



STORMSHIELD



NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURATION SSO : MICROSOFT SPNEGO

Produits concernés : SNS 3.x, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-configuration_SSO_Microsoft_SPNEGO_note_technique



Table des matières

Avant de commencer	3
Pré-requis	4
Fonctionnement de SPNEGO avec le firewall	4
Configurer SPNEGO	7
Configurer le serveur DNS	7
Créer la zone de recherche inversée	7
Créer l'enregistrement correspondant au nom du firewall	8
Configurer le contrôleur de domaine Active Directory	8
Configurer le firewall	10
Configurer la méthode d'authentification SPNEGO	10
Configurer la méthode de redirection du proxy	11
Configurer la politique de filtrage	11
Configurer les clients (navigateurs WEB)	12
Configurer Microsoft Internet Explorer, Microsoft Edge et Google Chrome	12
Configurer Mozilla Firefox	13
Configurer SPNEGO dans le cadre de la Haute Disponibilité	15
Configurer SPNEGO en modifiant l'identifiant du firewall	15
Créer l'autorité de certification	15
Créer le certificat serveur	15
Personnaliser le portail captif	16
Terminer la configuration de SPNEGO	16
Problèmes fréquemment rencontrés	17
Pour aller plus loin	18



Avant de commencer

Un utilisateur doit gérer de nombreux mots de passe : un mot de passe pour la connexion au poste de travail, un mot de passe pour la messagerie et de multiples mots de passe applicatifs. Quand ce nombre atteint une dizaine ou une quinzaine pour certains utilisateurs ou administrateurs, la gestion de ces mots de passe devient alors problématique. En effet, cela encourage un comportement négligent, qui se manifeste par exemple sous forme de mots de passe simples, mots de passe identiques sur tous les systèmes, ou des mots de passe notés sur des post-it ou dans un cahier.

L'objectif de cette protection des applications par le biais d'un mot de passe est d'assurer la sécurité des données qu'elles contiennent. En revanche, avoir trop de mots de passe à gérer multiplie les risques que ceux-ci tombent aux mains de personnes mal intentionnées, engendrant de lourdes conséquences.

Ce dilemme a donné lieu à la création du programme à authentification unique, ou SSO pour « Single Sign-On » en anglais. Il permet aux utilisateurs de s'authentifier une seule fois pour accéder à toutes leurs ressources, sans devoir saisir systématiquement les mots de passe propres à chaque application.

SPNEGO (Simple and Protected GSS-API Negotiation Mechanism, mécanisme de négociation de GSS-API simple et protégé) est un protocole défini par l'IETF, rendant possible la négociation entre différents mécanismes GSS-API (Generic Security Service Application Program Interface) afin d'établir un contexte de sécurité commun pour un client et un serveur. Ceci est la méthode choisie par Stormshield pour offrir les fonctionnalités d'authentification unique.

La GSS-API est une interface de programmation mettant à disposition des applications faisant appel à un ensemble de services liés à la sécurité. Elle permet entre autres de prendre en charge l'authentification d'un utilisateur, et de garantir la confidentialité et l'intégrité de chaque message échangé. De plus, elle fournit une interface unique prédominant les différents mécanismes de sécurité. De cette manière, si les correspondants acquièrent les crédences GSS-API pour le même mécanisme de sécurité, un contexte de sécurité sera établi entre eux.



Pré-requis

Pour faire fonctionner le SSO (SPNEGO) avec les Firewalls SNS, les outils suivants sont nécessaires :

- Un Firewall Stormshield en version 3 ou supérieure,
- Un serveur Windows avec Active Directory activé et configuré. Les versions Microsoft Windows Server compatibles sont les suivantes :
 - Windows Server 2008 et 2008 R2,
 - Windows Server 2012 et 2012 R2,
 - Windows Server 2016.
- Le script *spnego.bat* v1.6 disponible dans votre Espace Client. Ce script requiert la présence des outils système suivants sur le serveur :
 - *Reg.exe* pour manipuler la base de registre du serveur,
 - *Setspn.exe* pour définir le nom de service dans l'annuaire Active Directory,
 - *Ktpass.exe* pour récupérer la clé de chiffrement (keytab),
 - *Ldifde.exe* pour interroger la base LDAP.

NOTE

- Des postes de travail connectés sur le domaine Active Directory, pourvus d'un navigateur compatible avec SPNEGO. Pour un fonctionnement optimal de SPNEGO, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Internet Explorer, Microsoft Edge, Google Chrome et Mozilla Firefox (version ESR - Extended Support Release). Pour de plus amples renseignements sur ces versions, nous vous invitons à consulter le Cycle de Vie des Produits des éditeurs concernés.

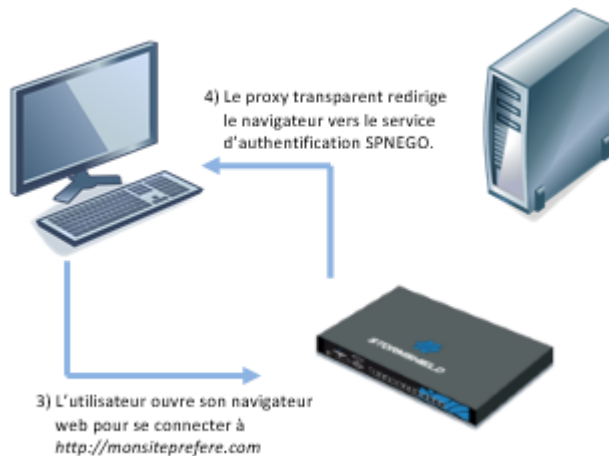
Fonctionnement de SPNEGO avec le firewall

Pour expliquer le principe de fonctionnement de SPNEGO, ce document prend l'exemple d'un utilisateur souhaitant accéder à Internet. Les différentes phases de l'authentification SPNEGO sont les suivantes :

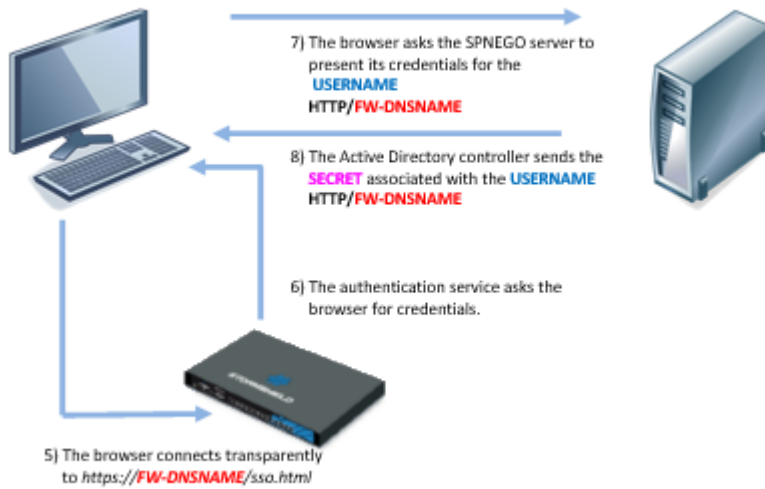
1. L'utilisateur s'authentifie sur le réseau (Domaine Microsoft Active Directory).
2. Le contrôleur de domaine autorise cette authentification.



3. L'utilisateur ouvre son navigateur Web pour se connecter au site Internet de son choix.
4. Le proxy HTTP activé sur le firewall redirige le navigateur Web vers le portail d'authentification sur le firewall.



5. Le navigateur Web se connecte de manière transparente sur le portail d'authentification du firewall en utilisant le numéro de série de ce dernier. Dans les schémas, ce numéro de série est représenté par « **FW-NOMDNS** ». Dans cette optique, il est nécessaire que ce « **FW-NOMDNS** » soit résolu par le serveur DNS configuré sur le poste client.
6. Le firewall informe le navigateur Web qu'il doit lui fournir un ticket client Kerberos associé à son service [SPN].
7. Le navigateur Web demande au contrôleur de domaine d'associer le ticket fourni lors de l'échange numéro 2 au service SPN du firewall. L'association est donc effectuée entre **USERNAME** et **HTTP/FW-NOMDNS**.
8. Après avoir vérifié que l'utilisateur est effectivement authentifié sur le domaine, le contrôleur du domaine fournit au navigateur Web le ticket demandé. Dans les schémas, le ticket est représenté par le « **SECRET** » (Paire **USERNAME** / **HTTP/FW-NOMDNS**).



9. Le navigateur Web transfère le nouveau ticket `USERNAME / HTTP/FW-NOMDNS@Domaine` au firewall qui en déchiffre le contenu grâce à une clé de chiffrement commune entre le contrôleur de domaine et le firewall (Keytab). L'utilisateur est alors authentifié pour une durée définie par l'administrateur. Dans les schémas, cette clé est représentée par « KEY ».
10. Le firewall redirige le navigateur Web vers le proxy HTTP du firewall qui fournit à l'utilisateur la page Web initialement demandée.



Tous les échanges d'informations décrits dans cet exemple s'effectuent de manière transparente pour l'utilisateur. L'utilisateur n'a ni besoin de se connecter manuellement au portail d'authentification, ni de renseigner son login ou son mot de passe.

Les échanges [5] à [9] sont chiffrés : [5], [6] et [9] en SSL et les échanges [7] et [8] se font en clair avec un ticket Kerberos chiffré [le ticket Kerberos est inexploitable sans la clé de chiffrement].

Il n'y a aucune interaction directe entre le firewall et le contrôleur de domaine.

Il est impératif que les horloges du poste client, du contrôleur de domaine et du firewall soient synchronisées. En effet un écart de quelques minutes peut entraîner un échec de l'authentification.



Configurer SPNEGO

Il faut créer une liaison logique entre Active Directory et le firewall afin de pouvoir utiliser le SSO (SPNEGO). Cette liaison est réalisée en 3 étapes :

1. Création d'un compte utilisateur spécifique dans l'annuaire Active Directory.
2. Mise en relation logique dans l'Active Directory de ce compte utilisateur et du service SSO à l'aide d'un script (spnego.bat : disponible dans l'espace client [Mystormshield](#)).
3. Transfert au firewall d'un fichier issu de cette mise en relation par l'intermédiaire de l'interface d'administration afin d'activer SPNEGO. Manipulez ce fichier avec précaution, car celui-ci contient un mot de passe (aussi appelé une « clé »). Malgré le chiffrement, il reste considéré comme sensible.

La mise en place des fonctionnalités SPNEGO nécessite également la modification des paramètres de configuration de chacun des éléments participant à l'architecture :

- Le contrôleur de domaine,
- Le firewall,
- Les postes clients (et notamment le navigateur Web).

Un équipement n'apparaissant pas sur les schémas joue également un rôle important : un serveur DNS.

Configurer le serveur DNS

Une partie du mécanisme SPNEGO nécessite la résolution de noms DNS et en particulier celui du firewall utilisé. Il est donc nécessaire d'ajouter une entrée dans le serveur DNS de manière à permettre la résolution du nom du firewall.

Par défaut, ce nom est le numéro de série du firewall. Référez-vous à la section [Configurer de SPNEGO dans le cadre de la Haute Disponibilité](#) pour l'utilisation d'un nom différent.

Les informations de configuration décrites ci-dessous sont propres à un serveur DNS hébergé sur une machine Microsoft Windows Server (le contrôleur de domaine AD par exemple).

Créer la zone de recherche inversée

Si la zone de recherche inversée dédiée au réseau incluant l'adresse IP du firewall n'existe pas encore, vous devez la créer (exemple : pour le réseau 192.168.56.0/24, il s'agit d'un enregistrement du type 56.168.192-in-addr.arpa).

Dans ce cas, sur le serveur DNS :

1. Dans le tableau de bord du **Gestionnaire de serveur**, cliquez sur le menu **Outils > DNS**.
2. Faites un clic droit sur **Zone de recherche inversée**.
3. Sélectionnez **Nouvelle zone...**
L'assistant de création de zone de recherche inverse se lance.
4. Suivez les différentes étapes de l'assistant en respectant les paramètres suivants :
 - Sélectionnez **Zone principale**.
 - Vérifiez que la case **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine** : *domain_name* est cochée.
 - Sélectionnez la case **Zone de recherche inversée IPv4**.



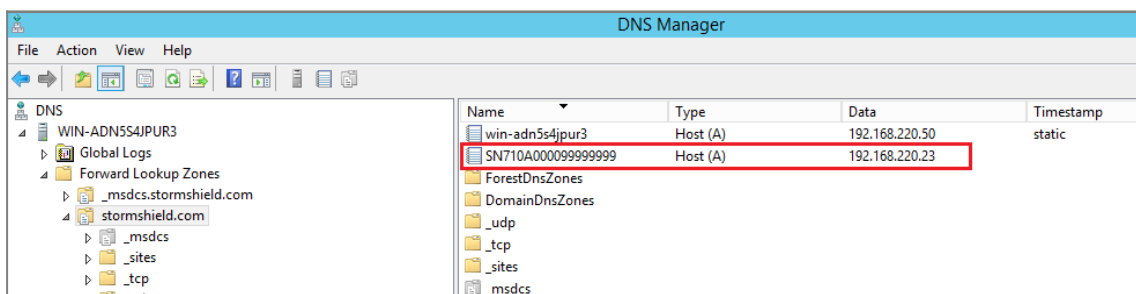
- Saisissez le réseau contenant l'adresse IP du firewall.
Exemples :
10.10 pour un réseau 10.10.0.0/255.255.00
192.168.56 pour un réseau 192.168.56.0/255.255.255.0
- Vérifiez que la case **N'autoriser que les mises à jour dynamiques sécurisées (recommandé par Active Directory)** est cochée.

Créer l'enregistrement correspondant au nom du firewall

Sur le serveur DNS :

1. Dans le tableau de bord du **Gestionnaire de serveur**, cliquez sur le menu **Outils > DNS**.
2. Développez l'arborescence **Zones de recherche directes**.
3. Faites un clic droit sur le nom de votre domaine.
4. Sélectionnez **Nouvel hôte (A ou AAAA)**.
5. Dans le champ **Nom**, renseignez le numéro de série du firewall.
6. Dans le champ **Adresse IP**, renseignez l'adresse IP du firewall.
7. Cliquez sur **Ajouter un hôte**.
8. Cliquez sur **Terminer**.

Le nouvel hôte est ajouté dans la fenêtre de droite du gestionnaire DNS.



Vérifiez depuis un poste client que la résolution du nom du firewall fonctionne (à l'aide d'une commande *ping* par exemple).

Configurer le contrôleur de domaine Active Directory

Modifiez la configuration du contrôleur de domaine Active Directory :

1. Sur le serveur, vérifiez la disponibilité des binaires nécessaires à la configuration du contrôleur de domaine : « reg.exe », « setspn.exe », « ktpass.exe » et « ldifde.exe ».
2. S'ils ne sont pas disponibles, récupérez-les (cf. [Pré-requis](#) selon la version de Microsoft Windows Server) et enregistrez-les dans un répertoire commun qui devra, si nécessaire, être ajouté à variable d'environnement PATH. Exemple « C:\SPNEGO\ ».
3. Récupérez le script *spnego.bat* dans votre espace client **Mystormshield** (menu **Téléchargements > Stormshield Network Security > Tools**) et enregistrez-le dans le même répertoire qu'à l'étape [2].
4. Dans l'invite de commande, placez-vous dans le répertoire contenant le script *spnego.bat* (les fichiers générés par le script seront ajoutés dans le répertoire courant).



5. Lancez le script *spnego.bat* à l'aide de la commande :

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

Où :

- <FW> représente le nom du firewall sur lequel vous configurez SPNEGO. Ce nom est identique à l'entrée effectuée dans le serveur DNS. Stormshield vous recommande de renseigner ce paramètre en MAJUSCULES.
 - <dns> représente le nom de domaine DNS (dans la configuration du serveur DNS ci-dessus le nom de domaine DNS serait « stormshield.com »). Ce paramètre DOIT être renseigné en MINUSCULES.
 - <AD_Domain> représente le nom de domaine Microsoft Active Directory pris en charge par le contrôleur de domaine. Dans la très grande majorité des cas ce nom de domaine Microsoft Active Directory est identique au nom de domaine DNS. Ce paramètre DOIT être renseigné en MAJUSCULES.
 - <password> représente le mot de passe que vous choisissez et qui sera utilisé pour l'utilisateur <FW> créé et le service SPNEGO. Ce mot de passe NE DOIT PAS comporter plus de 14 caractères.
 - <fichier> représente un nom de fichier que vous choisissez. Ce fichier contient une clé de chiffrement à installer lors de la configuration du firewall.
6. Avant de continuer la configuration, il est important d'enregistrer les informations indiquées à la fin de l'exécution du script *spnego.bat* :

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

- SPN est le nom du service principal de la configuration SPNEGO. Dans l'exemple présenté ce SPN serait « HTTP/SN710A000099999999.stormshield.com ».
- DOMAIN est le nom de domaine Microsoft Active Directory de la configuration SPNEGO. Dans l'exemple présenté ce DOMAIN serait « STORMSHIELD.COM ».

Ces informations sont disponibles dans le fichier log stocké dans le même répertoire que le script.

Exemple des détails de l'utilisateur créé sur le contrôleur de domaine grâce au script *spnego.bat* :

The image shows two side-by-side screenshots of the 'SN710A000099999999 Properties' dialog box. The left screenshot shows the 'General' tab with fields for first name, last name, display name (SN710A000099999999), and description (SPNEGO service enabler). The right screenshot shows the 'Account' tab with fields for user logon name (HTTP/SN710A000099999999.stom@stormshield.com) and user logon name (pre-Windows 2000) (STORMSHIELD\SN710A000099999999). It also shows account options like 'User cannot change password' and 'Password never expires'.



AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	CAPTIVE PORTAL PROFILES
Captive portal			
AUTHENTICATION PROFILE AND INTERFACE MATCH			
+ Add X Delete			
Interface	Profile	Default method or directory	
in	Internal	Directory (none)	

Onglet Profils du portail captif

1. Dans le profil d'authentification sélectionné (*Internal* dans l'exemple), sélectionnez l'annuaire qui sera utilisé par défaut. Il doit correspondre à l'annuaire renseigné dans la règle d'authentification (*None* si aucun annuaire correspondant au domaine Active Directory n'est défini sur le firewall).
2. Dans la **Configuration avancée**, vérifiez que la case **Activer le portail captif** est bien cochée.

AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	CAPTIVE PORTAL PROFILES
For transparent authentication: 4 hour(s) 0 minute(s)			
Advanced properties			
<input checked="" type="checkbox"/> Enable the captive portal			

Configurer la méthode de redirection du proxy

La configuration de la méthode de redirection du proxy HTTP n'est pas indispensable, mais elle permet d'automatiser les étapes (3) à (5) du fonctionnement de SPNEGO, ce qui participe grandement à l'ergonomie de la fonction.

Dans le module **Configuration > Système > Configuration**, onglet **Configuration Générale > cadre Configuration avancée** :

1. Dans le champ **Redirection vers le portail captif**, sélectionnez **Préciser un nom de domaine (FQDN)**.
2. Dans le champ **Nom de domaine (FQDN)**, saisissez le nom du firewall tel qu'ajouté au serveur DNS : *numéro_de_série_du_firewall.nom_de_domaine_AD* par défaut (*SN710A000099999999.stormshield.com* dans l'exemple).

Configurer la politique de filtrage

La politique de filtrage nécessaire à la méthode SPNEGO se compose d'une règle d'authentification et d'une règle de filtrage.

Ajouter une règle d'authentification

Cette règle est destinée à rediriger vers le portail captif toutes les connexions HTTP à destination d'Internet et émanant d'utilisateurs non encore authentifiés :

1. Dans le module **Configuration > Politique de sécurité > Filtrage et NAT**, cliquez sur **Nouvelle règle** et sélectionnez **Règle d'authentification**.
2. Modifiez les objets prédéfinis en fonction de vos besoins. Dans notre exemple nous utilisons les objets proposés par défaut.



Ajouter une règle de filtrage

Cette règle autorise les utilisateurs authentifiés à accéder à Internet :

1. Dans la politique de filtrage active, cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
2. Double cliquez sur cette règle pour l'éditer.
3. Dans le menu **Action** > onglet **Général**, sélectionnez l'**Action passer**.
4. Dans le menu **Source** > onglet **Général**, sélectionnez l'**Utilisateur Any user@annuaire**. Dans le cas où aucun annuaire correspondant au domaine Active Directory n'est configuré sur le firewall, choisissez **Any user@none**.
5. Dans le menu **Source** > onglet **Général**, sélectionnez les **Machines sources** (exemple : **Network_internals**).
6. Dans le menu **Destination** > onglet **Général**, sélectionnez **Internet** comme **Machines destinations**.
7. Dans le menu **Port / Protocole** > **Port**, sélectionnez **http** comme **Port destination**.
8. Dans le menu **Inspection**, sélectionnez les inspections applicatives souhaitées (Filtrage URL, ...).
9. Validez et activez cette règle à l'aide d'un double clic dans la colonne État.

La politique de filtrage pour la partie SPNEGO prend donc la forme suivante :

FILTERING		NAT						
Searching...		+ New rule - X Delete ↑ ↓ Cut Copy Paste Search in logs						
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
1	on	Authentication portal Except: authentication_bypass	unknown @ Network_internals	Internet	http		IPS	
2	on	pass	any @ Network_internals	Internet	http		IPS	

Configurer les clients (navigateurs WEB)

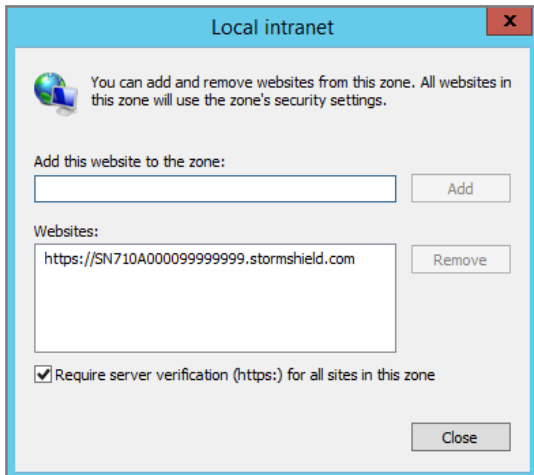
Avant de configurer votre navigateur Web, vérifiez que le portail d'authentification du firewall utilisé pour SPNEGO est bien joignable depuis un poste client :

1. Démarrez le navigateur Web du poste.
2. Saisissez l'URL `https://numero_de_serie_du_firewall.domaine_dns` (`https://SN710A000099999999.stormshield.com` dans l'exemple).
Si le portail ne s'affiche pas, vérifiez vos connexions réseau ainsi que la configuration effectuée jusqu'ici avant de poursuivre.

Configurer Microsoft Internet Explorer, Microsoft Edge et Google Chrome

Microsoft Edge et Google Chrome se basant sur les **Options Internet** de Microsoft Windows, leur configuration est identique à celle réalisée pour Microsoft Internet Explorer :

1. Démarrez Internet Explorer.
2. Ouvrez le menu **Outils** > **Options Internet**.
3. Dans l'onglet **Sécurité** > zone **Intranet Local**, cliquez sur le bouton **Sites** puis **Avancé**.
4. Ajoutez le site Web `https://numero_de_serie_du_firewall.domaine_dns` à la zone (`https://SN710A000099999999.stormshield.com` dans l'exemple).
5. Veillez à ce que l'option **Exiger un serveur sécurisé (https:)** pour tous les sites dans cette zone soit cochée.



6. Validez et retournez dans le menu **Outils > Options Internet > onglet Sécurité**.
7. Dans la zone **Intranet local**, cliquez sur le bouton **Personnaliser le niveau**.
8. Dans la section **Paramètres > Authentification utilisateur > Connexion**, vérifiez que l'option **Connexion automatique uniquement dans la zone intranet** est cochée.
9. Validez la configuration.
10. Dans le menu **Outils > Options Internet > onglet Avancé > Paramètres > section Sécurité**, vérifiez que l'option **Activer l'authentification Windows intégrée*** est cochée.
11. Validez la configuration des **Options Internet**.

Si vous utilisez un proxy pour accéder à Internet, mettez en place une exception pour le firewall :

1. Dans le menu **Outils > Options Internet > onglet Connexion**, cliquez sur **Paramètres réseau**
2. Cochez l'option **Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN)** puis cliquez sur **Avancé**.
3. Dans le champ **Exceptions**, ajoutez **https://numero_de_serie_du_firewall.domaine_dns** [exemple : « https://SN710A000099999999.stormshield.com »].

Configurer Mozilla Firefox

1. Démarrez Firefox et tapez **about:config** dans la barre d'URL.
Une liste de paramètres de configuration apparaît.
2. Recherchez les paramètres **network.negotiate-auth.delegation-uris** et **network.negotiate-auth.trusted-uris** :

Preference Name	Status	Type	Value
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	default	string	
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	default	string	
network.negotiate-auth.using-native-gsslib	default	boolean	true



1. Dans le module **Configuration** > **Objets** > **Certificats et PKI**, cliquez sur **Ajouter** puis sélectionnez **Identité serveur**.
2. Dans le champ **Nom de domaine qualifié (FQDN)**, indiquez l'identifiant choisi (*portail.stormshield.com* dans l'exemple).
3. Cliquez sur **Suivant**.
4. Sélectionnez l'**Autorité de Certification** précédemment créée (**CA-SPNEGO** dans l'exemple) pour signer ce certificat.
Les attributs du certificat sont automatiquement complétés à l'aide de ceux de l'autorité.
5. Renseignez le **Mot de passe de l'autorité**.
6. Cliquez sur **Suivant**.
7. Sauf besoins très spécifiques, laissez la **Validité** et la **Taille de clé** aux valeurs proposées.
8. Cliquez sur **Suivant**.
9. Validez la création du certificat en cliquant sur **Terminer**.

Personnaliser le portail captif

Sur le firewall principal, modifiez le portail captif pour qu'il présente l'identifiant du cluster à la place du numéro de série du firewall :

1. Placez-vous dans le menu **Configuration** > **Utilisateurs** > **Authentification** > onglet **Portail captif**,
2. Dans le champ **Certificat (clé privée)**, sélectionnez le certificat précédemment créé.

Terminer la configuration de SPNEGO

Une fois le certificat affecté au portail captif, la configuration de SPNEGO se déroule de manière identique à la procédure initiale de la modification du serveur DNS à la configuration des clients. A ceci près que :

1. Vous devez ajouter l'entrée « *identifiant personnalisé* » au serveur DNS. Ainsi, la chaîne « *numero_de_serie_du_firewall.domaindns* » est à remplacer par « *identifiant personnalisé* ». Dans cet exemple, on remplace donc *https://SN710A000099999999.stormshield.com* par *https://portail.stormshield.com*.
2. Lors de l'utilisation du script *spnego.bat*, la variable <FW> représentant l'identifiant du firewall prend cette fois-ci la valeur « *identifiant personnalisé* » sans le nom de domaine DNS. Dans cet exemple, il s'agit donc de *portail*.



Problèmes fréquemment rencontrés

Lors de l'exécution du script *spnego.bat*, divers messages d'erreurs peuvent être affichés.

Message

- "Some arguments are missing, please provide the correct arguments."

-ou-

- "Too many arguments, please provide the correct arguments."

Solution

Vérifiez la présence des arguments <FW>, <dns>, <WINDOWS>, <password> et <fichier>.

Chacun de ces arguments est indispensable à l'exécution du script.

Message

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

Solution

Un fichier keytab portant le nom fourni est déjà présent dans le répertoire d'exécution du script. Renommez ce fichier.

Message

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

-ou-

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

-ou-

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

-ou-

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

Solution

Vérifiez la présence des outils de support ou du chemin au sein du système.

Message

- "This computer does not seem to be running Windows XXXX Server or Windows YYYY Server >> %log%".

-ou-

- "This computer does not seem to be running a Server edition of Windows".

-ou-

- "This script should only be run on a Windows Domain Controller which requires a Server edition of Windows".

Solution



Vérifiez la compatibilité de votre version de Microsoft Windows avec l'exécution du script *spnego.bat*.

Message

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

Solution

- La création de l'utilisateur a été interrompue. Vérifiez que le mot de passe est conforme à la politique de sécurité.
- Vérifiez que l'utilisateur qui exécute le script ait les droits pour en créer un nouveau.
- Vérifiez que l'utilisateur ait les droits pour créer le nom de service.
- Vérifiez que l'utilisateur ait les droits pour créer le keytab.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sur la méthode SPNEGO sont disponibles dans la [base de connaissances Stormshield](#) (authentification nécessaire).



STORMSHIELD

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2019. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.