STORMSHIELD

TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

SSO CONFIGURATION: MICROSOFT SPNEGO

Product concerned: SNS 3.x

Document last update: October 6, 2021

Reference: sns-en-SSO_configuration_Microsoft_SPNEGO_technical_note

Table of contents

Getting started

Users have to manage many passwords – one for connecting to the workstation, one for the mail program and as many passwords as there are applications. Once this number reaches a dozen or so for certain users or administrators, managing these passwords then becomes tricky. This would encourage careless behavior, for example, in the form of simple passwords, or using the same passwords across all systems, or even passwords written on post-its or in notebooks.

The aim of protecting applications with passwords is to ensure the security of the data they contain. However, having too many passwords to manage multiplies the risk of them falling into the wrong hands, with dire consequences.

To resolve this dilemma, Single Sign-On (SSO) authentication programs were created, allowing users to authenticate only once to access all their resources, without having to systematically enter the individual passwords to each application.

SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) is a protocol that has been defined by the IETF, making it possible to negotiate between different GSS-API (Generic Security Service Application Program Interface) mechanisms in order to establish a common security context for a client and a server. This is the method that Stormshield has chosen to provide single authentication features.

GSS-API is a programming interface offering applications that access a set of security services. Among other possibilities, it allows handling user authentication and guaranteeing the confidentiality and integrity of each message exchanged. Furthermore, it provides a unique interface that places itself above the different security mechanisms in such a way that in the event one of the peers acquires GSS-API credentials for the same security mechanism, a security context can then be established between them.

Requirements

The following are required in order to run SSO (SPNEGO):

- An SNS firewall in version 3.x or higher,
- A domain controller in Windows Server 2012, 2012 R2, 2016 or 2019,
- The *spnego.bat* v1.7 script provided in the MyStormshield personal area (authentication required), under **Downloads > Downloads > Stormshield Network Security > TOOLS**.
- The following binary files on the server: *reg.exe*, *setspn.exe*, *ktpass.exe* and *ldifde.exe*.
- Workstations connected to the Active Directory domain, with an SPNEGO-compatible web browser.
  For best results, you are advised to use the latest version of Microsoft Internet Explorer, Microsoft Edge, Google Chrome and Mozilla Firefox (ESR version - Extended Support Release). For further information on these versions, please refer to the relevant vendors for the life cycles of their products.

Running SPNEGO with the firewall

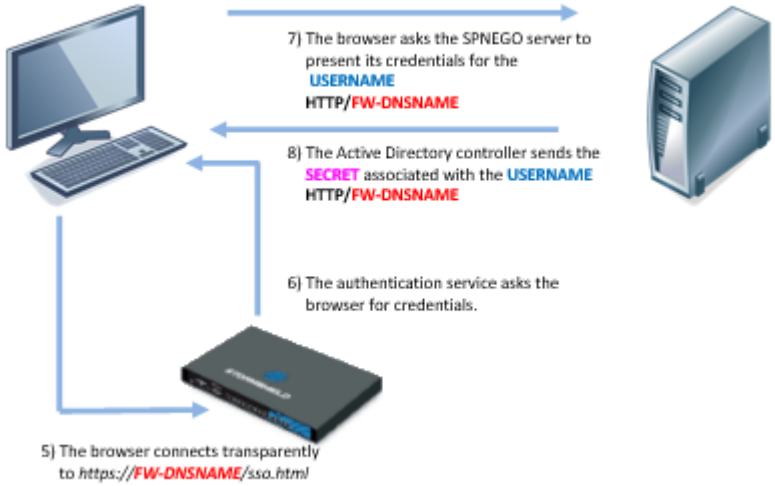
To explain how SPNEGO operates, this document will rely on the example of a user who wishes to access the Internet. The various phases of SPNEGO authentication are as follows:

1. The user authenticates on the network (Microsoft Active Directory domain).
2. The domain controller authorizes this authentication.

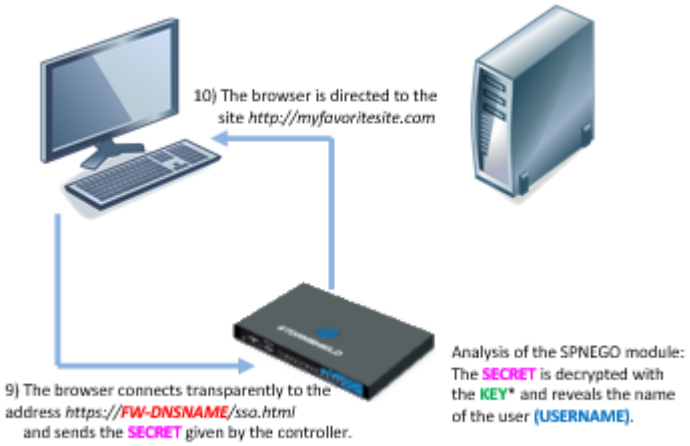
3. The user opens his web browser to connect to the website of his choice.
4. The HTTP proxy enabled on the firewall redirects the web browser to the authentication portal on the firewall.

5. The web browser will then connect transparently to the firewall's authentication portal using its serial number. In the diagrams, this serial number is represented by "FW-DNSNAME". For this purpose, this "FW-DNSNAME" has to be resolved by the DNS server configured on the client workstation.
6. The firewall will inform the web browser that it needs to issue a Kerberos client ticket associated with its service (SPN).
7. The web browser will then ask the domain controller to associate the ticket provided during exchange number 2 with the firewall's SPN service. USERNAME will then be associated with HTTP/FW-DNSNAME.

8. After having checked that the user has indeed been authenticated on the domain, the domain controller will provide the web browser with the requested information. In the diagrams, the ticket is represented as "SECRET" (USERNAME / HTTP/FW-DNSNAME pair).



9. The web browser forwards the new USERNAME / HTTP/FW-DNSNAME@Domain ticket to the firewall, which then decrypts its contents using the encryption key shared between the domain controller and the firewall (Keytab). The user is then authenticated for the duration defined by the administrator. In these diagrams, this key is represented by "KEY".
10. The firewall redirects the web browser to the firewall's HTTP proxy, which provides the user with the web page initially requested.



All the exchanges of information described above take place transparently for the user. The user does not need to either log on manually to the authentication portal or enter his login or password.

Exchanges (5) to (9) are encrypted: (5), (6) and (9) in SSL and exchanges (7) and (8) are made in plaintext with an encrypted Kerberos ticket (the Kerberos ticket cannot be used without an encryption key).

Note that there is no direct interaction between the firewall and the domain controller.

The clocks on the client workstation, domain controller and the firewall must all be synchronized, as any discrepancy of a few minutes may cause an authentication failure.

Configuring SPNEGO

A logical link needs to be created between Active Directory and the firewall in order for SSO (SPNEGO) to be used. This link is created in three steps:

1. Creation of a specific user account in Active Directory.
2. Creation of a logical link between this user account and the SSO service in Active Directory using the spnego.bat script..
3. Transferring a file produced from this association to the firewall via the administration interface in order to enable SPNEGO. Handle this file with care, as it contains a password (also called a "key"). Even though it is encrypted, it is still considered sensitive.

The configuration parameters of each component of the architecture need to be modified in order to set up SPNEGO features:

- The domain controller,
- The firewall,
- Client workstations (especially the web browser).

An appliance that does not appear in the diagrams also plays an important role – the DNS server.

Configuring the DNS server

One part of the SPNEGO mechanism requires the resolution of DNS names and in particular, the name of the firewall used. It is therefore necessary to add an entry to the DNS server so that the firewall's name can be resolved.

By default, its name is the firewall's serial number. Refer to the section Configuring SPNEGO in high availability on how to use a different name.

The configuration information described below is specific to DNS servers hosted on Microsoft Windows Server hosts (the AD domain controller, for example).

Creating the reverse lookup zone

If the reverse lookup zone dedicated to the network that includes the firewall's IP address does not yet exist, you need to create it (example: for the network 192.168.56.0/24, it is a 56.168.192-in-addr.arpa registration).

In this case, on the DNS server:

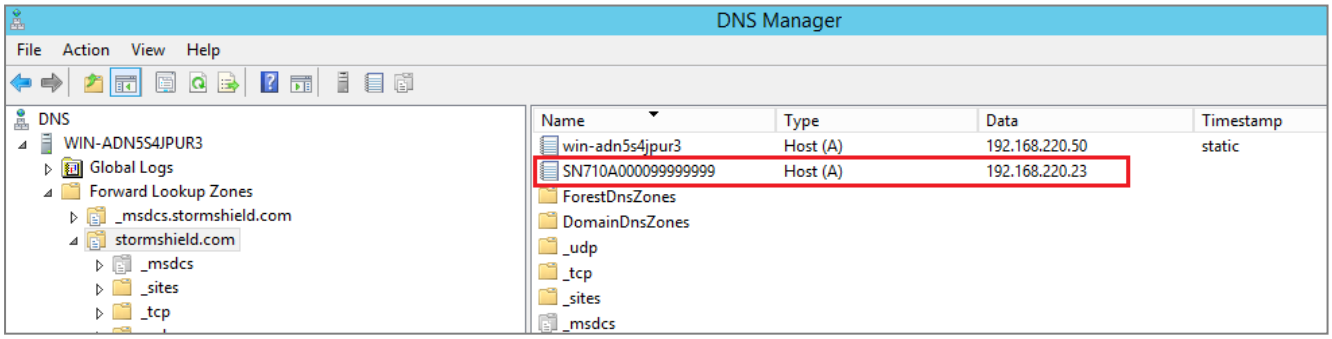
1. In the **Server Manager** dashboard, click on the **Tools** > **DNS** menu.
2. Right-click on **Reverse lookup zone**.
3. Select **New zone...**
   The reverse lookup zone wizard then launches.

4. Follow the various steps in the wizard, ensuring that you use the same parameters below:
   - Select **Main zone**.
   - Check that the **To all DNS servers running on domain controllers in this domain:** *domain_name* checkbox has been selected.
   - Select **Reverse IPv4 lookup zone**.
   - Enter the network containing the firewall's IP address.
     Examples:
     10.10 for a 10.10.0.0/255.255.00 network
     192.168.56 for a 192.168.56.0/255.255.255.0 network
   - Check that the **Allow only secure dynamic updates (recommended for Active Directory)** checkbox has been selected.

Creating the registration matching the name of the firewall

On the DNS server:

1. In the **Server Manager** dashboard, click on the **Tools** > **DNS** menu.
2. Expand the **Forward lookup zones** tree.
3. Right-click on the name of your domain.
4. Select **New host (A or AAAA)**.
5. In the **Name** field, enter the firewall's serial number.
6. In the **IP address** field, enter the firewall's IP address.
7. Click on **Add a host**.
8. Click on **Finish**.
   The new host will be added to the window on the right in the DNS Manager.



Using a client workstation, check whether name resolution works for the firewall's name (with the *ping* command, for example).

Configuring the Active Directory domain controller

1. On the server, check whether the binary files needed in the configuration of the domain controller are available:
   - *reg.exe* to handle the server's registry base,
   - *setspn.exe* to define the name of the service in the Active Directory,
   - *ktpass.exe* to retrieve the encryption key (keytab),
   - *ldifde.exe* to query the LDAP.

   Otherwise, retrieve them and save them in a shared folder which, if necessary, must be added to the PATH environment variable (e.g., *C:\SPNEGO*).
2. Retrieve the *spnego.bat* v1.7 script by logging in to your MyStormshield personal area (authentication required), under **Downloads > Downloads > Stormshield Network Security > TOOLS**. Save the script in the same folder as the one that contains the binary files in step 1.
3. In the command prompt, go to the directory containing the *spnego.bat* script (the files generated by the script will be added to the current directory).
4. Run the *spnego.bat* script using the command:

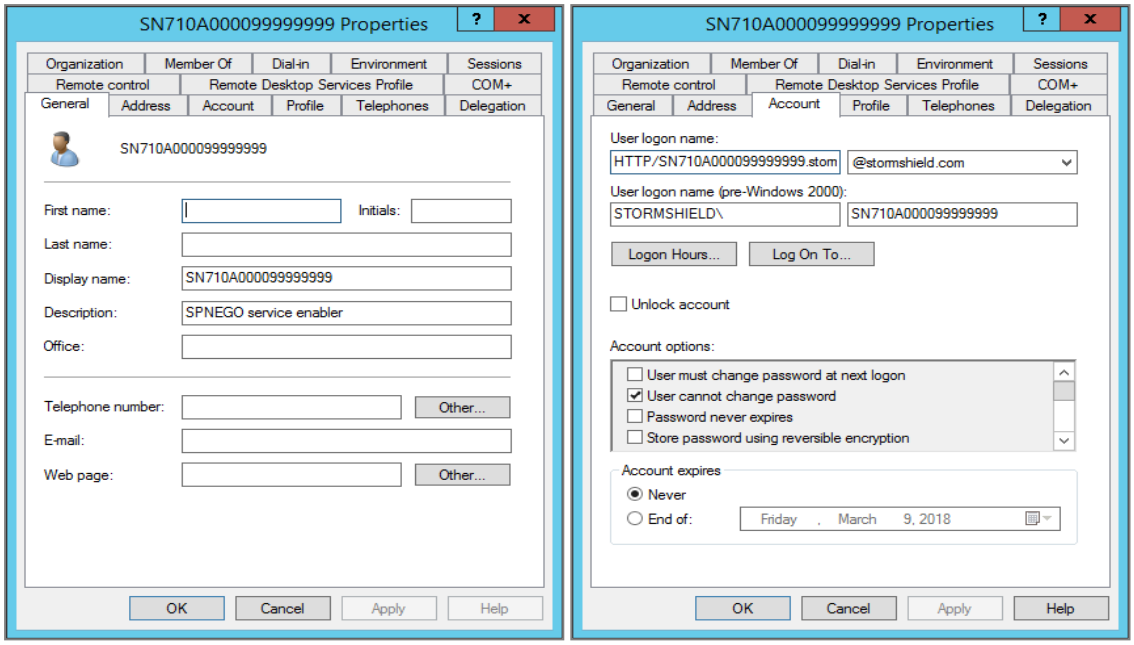
```
Spnego.bat <FW> <dns> <AD_Domain> <password> <file>
```

<FW>	Represents the name of the firewall on which you are configuring SPNEGO. This name is identical to the entry made in the DNS server. We recommend that you enter this parameter in UPPERCASE.
< dns>	Represents the DNS domain name (in the configuration of the DNS server, the DNS domain name will be *stormshield.com*). This parameter MUST be entered in LOWERCASE.
<AD_Domain>	Represents the Active Directory domain name handled by the domain controller. In most cases, this Active Directory domain name is the same as the DNS domain name. This parameter MUST be entered in UPPERCASE.
<password>	Represents the password that you have chosen and which will be used for the <FW> user created and the SPNEGO service. This password MUST NOT exceed 14 characters.
<file>	Represents the name of a file that you have chosen. This file contains an encryption key that needs to be installed during the configuration of the firewall.

5. Save the information indicated once the *spnego.bat* script has finished running. This information can also be found in the log file stored in the same folder as the script.

```
values to insert in the manager
SPN=HTTP/<FW>.<dns>
DOMAIN=<AD_Domain>
FILE=<file>
```

   - SPN is the name of the main service in the SPNEGO configuration (e.g., *HTTP/SN710A000099999999.stormshield.com*).
   - DOMAIN represents the Microsoft Active Directory domain name in the SPNEGO configuration (e.g., *STORMSHIELD.COM*).
6. Enable **support for AES 256-bit encryption via Kerberos** in the properties of the firewall account that was just created in Active Directory, in the **Account** tab, under **Account options**.


SN710A000099999999 Properties
Organization
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Delegation
SN710A000099999999
First name:
Initials:
Last name:
Display name:
SN710A000099999999
Description:
SPNEGO service enabler
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help
SN710A000099999999 Properties
Organization
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Delegation
User logon name:
HTTP/SN710A000099999999.stom
@stormshield.com
User logon name (pre-Windows 2000):
STORMSHIELD\
SN710A000099999999
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Friday , March 9, 2018
OK
Cancel
Apply
Help

Configuring the firewall

Your firewall is configured in three steps :

- Configuring the SPNEGO authentication method.
- Configuring the HTTP proxy redirection method.
- Configuring the filter policy.

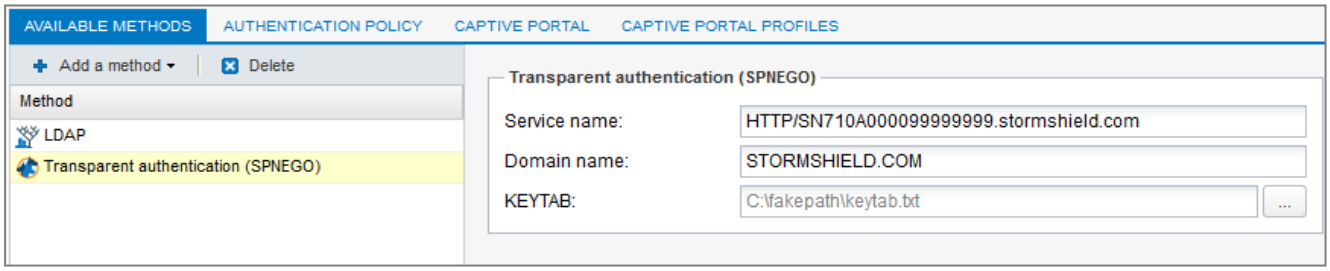
Configuring the SPNEGO authentication method

To configure the SPNEGO authentication method, go to the **Configuration** > **Users** > **Authentication** module in the web interface. Then refer to the following procedure.

In this example, SPNEGO is configured on the firewall's internal interfaces, through which clients can log on.

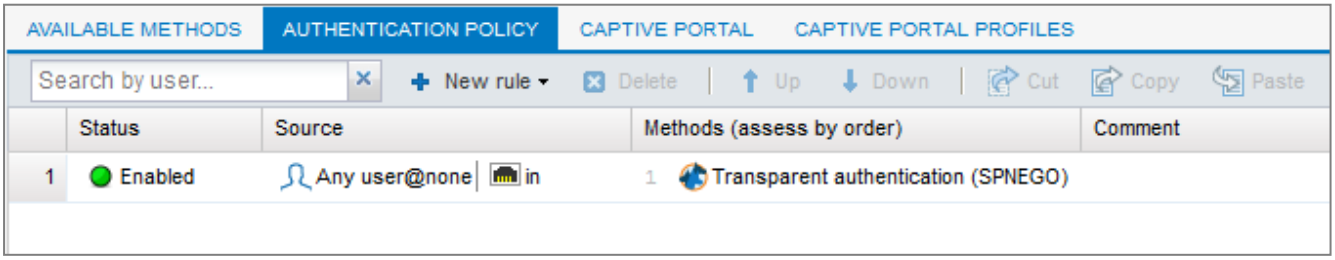
Available methods tab

1. Click on **Add a method** and select Transparent authentication (SPNEGO).
2. Fill in the **Service name** and **Domain name** fields with the information provided at the end of the log file (SPN and DOMAIN respectively), taking care the use the same case that was used when running the script on the domain controller.
3. Select the keytab file created using the spnego.bat script.
4. Apply changes.



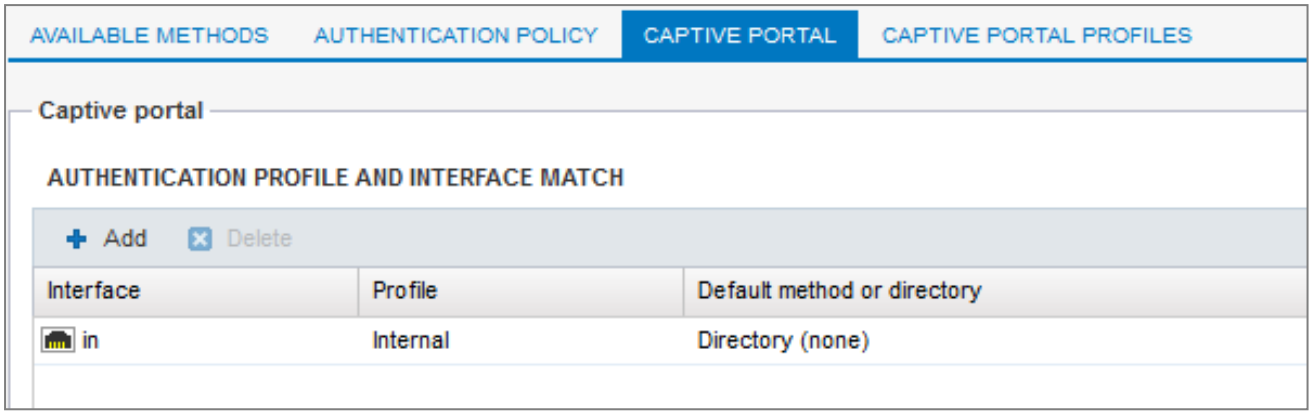
Authentication policy tab

1. Create a new rule (standard rule).
2. If no directories matching the Active Directory domain have been defined on the firewall, use the domain "none" (Any user@none) for users.
3. Select the connection source (*in* interface in the example).
4. Select the SPNEGO authentication method, then confirm.
5. Enable the rule by double-clicking in the **Status** column.



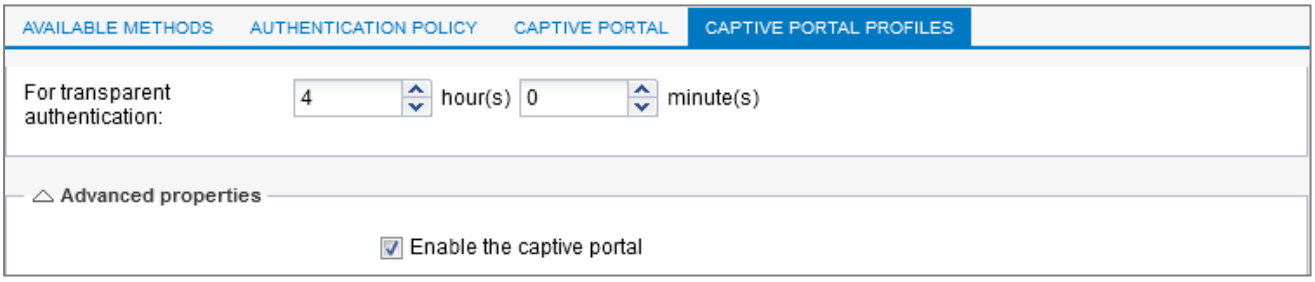
Captive portal tab

Next, associate the selected authentication profile (*Internal* in the example) with the various interfaces from which users will log on:



Captive portal profiles tab

1. In the authentication profile selected (*Internal* in the example), select the directory that will be used by default. It must match the directory entered in the authentication rule (*None* if no directories matching the Active Directory domain have been defined on the firewall).
2. In the **Advanced properties**, ensure that the **Enable the captive portal** checkbox has been selected.



Configuring the HTTP proxy redirection method

The HTTP proxy redirection method does not really need to be configured, but makes it possible to automate steps (3) to (5) of the SPNEGO process, a major advantage of this feature.

In the **Configuration** > **System** > **Configuration** module, **General configuration** > **Advanced properties** section:

1. In the **Redirect to the captive portal** field, select **Specify a domain name (FQDN)**.
2. In the **Domain name (FQDN)** field, enter the name of the firewall as it was added to the DNS server: *firewall_serial_number.AD_domain_name* by default (SN710A000099999999.stormshield.com in the example).

Configuring the filter policy

The filter policy required in the SPNEGO method consists of an authentication rule and a filter rule.

Adding an authentication rule

This rule is meant to redirect all Internet-bound HTTP connections by users that have not yet been authenticated to the captive portal instead.

1. In the **Configuration** > **Security Policy** > **Filter - NAT** module, click on **New rule** and select **Authentication rule**.

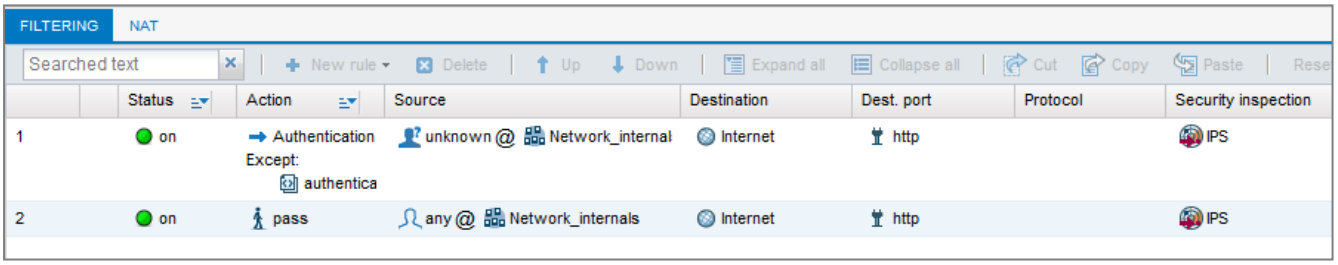
2. Change the predefined objects where necessary. In our example, we will use the objects suggested by default.

Adding a filter rule

This rule allows authenticated users to access the Internet:

1. In the active filter policy, click on **New rule** and select **Single rule**.
2. Double-click on this rule to edit it.
3. In the **Action** menu > **General** tab, select the **Action** *pass*.
4. In the **Source** menu > **General** tab, select the **User** *Any user@directory*. If no directories matching the Active Directory domain have been defined on the firewall, select *Any user@none*.
5. In the **Source** menu > **General** tab, select the **Source hosts** (e.g.: *Network_internals*).
6. In the **Destination** menu > **General** tab, select *Internet* as **Destination host**.
7. In the **Port / Protocol** > **Port** menu, select *http* as **Destination port**.
8. In the **Inspection** menu, select the desired application inspections (URL filtering, etc).
9. Confirm and enable this rule by double-clicking in the Status column.

The filter policy for the SPNEGO section will then look like this:



Configuring clients (web browsers)

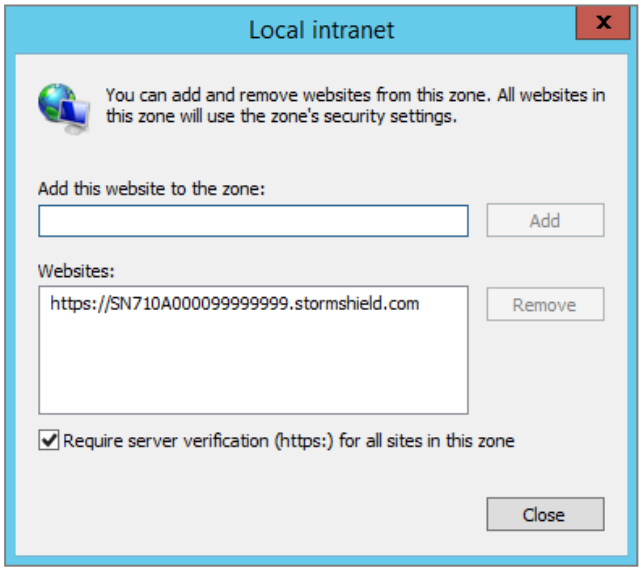
Before configuring your web browser, check that the authentication portal on the firewall used for SPNEGO can indeed be contacted from a client workstation:

1. Start the workstation's web browser.
2. Enter the URL *https://firewall_serial_number.dns_domain* (*https://SN710A000099999999.stormshield.com* in the example).
   If the portal does not appear, check your network connections and the configuration so far before going further.

Configuring Microsoft Edge and Google Chrome

The configuration of Microsoft Edge and Google Chrome is based on the **Internet options** in Microsoft Windows.

1. Open **Internet options** in one of the following ways:
   1. Start Internet Explorer and open the **Tools > Internet options** menu.
   2. Open the Windows **Run** program (press Windows + R) and type **inetcpl.cpl**.
2. In the **Security** tab, select **Local intranet**.
3. Click on **Sites,** then on **Advanced**.
4. Add the website *https://firewall_serial_number.dns_domain* to the zone (e.g., *https://SN710A000099999999.stormshield.com*).
5. Ensure that the option **Require server verification (https:) for all sites in this zone** has been selected.



6. Confirm and go back to the **Security** tab in the **Tools > Internet options** menu.
7. With the **Local intranet** selected, click on **Custom level**.
8. Under **Settings** > **User authentication** > **Logon**, check that the option **Automatic logon only in Intranet zone** has been selected.
9. Confirm and go back to the **Security** tab in the **Tools > Internet options** menu.
10. Open the **Advanced** tab, and under **Settings > Security**, ensure that **Enable Integrated Windows Authentication*** is checked.
11. Apply the configuration.

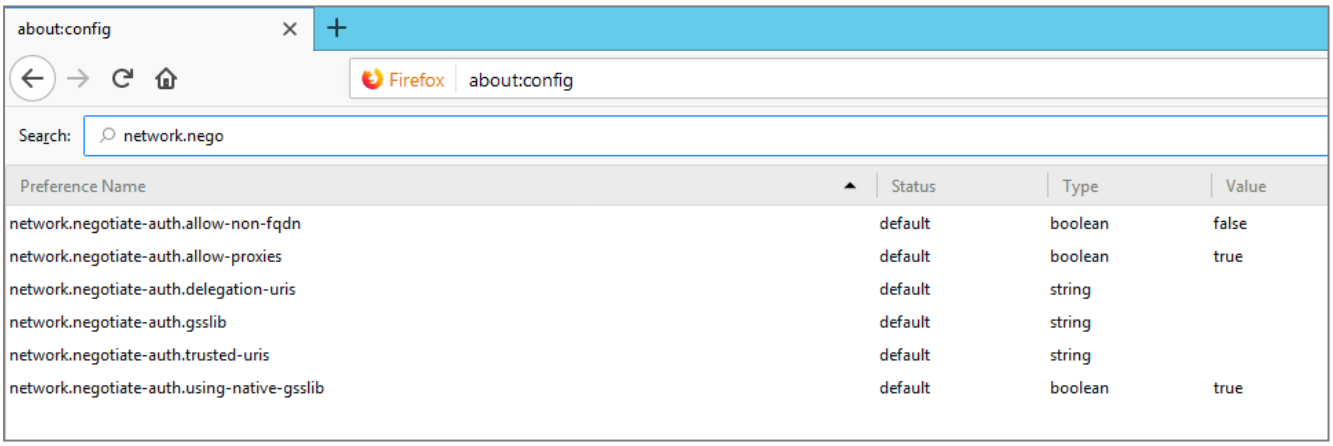
If you are accessing the Internet via a proxy, set up an exception for the firewall:

1. In **Tools > Internet Options**, select the **Connections** tab.
2. Click on **LAN settings** and select **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)**.
3. Click on **Advanced.**
4. In the **Exceptions** field, add *https://firewall_serial_number.dns_domain* (e.g., *https://SN710A000099999999.stormshield.com*).
5. Apply the configuration.

Configuring Mozilla Firefox

1. Start Firefox and type *about:config* in the URL address bar.
   A list of configuration parameters appears.
2. Using the search bar, edit the following parameters:
   1. *network.negotiate-auth.delegation-uris*,
   2. *network.negotiate-auth.trusted-uris*.

   For both of these parameters, enter the value https://firewall_serial_number.dns_domain (e.g., *https://SN710A000099999999.stormshield.com*).
3. Close the browser to confirm the configuration.



Configuring SPNEGO in High Availability

The SPNEGO configuration described in the earlier sections does not apply to high availability because this entire configuration is based on the identification of the firewall used for authentication, i.e., by its serial number.

In high availability, two firewalls do not have the same serial number. In such a configuration, the difference therefore consists of replacing each firewall's identifier (its serial number) with a single name for both members of the cluster.

As the SPNEGO protocol verifies the firewall's full domain name, this identifier must therefore be in the form of a *domain.name*.

Configuring SPNEGO by modifying the firewall's identifier

In this example, we need to replace *https://SN710A000099999999.stormshield.com* with *https://stormshield.portal.com*. To do so, you need to create a server certificate/private key pair under the name of the selected identifier:

- Either through a root authority created on each of the firewalls
- Or through specialized organizations such as Verisign, Thawte or others.

In the rest of this section, we will present the method based on certificates signed by a root authority of the firewall.

Creating the certificate authority

On the main firewall:

1. In the **Configuration** > **Objects** > **Certificates and PKI** module, click on **Add** and select **Add a root CA**.
2. In the **CN** field, enter the name of the authority (e.g.: **CA-SPNEGO**).
   The **ID** suggested by default will take on this name.
3. In **Certificate authority attributes**, fill in the **Organization** (mandatory), **Organizational Unit** (mandatory), **Locality** (optional), **State or province** (mandatory) and **Country** (mandatory) fields
4. Click on **Next**.
5. Type and confirm the **CA password**.
6. Unless there is a specific need, leave the suggested **Validity** and **Key size** values as is.
7. Click on **Next**.
8. Indicate any potential CRL distribution points.
9. Click on **Next**.
10. Confirm the creation of the authority by clicking on **Finish**.

Creating the server certificate

On the main firewall:

1. In the **Configuration** > **Objects** > **Certificates and PKI** module, click on **Add** and select **Server identity**.

2. In the **Fully qualified domain name (FQDN)** field, indicate the chosen ID (*stormshield.portal.com* in the example).
3. Click on **Next**.
4. Select the **Certificate authority** created earlier (**CA-SPNEGO** in the example) to sign this certificate.
   The attributes of the certificate are automatically filled in with the authority's attributes.
5. Enter the **CA password**;
6. Click on **Next**.
7. Unless there is a specific need, leave the suggested **Validity** and **Key size** values as is.
8. Click on **Next**.
9. Confirm the creation of the certificate by clicking on **Finish**.

Customizing the captive portal

On the main firewall, modify the captive portal so that it presents the ID of the cluster instead of the firewall's serial number:

1. Go to the **Configuration** > **Users** > **Authentication** menu > **Captive portal** tab,
2. In the **Certificate (private key)** field, select the certificate created earlier.

Finishing the configuration of SPNEGO

Once the certificate has been assigned to the captive portal, SPNEGO configuration will be the same as for the initial procedure for modifying the client configuration on the DNS server, except for the following:

1. You need to add the entry *custom_ID* to the DNS server. Therefore the string "firewall_serial_number.dnsdomain" needs to be replaced with *custom_ID*". In this example, *https://SN710A000099999999.stormshield.com* is therefore replaced with *https://stormshield.portal.com*.
2. When the *spnego.bat* script is used, the <FW> variable representing the firewall's ID now takes on the value *"custom_ID"* without the name of the DNS domain. In this example, it is therefore *portal*.

Frequently encountered issues

When the *spnego.bat* script is run, various error messages may appear.

Issue 1

If any of the following messages appears:

- "Some arguments are missing, please provide the correct arguments."
- “Too many arguments, please provide the correct arguments”.

Check whether the arguments <FW>, <dns>, <WINDOWS>, <password> and <file> are present. Each of these arguments is needed to run the script.

Issue 2

If the following message appears:

- "The file *keytab_filename* already exists, please choose another filename to output the keytab."

A keytab file with the provided name already exists in the folder in which the script is to be run. Rename this file.

Issue 3

If any of the following messages appears:

- "The setspn program is not present on the system or is not in the path".
- "The ktpass program is not present on the system or is not in the path".
- "The reg program is not present on the system or is not in the path".
- "The ldifde program is not present on the system or is not in the path".

Check whether support tools or the path are present in the system.

Issue 4

If any of the following messages appears:

- "This computer does not seems to be running Windows XXXX Server or Windows YYYY Server >> %log%".
- "This computer does not seem to be running a Server edition of Windows".
- "This script should only be run on a Windows Domain Controller which requires a Server edition of Windows".

Ensure that your version of Microsoft Windows is compatible with the running of the *spnego.bat* script.

Issue 5

If any of the following messages appears:

- Creating the user returned an error, please check your arguments.
- It is possible that your password restrictions applied.
- Setting the principal name returned an error, please check your arguments.
- Creating the keytab file did not work, please check your arguments.

A possible solution:

- The user creation process has been disrupted. Check that the password complies with the security policy.
- Check that the user running the script has sufficient privileges to create a new one.
- Check that the user has sufficient privileges to create the service name.
- Check that the user has sufficient privileges to create the keytab.

Further reading

Additional information and responses to questions you may have about the SPNEGO method are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu