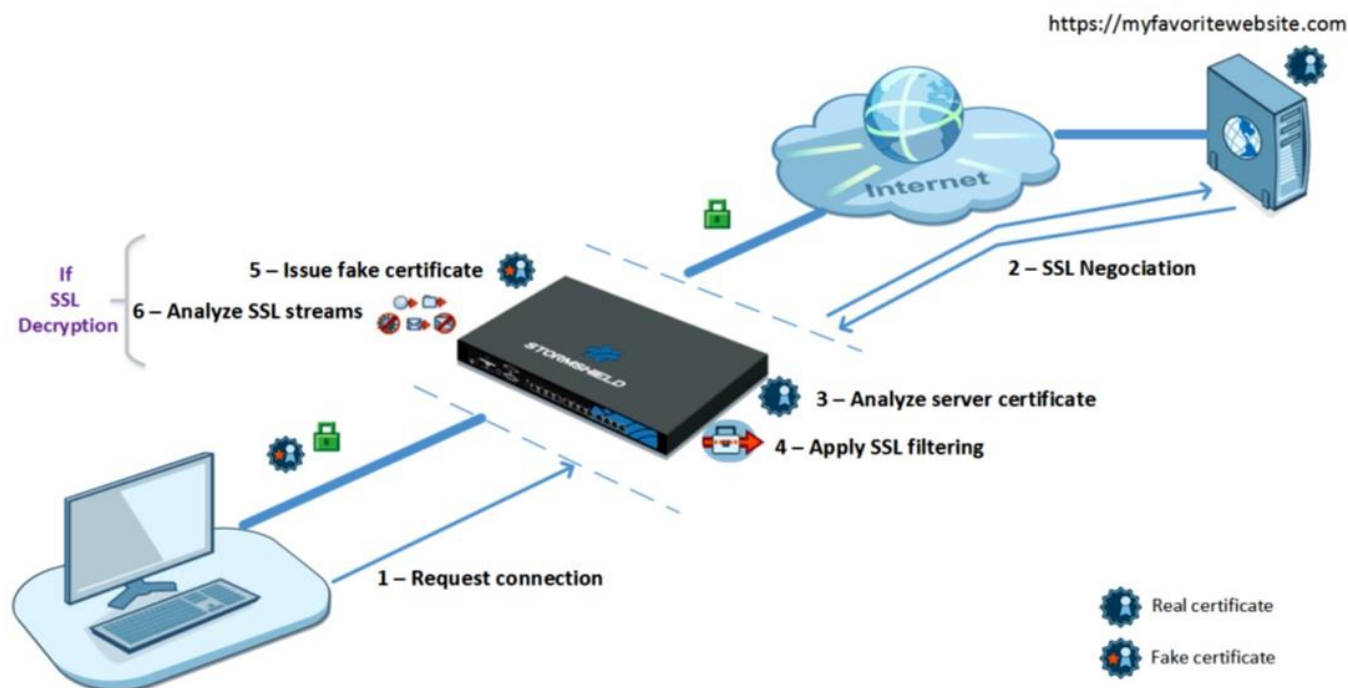


En revanche, cette méthode ne permet pas d'analyser les connexions HTTPS avec les protections applicatives tels que l'anti-virus, le sandboxing, Google SafeSearch, etc.

Le déchiffrement des données personnelles étant encadré par la loi dans la majorité des pays, le filtrage SSL doit prendre en compte cette législation. Vous devez exclure les sites qui ne doivent pas être déchiffrés en leur appliquant l'action **Passer sans déchiffrer** (e.g., en France les sites bancaires). Pour la France, les aspects juridiques liés au déchiffrement SSL sont détaillés en annexe du document [Recommandations de sécurité concernant l'analyse des flux HTTPS](#) de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations).

4B. Fonctionnement du proxy SSL

Le proxy SSL est positionné en « homme du milieu » (Man in the middle) sur le trafic SSL entre le client et le serveur web. Il se charge des négociations SSL et sécurise ainsi les connexions proxy SSL/serveur, et proxy SSL/client. Entre les deux, il autorise ou bloque les connexions selon la politique de filtrage, et si besoin, il déchiffre les flux SSL.



Les différentes étapes du filtrage SSL sont les suivantes :

- 1) Le proxy SSL intercepte les connexions du client sur le port TCP/443.
- 2) Il effectue les négociations SSL avec le serveur web au nom du client.
- 3) Il analyse le certificat envoyé par le serveur. En cas de non-conformité du certificat, l'accès au serveur est bloqué.
- 4) Si le certificat est conforme, le proxy SSL consulte les règles de filtrage SSL :
 - **Bloquer sans déchiffrer** : il bloque les connexions,
 - **Passer sans déchiffrer** : il laisse passer les connexions,
 - **Déchiffrer** : il déchiffre le flux qui est ensuite évalué par les règles de filtrage suivantes.
- 5) Si l'action est **Déchiffrer**, le proxy SSL génère un certificat usurpé (fake certificate) et le présente au client qui vérifie le certificat. Si le certificat de l'autorité signataire n'a pas été installé dans le navigateur ou dans le système et déclaré comme autorité de confiance, un message d'erreur s'affiche.
- 6) Si le certificat est présent, le trafic est sécurisé. Les protections applicatives sont appliquées (e.g., anti-virus, antispam, sandboxing).

NOTE : les étapes 5 et 6 ont lieu uniquement si vous appliquez la méthode de filtrage AVEC déchiffrement des flux SSL.

4C. Configuration du proxy SSL pour le filtrage des sites https

Étape 4 : nous allons créer une catégorie personnalisée `black_list_https`.

- Ouvrez le menu **Configuration / Politique de sécurité / Filtrage SSL**
- Dans la liste déroulante des politiques de sécurité, choisissez **(0) SSLFilter_00**.

➔ POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00				
Editer Fournisseur de base URL : Base URL embarquée				
+ Ajouter X Supprimer ↑ Monter ↓ Descendre ✂ Couper 📄 Copier 📄 Coller + Ajouter toutes les catégories				
	État	Action	URL - CN	Commentaire
1	on	Passer sans déchiffrer	proxysl_bypass	don't decrypt some specific ssl servers
2	on	Déchiffrer	any	default rule (decrypt all)

Deux règles sont déjà présentes par défaut. La règle numéro 1 spécifie de **Passer sans déchiffrer** les **URL-CN** qui font partie de la catégorie **proxysl_bypass**. En effet, ces serveurs détectent que le proxy SSL génère un certificat usurpé et sont susceptibles de refuser les connexions (c'est le cas par exemple de mozilla.org).

La règle numéro 2 spécifie de déchiffrer tous les autres.

Les règles de filtrage SSL sont composées d'une colonne **Action** et d'une colonne **URL-CN**. Cette dernière correspond au nom que l'on retrouve dans le certificat du serveur concerné.

— Ouvrez **Configuration / Objets / Objets Web** onglet **NOM DE CERTIFICAT (CN)**.

OBJETS / OBJETS WEB

URL	NOM DE CERTIFICAT (CN)	GRUPE DE CATÉGORIES
Ajouter une catégorie personnalisée Supprimer Vérifier l'utilisation		
Catégorie de noms de certificat (CN)		Commentaire
proxysl_bypass		

On retrouve la catégorie par défaut **proxysl_bypass** qui contient une liste de noms de certificats que Stormshield recommande de laisser passer sans déchiffrer.

Pour faciliter l'élaboration de règles de filtrage SSL nous vous recommandons de créer les catégories suivantes pour les sites https :

- Une catégorie de **liste blanche** (white_list_https) contenant toutes les URL que vous estimez fiables. Par exemple les sites que la législation ne vous autorise pas à déchiffrer, vos sites internes, ainsi que les sites de mise à jour des systèmes et des logiciels (e.g., Microsoft, antivirus etc.). Appliquez à cette nouvelle catégorie l'action **Passer sans déchiffrer**.
- Une catégorie de **liste noire** (black_list_https) contenant des URL que vous estimez malveillantes et que vous ne trouvez pas dans les catégories prédéfinies. Appliquez à cette nouvelle catégorie l'action **Bloquer sans déchiffrer**.
 - Dans l'onglet **NOM DE CERTIFICAT (CN)**, cliquer **Ajouter une catégorie personnalisée** puis donnez-lui le nom **black_list_https**.
 - Dans la zone **Catégorie d'URL** cliquer **Ajouter un nom de certificat URL** saisir ***.badssl.com**, puis saisir également **badssl.com**.

Étape 5 : nous allons créer une règle de filtrage SSL pour la catégorie personnalisée black_list_https.

- Ouvrez le menu **Configuration / Politique de sécurité / Filtrage SSL**
- Dans la liste déroulante des politiques de sécurité, choisissez **(0) SSLFilter_00**, cliquez **Éditer** puis **Renommer « Lab6_SSL »** puis **Mettre à jour**.
- Positionnez-vous sur la règle 1 et cliquez **+ Ajouter** pour ajouter une nouvelle règle de filtrage SSL.
- Dans la règle 2, dans **Action**, choisir **Bloquer sans déchiffrer**, dans la colonne **URL-CN**, choisissez **black_list_https**, cliquez **Appliquer** puis **Sauvegarder**.

Étape 6 : nous allons activer dans une règle de filtrage classique le déchiffrement pour le protocole https.

Une fois la politique de filtrage SSL définie, il convient de l'appliquer, ainsi que l'action **Déchiffrer**, à une règle de filtrage autorisant les flux HTTPS sortants, comme le montre l'exemple ci-après.

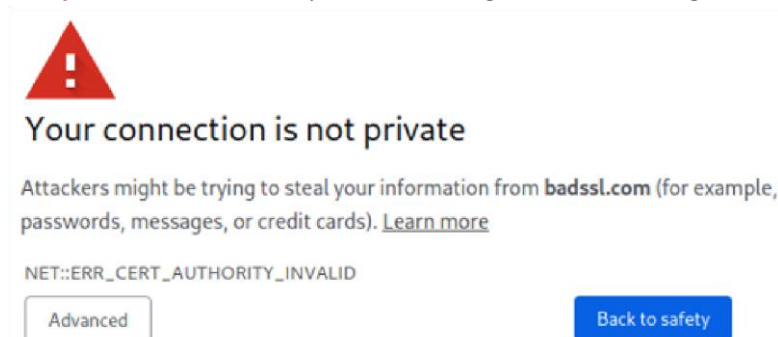
Cette manière de procéder permet d'activer plusieurs politiques de filtrage SSL simultanément afin de gérer les accès de différents réseaux ou machines sources.

- Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.
- Dans l'onglet **Filtrage**, ouvrez la règle 3 qui autorise l'accès à Internet avec le protocole **https**. Dans l'onglet **Action** choisir **Déchiffrer**.
- Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection applicative** choisir **LAB6_SSL** dans la liste **Filtrage SSL**.

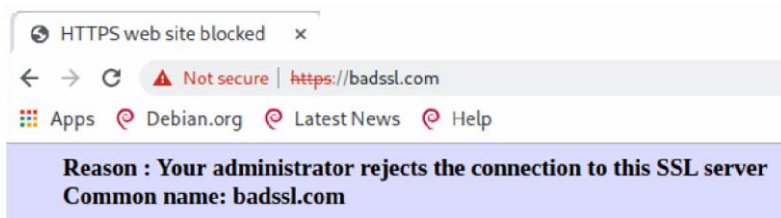
Vous devez obtenir la règle suivante :



- Videz le cache de votre navigateur, afin de purger le cache des sites des essais précédents.
- Ouvrez la page web <https://badssl.com/> depuis votre navigateur, un message de certificat invalide apparaît.



- Si vous choisissez **Advanced** et **Proceed**, vous aurez accès à la page de blocage du pare-feu SNS :



Le filtrage SSL a donc bien correctement fonctionné.

5. Mise en place des règles de filtrage d'URL

Étape 1 : mettre en place une première série de règles de filtrage standard pour les sites web.

Trafics sortants :

- 1) Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (tester avec www.visitkorea.or.kr).
- 2) L'accès au site <https://www.cnn.com> doit être bloqué depuis le réseau interne. Pour cela vous créez et utilisez un objet FQDN.
 - Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT**, au besoin choisir la politique **(06) Lab6_URL_NAT_Pass all**.
 - Ajoutez les deux règles ci-dessous, juste après la règle 1 qui autorise la résolution DNS.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	network_internals	Any	dns_udp		IPS
2	on	block	Network_in	Internet geo Republic of Ko	http https		IPS
3	on	block	Network_in	www.cnn.com	http https		IPS

➤ Testez ces nouvelles règles, vérifiez que vous obtenez bien le comportement attendu.

Étape 2 : mettre en place le filtrage d'URL selon un cahier des charges.

- 3) Trouvez les catégories dans lesquelles sont classées les URL www.netbsd.org, neverssl.com, twitter.com, allocine.fr,
- 4) Configurez une politique de filtrage URL, permettant l'accès à tous les sites Web sauf les sites http listés au point précédent.
- 5) Configurez une politique de filtrage SSL, permettant l'accès à tous les sites Web sauf les sites listés au point 3 et les sites des catégories « shopping » et « news ». Cependant, assurez-vous que le site bbc.com reste joignable.
- 6) Tentez d'accéder au site cnn.com et ensuite à euronews.com. Pourquoi la page de rejet du trafic SSL ne s'affiche pas pour cnn.com ?

À faire : rédiger un rapport répondant aux questions ci-dessus.