NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

FILTRER LES CONNEXIONS HTTPS

Produits concernés : SNS 1.0 et versions supérieures

Date : Janvier 2019

Référence : sns-fr-filtrer_les_connexions_https_note_technique

Table des matières

Avant de commencer

De nombreux services réseau tels que le web, la messagerie, la messagerie instantanée etc... utilisent le protocole TLS (plus connu sous son ancien nom 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 firewall, vous devez configurer le proxy SSL.

Ce document décrit le fonctionnement du proxy SSL, sa configuration, et les bonnes pratiques à adopter pour optimiser le filtrage et l'analyse de connexions HTTPS.

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.

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. Il n'est donc pas nécessaire d'installer un certificat sur tous les navigateurs de chaque poste de travail.

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.

De plus, un message de certificat invalide apparaît en cas de blocage et vous ne pouvez pas personnaliser la page de blocage.

Avec ce type de filtrage, les firewalls SNS sont compatibles avec les extensions SNI (Server Name Indication), vous permettant de décrire explicitement le nom de l'hôte avec lequel une session TLS est en négociation.

Filtrage AVEC déchiffrement des flux SSL

Cette méthode permet de bloquer les sites web HTTPS indésirables et d'analyser les connexions HTTPS avec les anti-virus, le sandboxing, Google SafeSearch, etc. Vous pouvez personnaliser la page de blocage qui s'affiche sur le poste de travail lorsqu'un site web HTTPS est bloqué.

Puisque les flux SSL sont déchiffrés par le firewall SNS, ce dernier va générer un certificat auto-signé que le navigateur ne pourra pas considérer de confiance. Un message d'erreur s'affichera sur le navigateur des utilisateurs indiquant la provenance suspecte du certificat présenté par le firewall SNS. Pour éviter ce type de message, vous devrez déployer l'autorité autosignée du firewall sur les navigateurs afin qu'elle soit reconnue.

Assurez-vous également de dresser une liste explicite des sites web HTTPS et/ou des catégories de sites web HTTPS que vous n'êtes pas autorisé à déchiffrer (e.g., en France les sites bancaires), afin de les laisser passer sans déchiffrement.

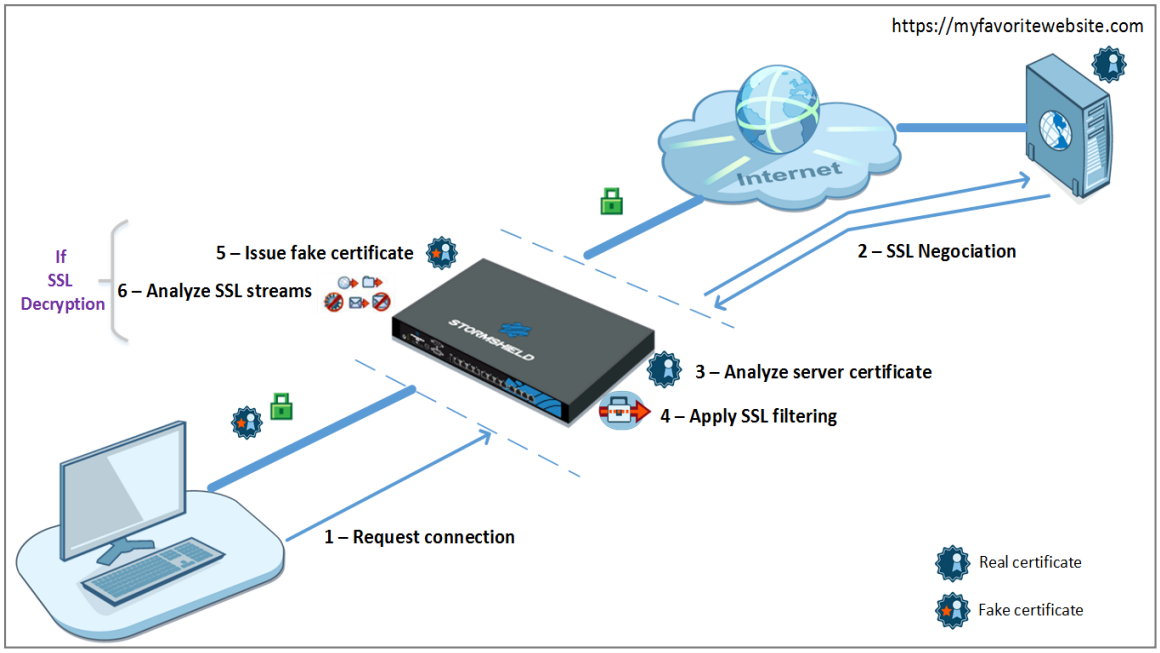
Résumé

Le tableau ci-dessous résume les caractéristiques de chaque méthode de filtrage :

	Sans déchiffrement	Avec déchiffrement
Blocage des sites web HTTPS	X	X
Analyse anti-virus, sandboxing, SafeSearch, etc.		X
Affichage d'une page de blocage personnalisée		X
Un certificat doit être installé sur chaque poste de travail		X
Ne pas déchiffrer les sites et/ou catégories de sites non autorisés	N/A	X
Accès possible pour les périphériques sans certificat (BYOD)	X	

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.

Configurer le filtrage HTTPS

Cette section détaille les différentes étapes de la configuration du filtrage HTTPS. Certaines de ces étapes ne sont applicables qu'à une seule des deux méthodes de filtrage (AVEC déchiffrement ou SANS déchiffrement). Dans ce cas, vous en serez informé.

Les étapes de configuration du filtrage HTTPS sont les suivantes :

Configurer le niveau de protection du protocole SSL

Par défaut, les firewalls Stormshield Network Security sont configurés avec un niveau de protection restrictif pour le protocole SSL : ils refusent tous les types de certificats incorrects et bloquent le trafic si le déchiffrement échoue.

Vous pouvez personnaliser cette configuration à votre convenance :

1. Connectez-vous à l'interface Web d'administration.
2. Dans le module **Configuration > Protection applicative > Protocoles**, sélectionnez le protocole **SSL**, puis le profil *(0) ssl_01* (ou un autre profil suivant votre configuration).
3. Dans l'onglet **Proxy**, zone **Inspection de contenu**, indiquez quelle action vous souhaitez effectuer dans le cas où les certificats présentés par les serveurs distants seraient des :
   - Certificats auto-signés. N'étant pas signés par une autorité de confiance publique (CA), ils peuvent être falsifiés plus facilement. Stormshield recommande de les bloquer.
   - Certificat expirés. Ils ne se trouvent plus dans la liste de révocation (CRL) et il est donc impossible de savoir s'ils sont valides ou révoqués. Stormshield recommande de les bloquer.
   - Certificat inconnus. Stormshield recommande de les bloquer.
   - Certificats de type incorrect,
   - Certificats avec FQDN incorrect,
   - Certificats avec FQDN différent du nom de domaine SSL.

   Trois types d'action sont disponibles :
   - **Bloquer** la connexion,
   - **Continuer l'analyse** du flux,
   - **Déléguer à l'utilisateur**. Cette action ajoutée en version v3.8.0 force le navigateur à présenter une alarme de sécurité informant des risques potentiels encourus. L'utilisateur prend alors la responsabilité de passer outre l'alarme s'il veut accéder au site demandé. Dans ce cas, l'administrateur est également informé par une alarme et une entrée dans le fichier de log des alarmes.
4. Cochez l'option **Autoriser les adresses IP dans les noms de domaine SSL** pour accéder à un site en utilisant son adresse IP à la place de son nom FQDN.

5. Dans la zone **Support**, indiquez les actions à effectuer au cas où :
   - Le déchiffrement échoue,
   - Le certificat n'a pas pu être classifié dans les catégories de la base URL (Base URL embarquée ou Extended Web Control).
6. Cliquez sur **Appliquer**.

Définir une politique de filtrage SSL

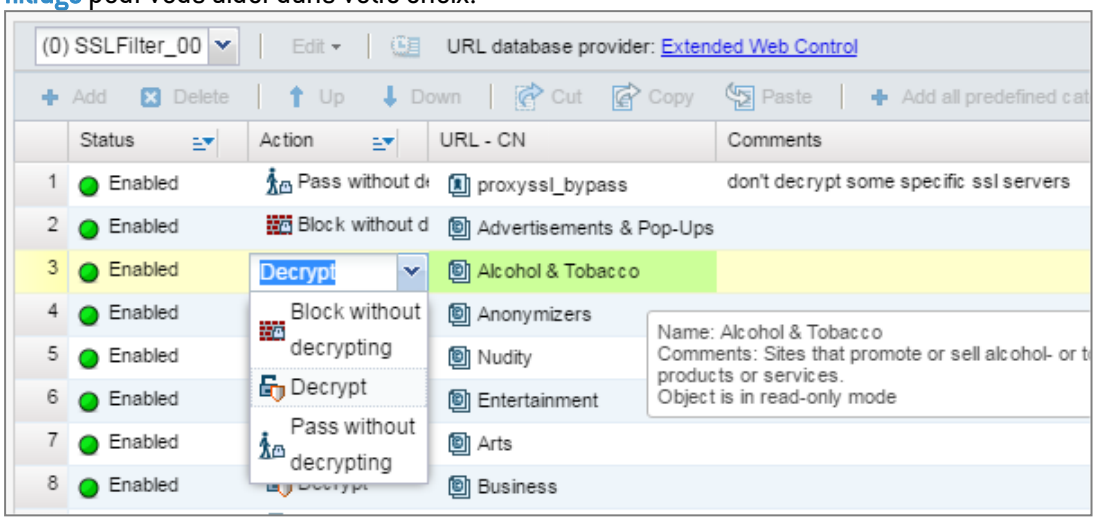
Une fois que le certificat du serveur distant a été vérifié, l'URL demandée est confrontée à toutes les règles de la politique de filtrage SSL.

- Une **règle de fitrage SSL** décrit l'action que doit effectuer le proxy SSL pour une catégorie d'URL ou de certificats donnés. Vous pouvez faire en sorte par exemple de bloquer toutes les URL qui appartiennent à la catégorie *Games* (Jeux).
- Une **politique de filtrage SSL** est un ensemble de règles qui seront parcourues séquentiellement par le firewall.

Créer une politique de filtrage SSL

1. Connectez-vous à l'interface Web d'administration.
2. Choisissez le menu **Configuration > Politique de sécurité > Filtrage SSL**, et choisissez une politique de filtrage, par exemple *SSLFilter_00*. Deux règles sont déjà présentes par défaut. La première spécifie de laisser passer sans déchiffrer certains URL-CN. La deuxième spécifie de déchiffrer tous les autres.
3. Si vous utilisez la méthode de filtrage SANS déchiffrement des flux SSL, supprimez les deux règles déjà présentes.
4. Cliquez sur **Ajouter toutes les catégories prédéfinies**.
   Une liste de catégories s'affiche, correspondant à votre base d'URL (Base URL embarquée ou Extended Web Control).
5. Supprimez toutes les catégories sur lesquelles vous ne souhaitez pas appliquer le traitement SSL.

6. Pour les catégories restantes, dans la colonne **Action**, choisissez l'action que le firewall doit effectuer sur chaque catégorie d'URL-CN. Référez-vous à la section Bonnes pratiques de filtrage pour vous aider dans votre choix.



- **Bloquer sans déchiffrer** : Le firewall refuse l'accès à l'URL-CN demandé sans effectuer d'analyse SSL préalable. Choisissez cette action pour toutes les catégories que vous souhaitez bloquer (e.g., weapons, violence, pornography, peer-to-peer, etc).
- **Passer sans déchiffrer** : Le firewall autorise l'accès à l'URL-CN demandé sans effectuer d'analyse SSL préalable. Choisissez cette action pour les catégories que vous n'êtes pas légalement autorisés à déchiffrer (e.g., sites contenant des données personnelles) et pour celles que vous estimez fiables.
- **Déchiffrer** : Le firewall déchiffre le flux SSL avant d'accepter ou refuser l'accès à l'URL-CN demandé. Utilisez cette action uniquement si vous avez choisi la méthode de filtrage AVEC déchiffrement des flux SSL.

7. Dans la colonne **URL-CN**, choisissez la catégorie d'URL ou le groupe de certificats (CN) concerné, par exemple *Violence*. S'il vous manque des catégories, vous pouvez les créer via le menu **Objets > Objets Web > Onglet URL > Ajouter des catégories personnalisées**. Pour plus d'informations, reportez-vous à la section Catégories personnalisées.
8. Cliquez sur **Ajouter** pour créer les autres règles nécessaires à votre politique et ordonnez-les en utilisant les boutons **Monter** et **Descendre** ou la fonction de copier-coller. Pour savoir comment les classer, référez-vous à la section Ordre des règles.
9. Double-cliquez dans la colonne **Etat** pour activer les règles ainsi créées.
10. Cliquez sur **Appliquer**.

La politique de filtrage SSL doit ensuite être associée à la politique de sécurité. Pour plus d'informations, reportez-vous à la section Créer une règle d'inspection SSL dans la politique de filtrage.

Bonnes pratiques de filtrage

Consultez les bonnes pratiques de filtrage lors de l'élaboration de votre politique de filtrage SSL.

Législation

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**. 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).

Catégories personnalisées

Si les catégories de sites web prédéfinies par votre base d'URL ne sont pas exactement adaptées à vos besoins, vous pouvez ajouter des catégories disponibles par défaut sur le firewall, ou créer vos propres catégories.

Par exemple, la catégorie *proxyssl_bypass* contient une liste de noms de certificats que Stormshield recommande de laisser passer sans déchiffrer. En effet, ces serveurs détectent que le proxy SSL génère un certificat usurpé et sont susceptibles de refuser les connexions.

Vous pouvez aussi créer les catégories suivantes pour faciliter l'élaboration des règles de filtrage SSL :

- Une catégorie de liste blanche (*sslproxy_whitelist*) 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 (*sslproxy_blacklist*) 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*.

Créez vos nouvelles catégories via le menu **Objets > Objets Web > Onglet URL > Ajouter des catégories personnalisées**. Pour plus d'informations, reportez-vous au *Guide d'administration et de configuration*.

Ordre des règles

Le proxy SSL parcourt la liste des règles de haut en bas. Vous pouvez organiser vos règles de deux manières :

- **Détailler les catégories autorisées** : Créez une règle pour chaque catégorie autorisée avec l'action *Passer sans déchiffrer* ou *Déchiffrer*. Ensuite la dernière règle doit bloquer toutes les autres catégories en spécifiant l'action *Bloquer sans déchiffrer* pour l'URL-CN *Any*.
- **Détailler les catégories à bloquer** : Créez une règle pour chaque catégorie indésirable avec l'action *Bloquer sans déchiffrer*. Ensuite la dernière règle doit autoriser toutes les autres catégories en spécifiant l'action *Passer sans déchiffrer* ou *Déchiffrer* pour l'URL-CN *Any*.

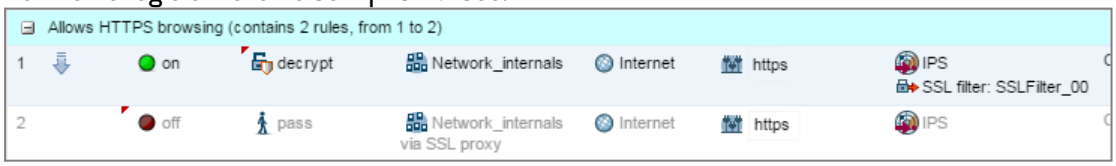
Notez aussi que dans la base d'URL Extended Web Control, les URL sont parfois répertoriées dans plusieurs catégories. Prêtez donc attention à l'ordre alphabétique des catégories. Par exemple si un site se trouve dans les deux catégories *Entertainment* (Loisirs) et *Nudity* (Nudité) et que vous souhaitez bloquer *Nudity* et autoriser *Entertainment*, assurez-vous que la catégorie *Nudity* précède *Entertainment* dans la liste des règles de filtrage SSL. Dans le cas contraire, le site en question, qui est catégorisé sous *Entertainment*, sera autorisé.

Créer une règle d'inspection SSL dans la politique de filtrage

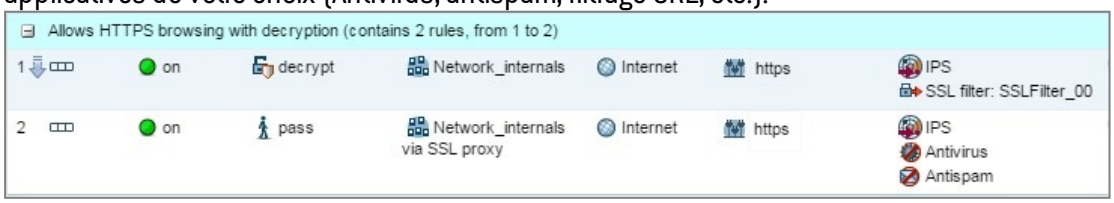
Pour que votre politique de filtrage SSL nouvellement créée soit prise en compte dans la politique de filtrage du firewall, vous devez créer une règle d'inspection SSL.

1. Connectez-vous à l'interface Web d'administration.
2. Dans le module **Configuration > Politique de sécurité > Filtrage et NAT**, sélectionnez l'onglet **Filtrage**.
3. Dans la liste déroulante, choisissez la politique de filtrage à laquelle associer le filtrage SSL.
4. Cliquez sur **Nouvelle règle > Règle d'inspection SSL**.
5. Dans la zone **Profil du trafic à déchiffrer** de l'Assistant d'inspection SSL, conservez les valeurs par défaut pour créer une règle qui interceptera tous les flux provenant du réseau interne à destination d'internet sur le groupe de port *ssl_srv*. Le groupe de port *ssl_srv* contient les ports standard des services utilisant une session TLS : HTTPS, SMTPS, POPS, etc. En revanche, FTPS n'est pas géré par le proxy SSL.

   Modifiez la valeur des champs si la configuration par défaut ne vous convient pas. Par exemple, si vous utilisez le proxy SSL exclusivement pour le flux HTTPS, indiquez *https* seul à la place de *ssl_srv* afin de réduire la consommation du firewall. Utilisez le groupe de port *ssl_srv* uniquement si tous les protocoles qu'il englobe doivent être déchiffrés.
6. Dans la zone **Inspecter le trafic chiffré**, entrez les informations suivantes :
   - **Profil d'inspection** : Sélectionnez le profil d'inspection souhaité. Pour plus d'informations, reportez-vous au *Guide d'administration et de configuration*.
   - **Politique de filtrage SSL** : Sélectionnez la politique de filtrage que vous avez créée dans la section Définir une politique de filtrage SSL (*SSLFilter_00*).
7. Cliquez sur **Terminer**. L'assistant crée deux règles de filtrage :
   - La première règle permet d'intercepter les flux provenant du réseau interne à destination d'internet sur le groupe de port *ssl_srv*. Ces flux sont dirigés vers le proxy SSL. Cette règle applique le filtrage SSL et l'action Déchiffrer.
   - La deuxième règle autorise les flux provenant du réseau interne et sortant du proxy SSL à destination d'Internet.
8. Si vous avez choisi la méthode de filtrage SANS déchiffrement des flux SSL, désactivez la deuxième règle car elle ne sera pas utilisée.



9. Si vous avez choisi la méthode de filtrage AVEC déchiffrement des flux SSL, double-cliquez dans la colonne **Inspection de sécurité** de la deuxième règle et activez les protections applicatives de votre choix (Antivirus, antispam, filtrage URL, etc.).



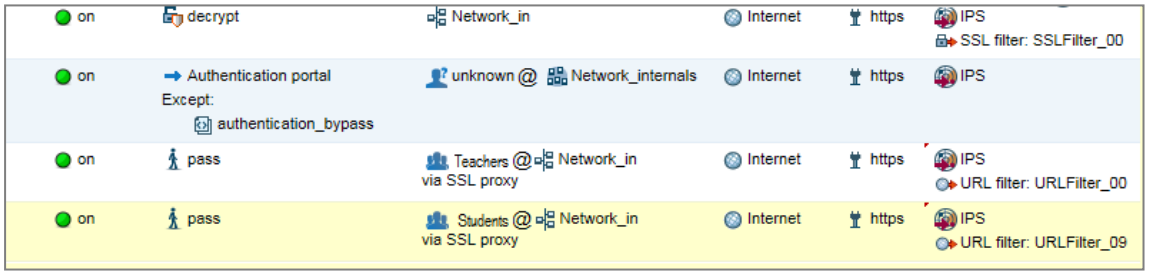
Filtrer selon des groupes d'utilisateurs

Vous pouvez établir des règles différentes selon les groupes d'utilisateurs. Par exemple dans le cas d'un lycée, on peut avoir deux groupes, *Élèves* et *Professeurs*, qui n'auront pas accès aux mêmes sites. Après avoir créé vos deux règles d'inspection SSL :

1. Double-cliquez sur la deuxième règle pour l'éditer.
2. Dans le menu **Source > Onglet Général > Champ Utilisateurs**, choisissez le groupe d'utilisateurs concerné par ce filtrage SSL (par exemple le groupe *Élèves*).
3. Faites un copier-coller des deux règles.
4. Double-cliquez sur la première règle que vous venez de copier pour l'éditer.
5. Dans le menu **Source > Onglet Général > Champ Utilisateurs**, choisissez le groupe d'utilisateurs concerné par ce filtrage SSL (par exemple le groupe *Professeurs*).
6. Dans le menu **Inspection > Champ Filtrage SSL**, choisissez la politique de filtrage SSL que vous souhaitez associer au groupe *Professeurs*.

Si les utilisateurs doivent s'authentifier lorqu'ils tentent de se connecter à un site HTTPS, vous devez ajouter une règle qui permet la redirection vers le portail captif. Cette règle doit être placée juste après la règle de déchiffrement.

Ajoutez cette règle en utilisant le menu **Nouvelle règle - Règle d'authentification** dans l'onglet **Filtrage** et en ajoutant ensuite *https* dans le **Port de destination**.



Configurer l'autorité signataire et les autorités de confiance

Suivez cette procédure uniquement si vous avez choisi la méthode de filtrage AVEC déchiffrement des flux SSL.

Par défaut, le proxy SSL signe les certificats usurpés avec l'autorité *SSL proxy default authority* déjà présente sur le firewall. Modifiez l'autorité signataire si la valeur par défaut ne vous convient pas.

De même vous pouvez personnaliser la liste des autorités ou certificats de confiance.

1. Connectez-vous à l'interface Web d'administration.
2. Dans le module **Configuration > Protection applicative > Protocoles**, sélectionnez le protocole **SSL**, puis cliquez sur **Accéder à la configuration globale**.
3. Dans l'onglet **Proxy**, zone **Génération des certificats pour émuler le serveur SSL**, indiquez la CA signataire, son mot de passe et sa durée de vie.
4. Dans l'onglet **Autorités de certification personnalisées**, ajoutez les autorités privées à qui vous souhaitez faire confiance.
5. Dans l'onglet **Autorités de certification publiques**, activez ou désactivez les autorités de confiance selon vos besoins. Le proxy SSL vérifie si le certificat du serveur distant est signé par une autorité de confiance publique ou privée. La liste des autorités publiques est mise à jour automatiquement par le module Active Update du firewall.

6. Dans l'onglet **Certificats de confiance**, ajoutez les certificats des serveurs auxquels vous souhaitez faire confiance.
7. Cliquez sur **Appliquer**.

Déployer le certificat de l'autorité signataire sur les navigateurs

Suivez cette procédure uniquement si vous avez choisi la méthode de filtrage AVEC déchiffrement des flux SSL.

1. Connectez-vous à l'interface Web d'administration.
2. Dans le module **Configuration > Objets > Certificats et PKI**, sélectionnez votre autorité signataire.
3. Cliquez sur le bouton **Téléchargement**, et choisissez **Certificat au format PEM** ou **Certificat au format DER**.
4. Importez le certificat dans le magasin de certificats de votre système d'exploitation ou de votre navigateur en utilisant votre méthode de déploiement habituelle.

> **NOTE**
> Si certains de vos utilisateurs disposent de navigateurs Chrome, assurez-vous que l'empreinte numérique des certificats serveur soit SHA-256 comme décrit dans cet article de la base de connaissance.

Optimiser les performances du filtrage HTTPS

Le proxy SSL du firewall SNS consomme une grande quantité de mémoire. Il alloue à chaque connexion HTTPS trois sockets et quatre zones de mémoire tampon. Une connexion TLS nécessite également de la mémoire pour la gestion de la cryptographie et des certificats usurpés.

Le proxy SSL, de même que les autres modules de SNS, ne peut utiliser qu'une quantité limitée de la mémoire du firewall. En effet, la mémoire est partagée de façon à ce que tous les modules puissent fonctionner simultanément.

Si vous constatez des problèmes de mémoire lors de l'utilisation du proxy SSL, vérifiez les paramètres du proxy SSL et effectuez les optimisations recommandées par Stormshield.

Obtenir les paramètres et statistiques du proxy SSL

Il est important de connaître les paramètres de dimensionnement en lien avec l'utilisation du proxy SSL. En croisant ces informations, vous pourrez anticiper d'éventuels problèmes de mémoire et optimiser les performances de votre firewall.

Connaître les paramètres mémoire du firewall

1. Connectez-vous en SSH au firewall.
2. Entrez l'une des commandes suivantes :

```
nmemstat -s
```
- ou -
```
sysctl hw.physmem
```

```
V50XXA3E0000016>
V50XXA3E0000016>nmemstat -s
Physical memory      :  2035MB
User memory          :  1544MB
Wired memory         :   490MB
Current user memory  :   221MB
Used user memory     : 14%
V50XXA3E0000016>
```

Dans cet exemple, le firewall a une mémoire de 2 Go.

Connaître les paramètres du proxy SSL

1. Connectez-vous en SSH au firewall.
2. Pour obtenir les paramètres de connexion, entrez la commande suivante : `tproxyd -s ssl`

```
----- Common part -----
. Min nb of connections=150
. Max nb of connections=150
. Max nb of connections from one ip=135
. Backlog=15 (may be hard limited by the kernel)
. Sockets rbufsize=57344 wbufsize=32768
. If nb connections > 75 then --> Sockets rbufsize=8192 wbufsize=8192
. Proxy buffers: clientbufsize=2048 serverbufsize=2048
. If nb connections > 37 then --> Proxy buffers: clientbufsize=2048 serverbufsiz
e=2048
. Apply NAT is Disabled
Use ALL the embedded CA trusted
Use the embedded CA custom :
List of trusted certificates :
Cipher Level = Low Medium High
SSL protocol usable                        = TLSv1.0 TLSv1.1 TLSv1.2
CA used to sign the fake certificates      = SSL proxy default authority

Hash used to sign the fake certificates    = SHA256
Max nb of IP in cache                     = 20
Limit of validity for the fake-certifs     = 7 days
Max number of fake certificates            = 256
Fake certificates currently used :
V50XXA3E0000016>
```

Dans cet exemple :

- Le nombre maximum de connexions autorisées pour le proxy SSL est de 150.
- La taille de la mémoire tampon diminue à partir de 75 connexions.

3. Pour connaître la quantité de mémoire utilisée par le proxy SSL, entrez la commande suivante : `nmemstat -a`

```
last pid:  5756;  load averages:  1.59,  1.76,  1.68    up 0+06:34:53  19:17:20
26 processes:  1 running, 24 sleeping, 1 zombie
CPU:  1.2% user,  0.0% nice,  1.6% system,  2.0% interrupt, 95.3% idle
Mem: 35M Active, 137M Inact, 491M Wired, 4K Cache, 229M Buf, 1321M Free
Swap: 2048M Total, 2048M Free

  PID USERNAME  THR PRI NICE   SIZE    RES STATE    TIME    WCPU COMMAND
 1308 admin      12  52   -5   123M 26244K nanslp   5:23   1.95% stated
  916 admin       9  52  -17 75552K 17120K nanslp  11:55   0.00% logd
  932 admin       8  52  -15   122M 41988K nanslp   3:25   0.00% asqd
 1888 admin       1  52    0 90744K 11072K select   2:34   0.00% cad
  937 admin       3  52  -20 62772K 12000K select   2:32   0.00% userreqd
 1412 admin       1  52    0   128M 19096K kqread   2:24   0.00% sld
 1325 admin       3  52    0   142M 21040K nanslp   2:16   0.00% snmpd
 1305 admin       7  52  -18 62572K 34536K semwai   2:08   0.00% corosync
  979 admin       3  52    0   176M 43856K select   2:08   0.00% serverd
  930 admin       1  52  -20 53368K  7456K nanslp   0:14   0.00% hardwared
  902 admin       1  52    0 42528K  7048K kqread   0:08   0.00% launchd
  922 admin       1  52    0 99368K 10704K kqread   0:06   0.00% monitord
 1120 admin       3  52    0   177M 25112K uwait    0:06   0.00% tproxyd
 1185 admin       1  52    0 54056K 10376K select   0:04   0.00% ancient
 1532 admin       1  52    0 49004K  7492K select   0:00   0.00% eventd
```

Dans cet exemple, la mémoire utilisée par le proxy SSL est 177 Mo.

Superviser les connexions du proxy SSL

Pour optimiser au mieux le proxy SSL, il est utile d'obtenir des statistiques sur le nombre de connexions SSL simultanées sur votre firewall. Si ce nombre se rapproche ou dépasse trop souvent du maximum autorisé par le proxy SSL, les performances du firewall risquent de chuter. Veuillez alors optimiser le proxy SSL comme préconisé dans la section Limiter l'utilisation du proxy SSL

1. Connectez-vous en SSH au firewall.
2. Entrez la commande suivante pour lister le nombre de connexions TCP ouvertes filtrées sur le port 8084 :

```
netstat -np tcp | grep 8084 |wc -l
```

```
V100XA04H7017A9>netstat -np tcp | grep 8084 | wc -l
      97
```

Dans cet exemple, il y a 97 connexions simultanées.

Obtenir des statistiques sur les connexions SSL

Deux articles de la Base de connaissances Stormshield fournissent des précisions sur comment obtenir des statistiques sur une période donnée :

- Activer des statistiques de proxy
- Comprendre les statistiques de proxy

Pour accéder à la Base de connaissances, utilisez l'identifiant de votre espace personnel MyStormshield.

Vous pouvez également utiliser un outil de supervision SNMP tel que Nagios, pour obtenir des informations sur les processus `tproxyd`, la CPU, la mémoire, etc. Consultez le site web de Stormshield pour plus d'informations sur les MIB compatibles.

Limiter l'utilisation du proxy SSL

Pour optimiser la consommation de la mémoire, limitez l'utilisation du proxy SSL en suivant les recommandations ci-dessous.

Eviter le proxy SSL pour les sites de confiance

Pour limiter l'utilisation du proxy SSL, vous pouvez autoriser une connexion directe pour les sites de confiance internes les plus fréquemment utilisés.

Dans l'onglet **Filtrage** du module **Configuration > Politique de sécurité > Filtrage et NAT**, ajoutez une règle simple au-dessus de vos règles SSL. Ses propriétés sont les suivantes :

- **Action** : Passer
- **Destination** : Objet FQDN représentant votre site de confiance (i.e., objet FQDN *mywebsite.com* créé au préalable).
- **Dest. port** : https

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
	on	pass	Network_internals	mywebsite.com	https		IPS
	on	decrypt	Network_internals	Internet	https		IPS SSL filter: SSLFilter_00
	on	pass	Network_internals via SSL proxy	Internet	https		IPS Antivirus Sandboxing

Dans cet exemple, toute connexion au site *https://mywebsite.com* sera autorisée sans être redirigée vers le proxy SSL. Elle consommera donc moins de mémoire et ne sera pas décomptée des connexions SSL.

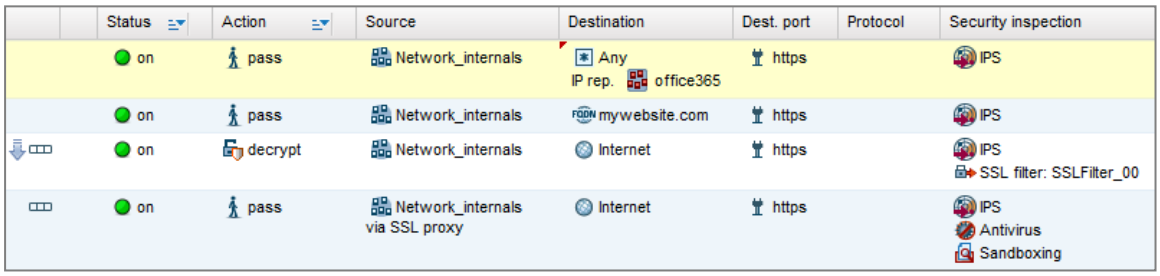
Ajoutez une règle pour chaque site de confiance.

Eviter le proxy SSL pour Office 365

Si vos utilisateurs disposent de comptes Office 365, vous pouvez autoriser une connexion directe vers toutes les ressources Office 365 sans redirection vers le proxy SSL.

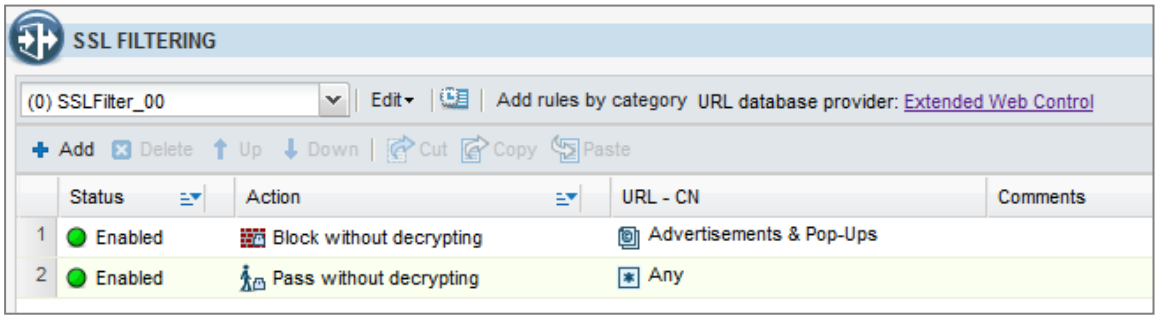
Dans l'onglet **Filtrage** du module **Configuration > Politique de sécurité > Filtrage et NAT**, ajoutez une règle simple au-dessus de vos règles SSL. Ses propriétés sont les suivantes :

- **Action** : Passer,
- **Dest. port** : https,
- **Destination** : Dans l'onglet **Géolocalisation/Réputation** de la destination, sélectionnez la catégorie de réputation Office 365.



Bloquer les publicités

Lorsqu'un utilisateur visite une page web, il ouvre une connexion vers le site associé, mais aussi de nombreuses autres connexions vers des sites publicitaires. Pour diminuer le nombre de connexions, il est donc fortement recommandé de bloquer les sites publicitaires (*Ads* ou *Adverstisements & Pop-Ups*) dans la politique de filtrage SSL.



Utiliser la base URL Extended Web Control

Pour pouvoir bloquer de plus nombreuses URL et les filtrer plus finement, préférez la base d'URL Extended Web Control à la Base d'URL embarquée. Les performances seront meilleures car cette base n'est pas chargée en mémoire.

Dans l'onglet **Base d'URL** du module **Configuration > Objets > Objets Web**, choisissez **Extended Web control** comme fournisseur de base d'URL.

Si vous ne disposez pas de l'option Extended Web Control sur votre firewall, contactez votre commercial Stormshield.

STORMSHIELD

documentation@stormshield.eu