STORMSHIELD

TECHNICAL NOTE

STORMSHIELD NETWORK SECURITY

FILTERING HTTPS CONNECTIONS

Product concerned: SNS 1.0 and higher versions

Date: January 2019

Reference: sns-en-filtering_https_connections_technical_note

Table of contents

Getting started

Many network services such as web, mail, chat, etc. use the TLS (Transport Layer Security) protocol, better known under its former name SSL (Secure Sockets Layer), to authenticate peers and encrypt their communications.

SNS firewalls are able to filter and decrypt HTTPS connections, making it possible to:

- Block inappropriate HTTPS websites or categories of HTTPS websites,
- Analyze HTTPS traffic for application protection purposes (e.g., anti-virus, sandboxing, URL filtering, Google SafeSearch, etc.).

To enable these features on your firewall, you need to configure the SSL proxy.

This guide explains how the SSL proxy works, how to configure it and the best practices to adopt in order to optimize the filtering and analysis of HTTPS connections.

Filtering methods for HTTPS

There are two possible methods for filtering HTTPS connections: with or without SSL traffic decryption. Both of these methods can be combined depending on various criteria such as authentication or the source IP network.

Filtering WITHOUT decrypting SSL traffic

In this method, undesirable HTTPS websites can be blocked by verifying only their certificates without decrypting traffic. Certificates therefore do not need to be installed on all browsers on all workstations.

However, this method does not allow HTTPS connections to be analyzed with application protections such as anti-virus, sandboxing, Google SafeSearch, etc.

Furthermore, when a website is blocked, a message indicating that the certificate is invalid will appear, and the block page cannot be customized.

With this type of filtering, SNS firewalls are compatible with SNI (Server Name Indication) extensions, allowing you to provide a clear description of the host with which a TLS session is being negotiated.

Filtering WITH SSL traffic decryption

This method makes it possible to block undesirable HTTPS websites and analyze HTTPS connections with an anti-virus, sandboxing, Google SafeSearch, etc. You can also customize the block page that appears on the workstation whenever an HTTPS website is blocked.

Since the SNS firewall decrypts SSL traffic, it will generate a self-signed certificate that the browser cannot consider trustworthy. An error message will be displayed on users' browsers, indicating that the source of the certificate presented by the SNS firewall is suspicious. To avoid seeing this type of message, you need to deploy the firewall's self-signed authority on browsers so that it will be recognized.

Ensure that you also compile a clear list of HTTPS websites and/or categories of HTTPS websites that you are not allowed to decrypt (e.g. banking websites in France), in order to let them pass through without decryption.

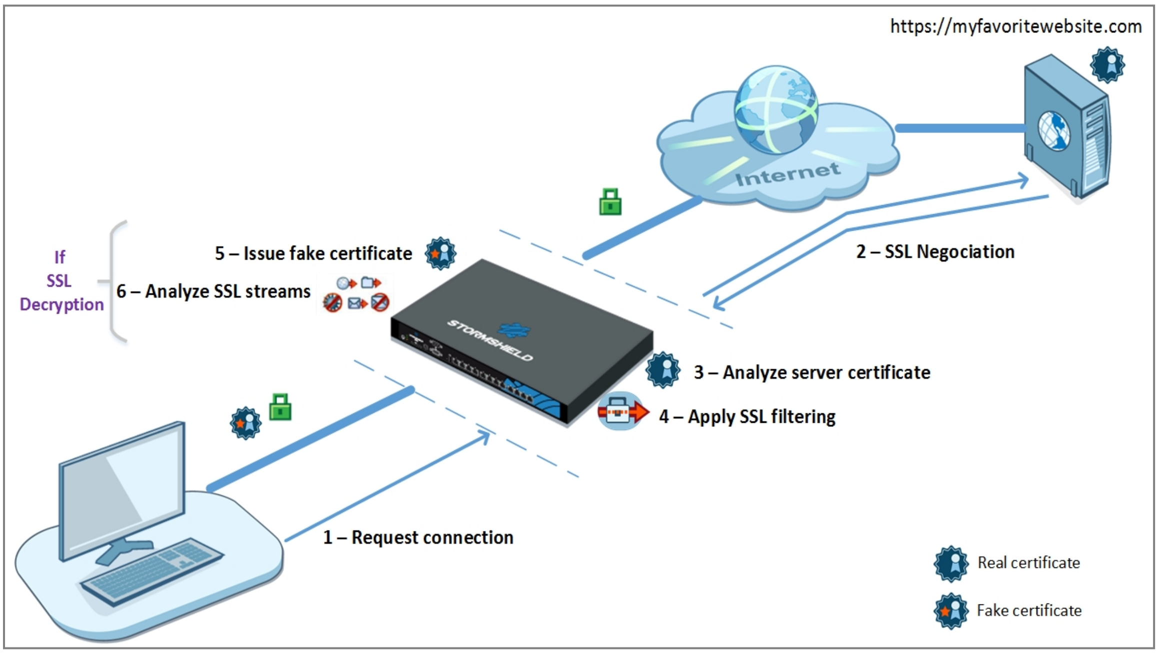
Summary

The table below shows the characteristics of each filtering method:

	Without decryption	With decryption
Blocking of HTTPS websites	X	X
Anti-virus analysis, sandboxing, SafeSearch, etc.		X
Display of customized block pages		X
A certificate must be installed on every workstation		X
Do not decrypt unauthorized websites and/or website categories	N/A	X
Access possible for devices without certificates (BYOD)	X	

How the SSL proxy works

The SSL proxy is placed as a "man in the middle" on the SSL traffic between the client and the web server. It manages SSL negotiations and thereby secures SSL proxy/server and SSL proxy/client connections. Between both sides, it allows or blocks connections according to the filter policy, and where necessary, it decrypts SSL traffic.



The various steps in SSL filtering are as follows:

1. The SSL proxy intercepts connections from the client over TCP port 443.
2. It carries out SSL negotiations with the web server on behalf of the client.
3. It analyzes the certificate sent by the server. If the certificate is non-compliant, access to the server will be blocked.
4. If the certificate is compliant, the SSL proxy will look up the SSL filter rules:
   - Block without decrypting: it blocks connections,
   - Pass without decrypting: it allows connections to pass through,
   - Decrypt: it decrypts traffic, which will then be evaluated by the filter rules that follow.
5. If the action is Decrypt, the SSL proxy will generate a fake certificate and present it to the client, which will verify the certificate. If the certificate from the signing authority has not been installed in the browser or on the system, and declared as a trusted authority, an error message will appear.
6. If the certificate is present, traffic will be secured. Application protections will then be applied (e.g., anti-virus, antispam, sandboxing).

NOTE
Steps 5 and 6 are relevant only if you apply filtering WITH SSL traffic decryption.

Configuring HTTPS filtering

This section sets out the various steps in the configuration of HTTPS filtering. Some of these apply only to either of the filtering methods (WITH or WITHOUT decryption). In such cases, you will be informed.

The steps in configuring HTTPS filtering are as follows:

Configuring the level of protection on the SSL protocol

Stormshield Network Security firewalls are configured by default with a restrictive level of protection for the SSL protocol: they reject all types of incorrect certificates and block traffic if decryption fails.

You can customize this configuration to fit your needs:

1. Log on to the web administration interface.
2. In the module **Configuration** > **Application protection** > **Protocols**, select the **SSL** protocol, then the profile *(0) ssl_01* (or another profile depending on your configuration).
3. In the **Proxy** tab, in the **Content inspection** area, select the action you wish to perform in cases where the certificates presented by remote servers are:
   - Self-signed certificates. Since they have not been signed by a trusted public certificate authority (CA), they can be more easily falsified. Stormshield recommends that you block them.
   - Expired certificates. They are no longer in the certificate revocation list (CRL) so it is impossible to know if they are still valid or have been revoked. Stormshield recommends that you block them.
   - Unknown certificates. Stormshield recommends that you block them.
   - Incorrect certificate type,
   - Certificates with incorrect FQDN,
   - When the FQDN of the certificate is different from the SSL domain name.

   Three types of actions are available:

   - **Block** the connection,
   - **Continue analysis** to scan traffic,
   - **Delegate to user**. This action, available from version v3.8.0, forces the browser to present a security alarm in order to inform the user of any potential risks. The user then bears the responsibility of disregarding the alarm if he wishes to access the requested website anyway. In this case, the administrator will also be notified through an alarm and a specific entry in the alarm log file.
4. Select the option **Allow IP addresses in SSL domain names** to access a website by using its IP address instead of its FQDN.

5. In the **Support** area, indicate which actions to perform when:
   - Decryption fails,
   - The certificate cannot be classified under any of the categories in the URL database (embedded URL database or Extended Web Control).
6. Click on **Apply**.

Defining SSL filter policies

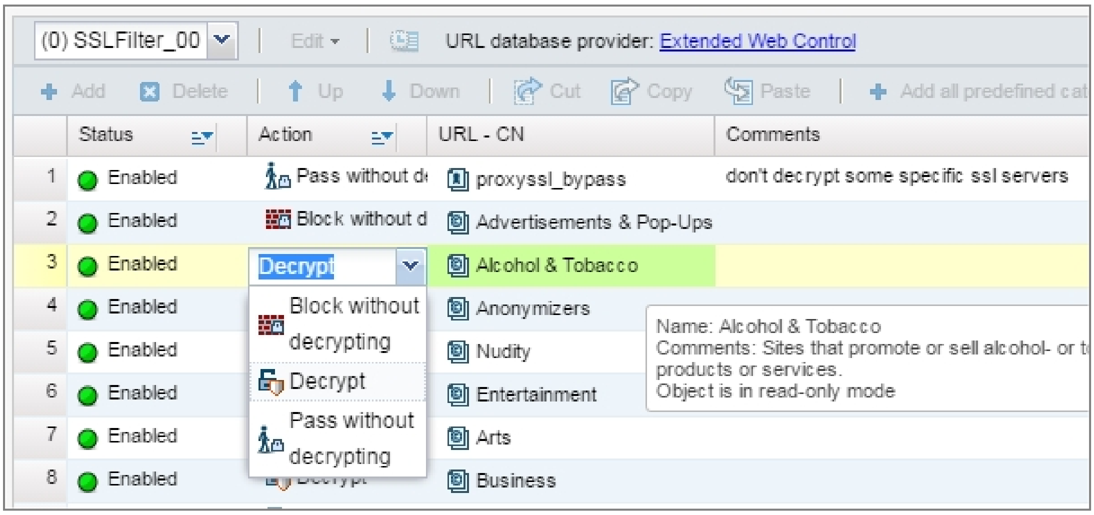
As soon as the remote server's certificate has been verified, the requested URL will be compared against all the rules in the SSL filter policy.

- An **SSL filter rule** describes the action that the SSL proxy needs to perform for a certain category of URLs or specific certificates. For example, you may choose to block all URLs that belong to the *Games* category.
- An **SSL filter policy** is a set of rules that the firewall will read sequentially.

Creating SSL filter policies

1. Log on to the web administration interface.
2. Select the **Configuration > Security policy > SSL Filtering** menu, and select a filter policy, for example *SSLFilter_00*. Two rules are already configured by default. In the first, certain URL-CNs are allowed to pass without decryption. The second rule specifies that all other rules need to be decrypted.
3. If you are filtering WITHOUT decrypting SSL traffic, delete both of the default rules.
4. Click on **Add all predefined categories**.
   A list of categories will appear, corresponding to your URL database (embedded URL database or Extended Web Control).
5. Delete all the categories to which you do not wish to apply SSL filtering.

6. For the remaining categories, in the **Action** column, choose the action that the firewall must perform on each URL-CN category. Refer to the section Best practices for filtering for help on which choices to make.



	Status	Action	URL - CN	Comments
1	Enabled	Pass without de	proxyssl_bypass	don't decrypt some specific ssl servers
2	Enabled	Block without d	Advertisements & Pop-Ups	
3	Enabled	Decrypt	Alcohol & Tobacco	
4	Enabled		Anonymizers	
5	Enabled		Nudity	
6	Enabled		Entertainment	
7	Enabled		Arts	
8	Enabled	Decrypt	Business	

Name: Alcohol & Tobacco
Comments: Sites that promote or sell alcohol- or t
products or services.
Object is in read-only mode

- **Block without decrypting**: The firewall will deny access to the requested URL-CN without performing any prior SSL analysis. Choose this action for all categories that you wish to block (e.g., weapons, violence, pornography, peer-to-peer, etc).
- **Pass without decrypting**: The firewall will allow access to the requested URL-CN without performing any prior SSL analysis. Choose this action for categories that you are not legally allowed to decrypt (e.g. websites containing private data) and for those that you consider trustworthy.
- **Decrypt**: The firewall will decrypt SSL traffic before allowing or denying access to the requested URL-CN. Use this action only if you have chosen filtering WITH SSL traffic decryption.

7. In the **URL-CN** column, select the URL category or certificate group (CN) concerned, for example *Violence*. If any categories are missing, you can create them through the menu **Objects** > **Web objects** > **URL tab** > **Add a customized category**. For more information, please refer to the section Customized categories.
8. Click on **Add** to create the other rules you would need in your policy and arrange them by using the **Up** and **Down** buttons or copy and paste them. To find out how to classify them, refer to the section Rule sequence.
9. Double-click in the **Status** column to enable the rules that have been created.
10. Click on **Apply**.

The SSL filter policy must then be associated with the security policy. For further information, refer to the section Creating SSL inspection rules in the filter policy.

Best practices for filtering

Refer to best practices for filtering whenever you build an SSL filter policy.

Legislation

As the decryption of private data is governed by law in most countries, SSL filtering must take such legislation into account. This means that websites that must not be decrypted must be excluded by applying the **Pass without decrypting** action. In France, the legal aspects of SSL decryption are set out in the appendix of the ANSSI's (French Net- work and Information Security

Agency) document *"Recommandations de sécurité concernant l'analyse des flux HTTPS*" (in French).

Customized categories

If the website categories that were predefined by your URL database do not exactly meet your needs, you can add categories available by default on the firewall, or create your own categories.

For example, in the category *proxyssl_bypass* you will find the list of certificates that Stormshield advises you to allow through without decryption. This is because these servers will detect that the SSL proxy is generating a fake certificate and may reject connections as a result.

You can also create the following categories to make it easier to build SSL filter rules:

- A whitelist category (*sslproxy_whitelist*) containing all the URLs that you deem trustworthy. For example, websites that legislation does not allow you to decrypt, your internal websites and system and software upgrade websites (e.g., Microsoft, antivirus etc.). Apply the action *Pass without decrypting* to this new category.
- A blacklist category (*sslproxy_blacklist*) containing URLs that you deem malicious and which you are unable to find in the predefined categories. Apply the action *Block without decrypting* to this new category.

Create your new categories through the menu **Objects > Web objects > URL tab > Add a customized category**. For more information, refer to the *Administration and configuration guide*.

Rule sequence

The SSL proxy runs through the list of rules from top to bottom. There are two ways in which you can organize your rules:

- **Itemize authorized categories**: Create a rule for each authorized category with the action *Pass without decrypting* or *Decrypt*. The last rule must block all other categories by specifying the action *Block without encrypting* for the URL-CN *Any*.
- **Itemize categories to be blocked**: Create a rule for each undesirable category with the action *Block without decrypting*. The last rule must allow all other categories by specifying the action *Pass without encrypting* or *Decrypt* for the URL-CN *Any*.

Do also note that in the Extended Web Control URL database, URLs are sometimes listed under several categories, so pay close attention to the alphabetical order of categories. For example, if a website falls under two categories such as *Entertainment* and *Nudity*, and you wish to block *Nudity* while allowing *Entertainment*, ensure that the category *Nudity* comes before *Entertainment* in the list of SSL filter rules. Otherwise, the website in question, which falls under the *Entertainment* category, will be allowed.

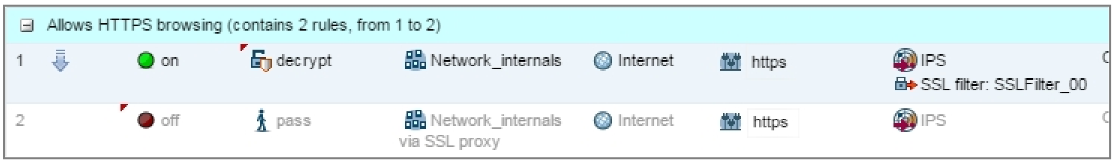
Creating SSL inspection rules in the filter policy

In order for your newly created SSL filter policy to be applied in the firewall's filter policy, you need to create an SSL inspection rule.

1. Log on to the web administration interface.
2. In the module **Configuration > Security policy > Filter - NAT**, select the **Filtering** tab.
3. In the drop-down list, select the filter policy with which SSL filtering needs to be associated.
4. Click on **New rule > SSL inspection rule**.

5. In the **Profile of traffic to be decrypted** area in the SSL inspection wizard, keep the default values to create a rule that will intercept all traffic originating from the internal network and going to the Internet over the port group *ssl_srv*. The port group *ssl_srv* contains standard ports of services that use TLS sessions: HTTPS, SMTPS, POP3S, etc. However, the SSL proxy does not manage FTPS.

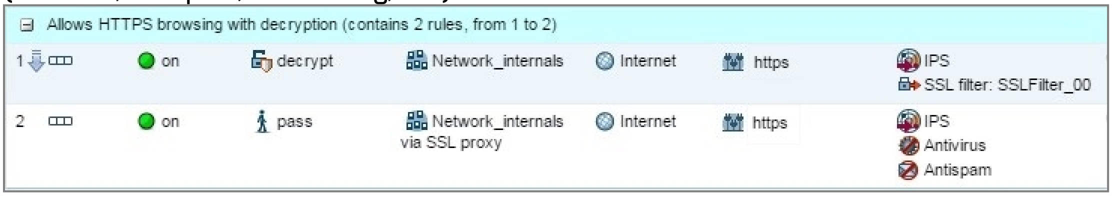
   Modify the values of fields where necessary if the default configuration is not suitable. For example, if you are using the SSL proxy only for HTTPS traffic, indicate *https* only instead of *ssl_srv* to minimize consumption of firewall resources. Use the port group *ssl_srv* only if all the protocols that it includes need to be decrypted.
6. In the **Inspect encrypted traffic** area, enter the following information:
   - **Inspection profile**: Select the desired inspection profile. For more information, refer to the *Administration and configuration guide*.
   - **SSL filter policy**: Select the filter policy that you have created in the section Defining SSL filter policies (*SSLFilter_00*).
7. Click on **Finish**. The wizard will generate two filter rules:
   - The first rule makes it possible to intercept traffic originating from the internal network to the Internet over the port group *ssl_srv*. All this traffic will be directed to the SSL proxy. This rule will apply SSL filtering and the Decrypt action.
   - The second rule allows traffic originating from the internal network and leaving through the SSL proxy to the Internet.
8. If you have chosen filtering WITHOUT decrypting SSL traffic, disable the second rule as it will not be used.



⊟ Allows HTTPS browsing (contains 2 rules, from 1 to 2)

1	● on	decrypt	Network_internals	Internet	https	IPS SSL filter: SSLFilter_00
2	● off	pass	Network_internals via SSL proxy	Internet	https	IPS

9. If you have chosen filtering WITH SSL traffic decryption, double-click in the **Security inspection** column of the second rule and enable the relevant application protection (antivirus, antispam, URL filtering, etc.).



⊟ Allows HTTPS browsing with decryption (contains 2 rules, from 1 to 2)

1	● on	decrypt	Network_internals	Internet	https	IPS SSL filter: SSLFilter_00
2	● on	pass	Network_internals via SSL proxy	Internet	https	IPS Antivirus Antispam

Filtering by user groups

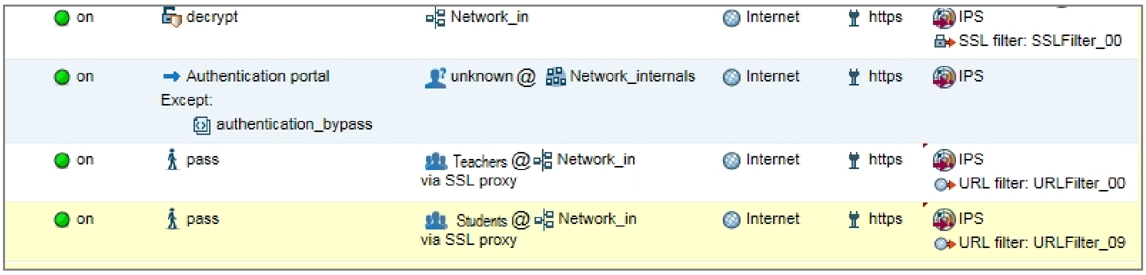
It is possible to set up different rules for different user groups. For example, in a school, you can have two groups – *Students* and *Teachers* – who will not have access to the same websites. After having created both of your SSL inspection rules:

1. Double-click on the second rule to edit it.
2. In the menu **Source > General tab > Users field**, select the user group that this SSL filter concerns (for example, the *Students* group).
3. Copy and paste both rules.
4. Double-click on the first rule that you have just copied to edit it.
5. In the menu**Source > General tab > Users field**, select the user group that this SSL filter concerns (for example, the *Teachers* group).

6. In the menu **Inspection > SSL filtering field**, select the SSL filter policy that you wish to associate with the *Teachers* group.

If users must authenticate whenever they attempt to log on to an HTTPS website, you need to add a rule that makes it possible to redirect them to the captive portal. This rule must be placed just after the decryption rule.

Add this rule using the menu **New rule - Authentication rule** in the **Filtering** tab, then adding *https* in the **Destination port**.



● on	decrypt	Network_in	Internet	https	IPS SSL filter: SSLFilter_00
● on	Authentication portal Except: authentication_bypass	unknown @ Network_internals	Internet	https	IPS
● on	pass	Teachers @ Network_in via SSL proxy	Internet	https	IPS URL filter: URLFilter_00
● on	pass	Students @ Network_in via SSL proxy	Internet	https	IPS URL filter: URLFilter_09

Configuring the signing authority and trusted authorities

Follow this procedure only if you have chosen filtering WITH SSL traffic decryption.

The SSL proxy signs fake certificates by default with the *SSL proxy default authority* already found on the firewall. Modify the signing authority if the default configuration is not suitable.

Likewise, you can customize the list of authorities or trusted certificates.

1. Log on to the web administration interface.
2. In the module **Configuration > Application protection > Protocols**, select the **SSL** protocol, then click on **Go to global configuration**.
3. In the **Proxy** tab, under **Generate certificates to emulate the SSL server**, specify the signing CA, its password and lifetime.
4. In the **Customized certificate authorities** tab, add the private authorities that you wish to trust.
5. In the **Public certificate authorities** tab, enable or disable the trusted authorities where necessary. The SSL proxy checks whether the remote server's certificate has been signed by a public or private trusted authority. The list of public authorities is automatically updated by the firewall's Active Update module.
6. In the **Trusted certificates** tab, add the certificates of servers that you wish to trust.
7. Click on **Apply**.

Deploying the certificate of the signing authority on browsers

Follow this procedure only if you have chosen filtering WITH SSL traffic decryption.

1. Log on to the web administration interface.
2. In the module **Configuration > Objects > Certificates and PKI**, select your signing authority.
3. Click on **Download**, and select **Certificate as a PEM file** or **Certificate as a DER file**.
4. Import the certificate into your operating system's or browser's certificate store using your usual deployment method.

> **NOTE**
> If some of your users have Chrome browsers, ensure that the digital hash of server certificates is in SHA-256 as described in this article in the Knowledge base.

Optimizing the performance of HTTPS filtering

The SSL proxy on the SNS firewall consumes a significant amount of memory. It allocates three sockets and four memory buffer zones to each HTTPS connection. TLS connections also require memory to manage cryptography and fake certificates.

The SSL proxy, like other SNS modules, can use only a limited amount of the firewall's memory. This is because memory is shared in such a way to allow all modules to run simultaneously.

If you notice memory issues while using the SSL proxy, check its parameters and perform the optimizations that Stormshield has recommended.

Getting parameters and statistics about the SSL proxy

It is important to know the capacity settings relating to the use of the SSL proxy. By intersecting such information, you will be able to anticipate potential memory issues and optimize your firewall's performance.

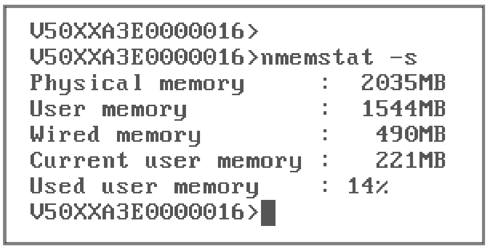
Finding out the firewall's memory settings

1. Log on to the firewall in SSH.
2. Enter one of the following commands:

```
nmemstat -s
```

- or -

```
sysctl hw.physmem
```

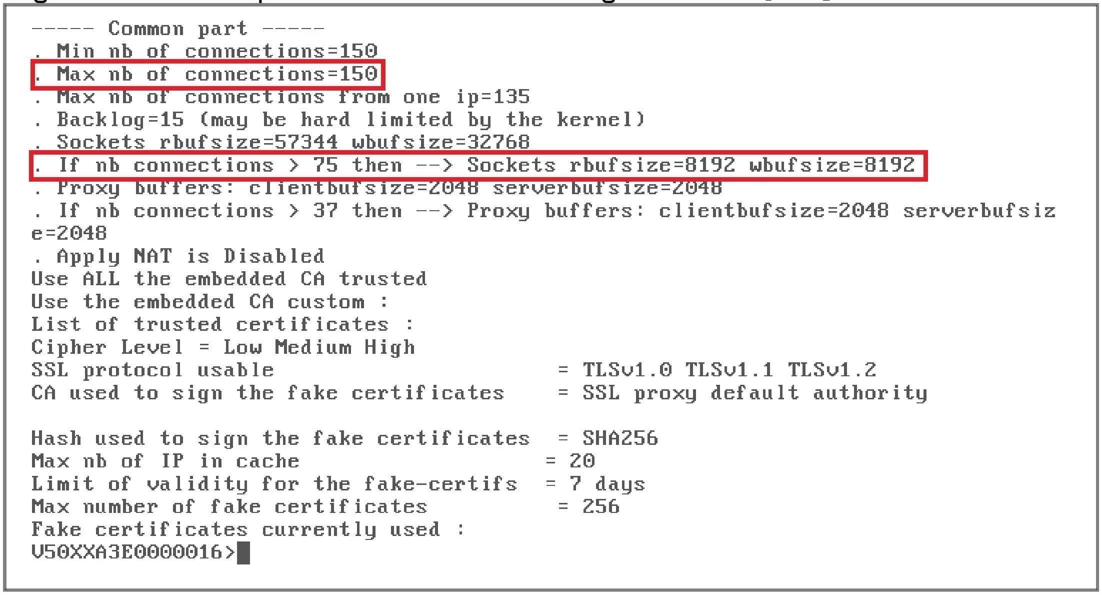


```
V50XXA3E0000016>
V50XXA3E0000016>nmemstat -s
Physical memory      :  2035MB
User memory          :  1544MB
Wired memory         :   490MB
Current user memory :   221MB
Used user memory     : 14%
V50XXA3E0000016>
```

In this example, the firewall has 2 GB of memory.

Finding out the SSL proxy's settings

1. Log on to the firewall in SSH.
2. To get the connection parameters, enter the following command: `tproxyd -s ssl`



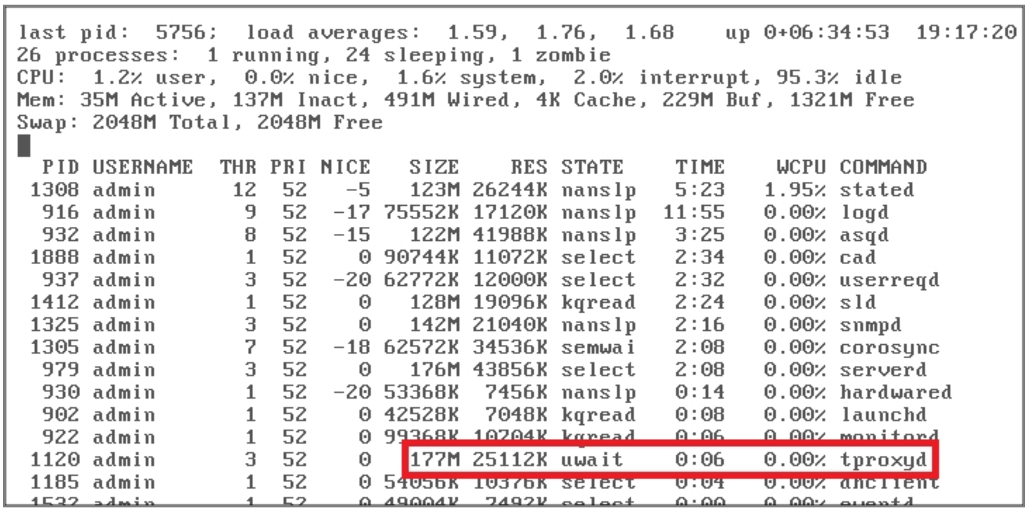
```
----- Common part -----
. Min nb of connections=150
. Max nb of connections=150
. Max nb of connections from one ip=135
. Backlog=15 (may be hard limited by the kernel)
. Sockets rbufsize=57344 wbufsize=32768
. If nb connections > 75 then --> Sockets rbufsize=8192 wbufsize=8192
. Proxy buffers: clientbufsize=2048 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>
```

In this example:

- The maximum number of connections allowed for the SSL proxy is 150.
- Buffer memory starts to decrease above 75 connections.

3. To find out the amount of memory that the SSL proxy uses, enter the following command: `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% dhclient
 1532 admin        1  52    0 49004K  7492K select   0:00   0.00% eventd
```

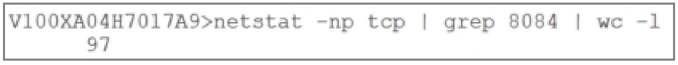
In this example, the SSL proxy uses 177 MB of memory.

Monitoring the SSL proxy's connections

To optimize the SSL proxy, it would be helpful to obtain statistics on the number of simultaneous SSL connections on your firewall. If this number is close to or often exceeds the maximum allowed by the SSL proxy, the firewall's performance may drop drastically. You are therefore advised to optimize the SSL proxy as recommended in the section Restricting the use of the SSL proxy.

1. Log on to the firewall in SSH.
2. Enter the following command to list out the number of filtered TCP connections open on port 8084:

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



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

In this example, there are 97 simultaneous connections.

Getting statistics on SSL connections

Two articles in the Stormshield Knowledge base provide explanations on how to obtain statistics for a given period:

- How can I enable proxy statistics?
- Proxy statistics understanding

To access the Knowledge base, use the ID for your MyStormshield personal area.

Alternatively, you can use an SNMP monitoring tool such as Nagios to obtain information about the `tproxyd` process, CPU, memory, etc. Refer to the Stormshield website for more information on compatible MIBs.

Restricting the use of the SSL proxy

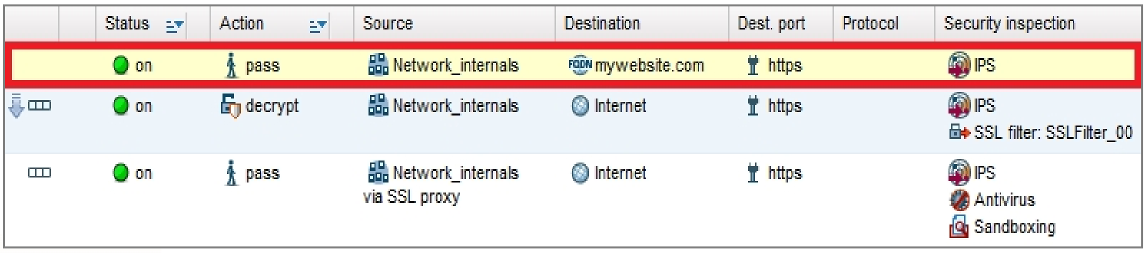
To optimize memory consumption, restrict the use of the SSL proxy by following the recommendations below.

Avoiding the SSL proxy for trusted websites

In order to restrict the use of the SSL proxy, you can allow direct connections for the most frequently visited trusted internal websites.

In the **Filtering** tab in the **Configuration** > **Security policy** > **Filter - NAT** module, add a single rule above your SSL rules with the following properties:

- **Action**: Pass
- **Destination**: FQDN object representing your trusted website (i.e., FQDN object *mywebsite.com* created beforehand).
- **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

In this example, any connection to the website *https://mywebsite.com* will be allowed without any redirection to the SSL proxy. It will therefore consume less memory and will not be deducted from SSL connections.

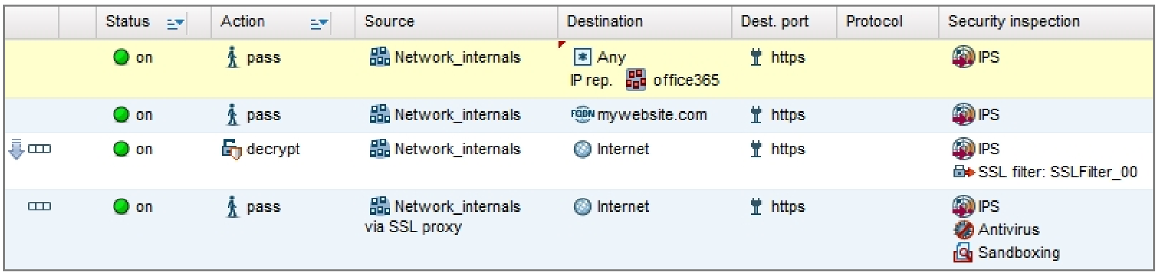
Add a rule for each trusted website.

Avoiding the SSL proxy for Office 365

If your users have Office 365 accounts, you can allow direct connections to all Office 365 resources without redirecting them to the SSL proxy.

In the **Filtering** tab in the **Configuration** > **Security policy** > **Filter - NAT** module, add a single rule above your SSL rules with the following properties:

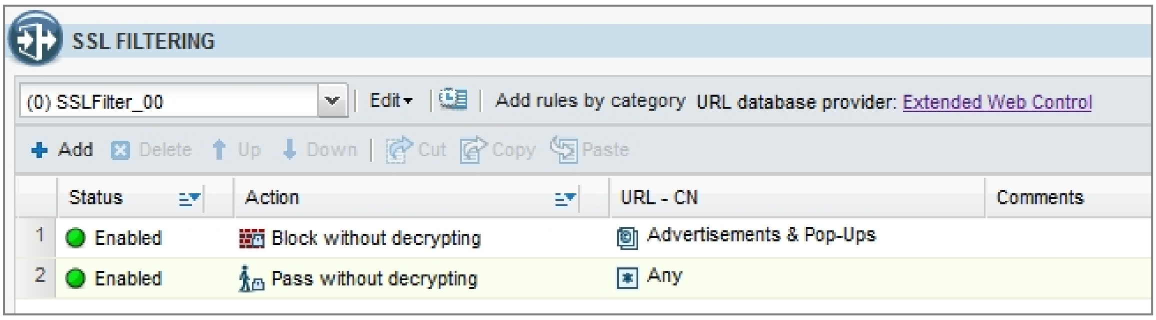
- **Action**: Pass,
- **Dest. port**: https,
- **Destination**: In the destination's **Geolocation/Reputation** tab, select the Office 365 reputation category.



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
	● on	pass	Network_internals	Any IP rep. office365	https		IPS
	● 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

Blocking advertisements

Whenever a user visits a web page, not only is he establishing a connection with the website in question, he is also connecting to many other advertising websites. To reduce the number of connections, you are therefore strongly advised to block advertising websites (*Ads* or *Advertisements & Pop-Ups*) in the SSL filter policy.



	Status	Action	URL - CN	Comments
1	● Enabled	Block without decrypting	Advertisements & Pop-Ups	
2	● Enabled	Pass without decrypting	Any	

Using the Extended Web Control URL database

In order to block as many URLs as possible and filter them more thoroughly, use the Extended Web Control URL database instead of the embedded URL database. This will boost performance as this database is not loaded in memory.

In the **URL database** tab in the **Configuration** > **Objects** > **Web Objects** module, select **Extended Web control** as the URL database provider

If you do not have the Extended Web Control option on your firewall, get in touch with your Stormshield contact.

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.