



STORMSHIELD

VPN SSL

CONCEPTS ET GÉNÉRALITÉS

VPN SSL

STORMSHIELD

Programme du module

- ➔ Concepts et généralités
 - Configuration d'un tunnel

CONCEPTS ET GÉNÉRALITÉS

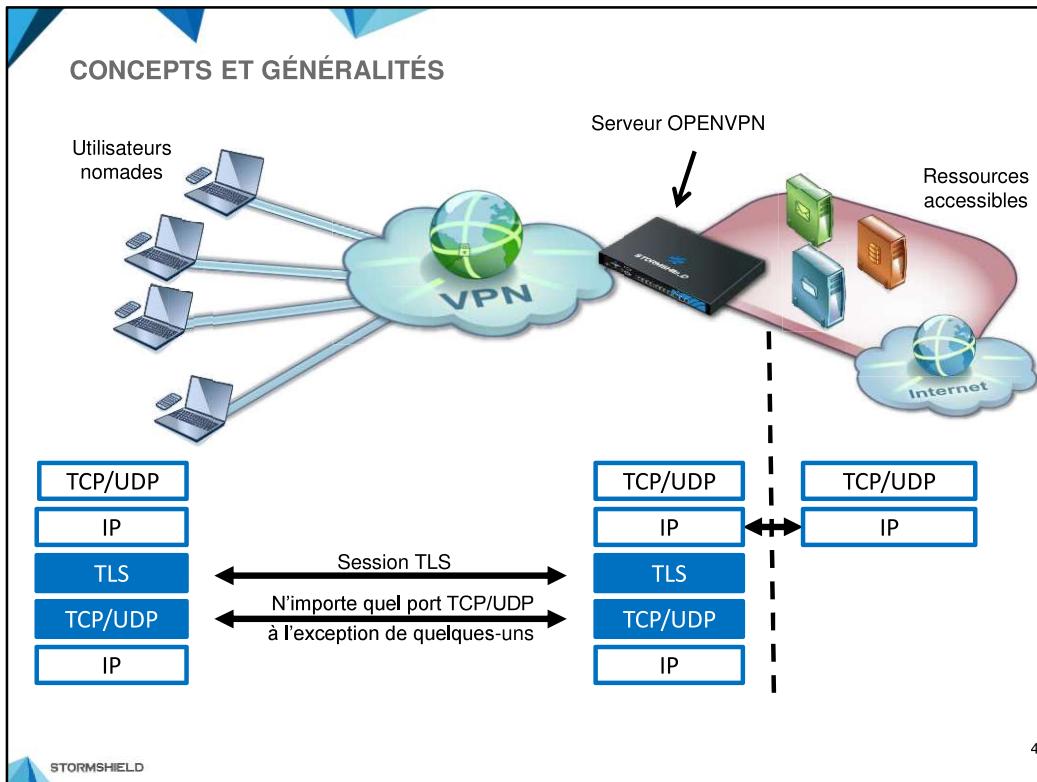
- Les firewalls Stormshield intègrent deux types de VPN SSL
- VPN SSL portail :
 - Accès aux serveurs Web HTTP et serveurs applicatifs via le portail captif après authentification
- VPN SSL (complet) :
 - Utilise un client VPN SSL (gratuit)
 - Accès au réseau interne d'une manière transparente



3

Note :

- Les deux modes VPN SSL (portail et complet) peuvent fonctionner simultanément.
- Le VPN SSL portail n'est pas abordé dans le cadre de cette formation. Aussi, toutes les références à « VPN SSL » dans le reste de ce document se rapportent exclusivement au VPN SSL en mode complet.



Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée aux ressources internes d'une entreprise. Les communications entre l'utilisateur distant et le firewall sont encapsulées et protégées via un tunnel TLS chiffré.

Sur le firewall, les tunnels VPN SSL sont gérés par le serveur OpenVPN (logiciel libre) qui est intégré dans le firmware en tant que nouveau service. OpenVPN peut fonctionner sur n'importe quel port TCP et/ou UDP à l'exception de quelques-uns qui sont utilisés pour le fonctionnement interne du firewall :

- smtp_proxy : 8081/TCP
- ftp_proxy : 8083/TCP
- pop3_proxy:8082/TCP
- ssl_proxy : 8084/TCP
- http_proxy : 8080/TCP
- loopback_proxyssl : 8085/TCP
- firewall_srv : 1300/TCP
- ldap : TCP/389, ldaps TCP/636
- pptp : TCP/1723, TCP/4444, TCP/8087
- smux_tcp : TCP/199.

En ce qui concerne les utilisateurs nomades, le tunnel est géré par le client VPN SSL (Stormshield ou openVPN standard), qui doit être installé sur les machines. Une fois le tunnel mis en œuvre, l'hôte distant récupère une adresse IP fournie par le serveur VPN SSL. Elle sera considérée comme faisant partie des réseaux internes (protégés) du firewall et l'utilisateur sera vu comme authentifié.



NOMBRE DE TUNNELS VPN SSL

- Le nombre de tunnels VPN maximum dépend du modèle d'UTM:

UTM	SN160 SN160W	SN210 SN210W	SN310	SN510	SN710	SN910	SN2100	SN3100	SN6100	SNi40
Nombre d'utilisateurs	5	20	20	100	150	150	400	500	500	100

- Limites des appliances virtuelles:

V-UTM	EVA1	EVA2	EVA3	EVA4	EVAU
Nombre d'utilisateurs	100	150	200	250	500

5

CLIENTS VPN SSL

- Pour monter le tunnel, le client peut utiliser :

- L'application standard OpenVPN
 - PC : Windows, macOS, GNU/Linux
 - Mobile : Android, IOS



- Le client SSL VPN Stormshield
 - PC : Windows



6

Clients VPN SSL compatibles :

- Le client VPN SSL Stormshield Network (basé sur le client OpenVPN) peut être lancé en toute transparence depuis un poste utilisateur Windows avec les droits d'utilisateur (toutefois, son utilisation nécessite des droits administrateur). Ce client peut être téléchargé gratuitement depuis votre espace privé mystormshield.com ou depuis le portail captif du firewall après authentification.
- Un client OpenVPN standard doit être lancé avec les droits d'administration du poste client.
- Les terminaux de type smartphones et tablettes (Android ou iOS) peuvent également se connecter via un VPN SSL avec un client OpenVPN Connect (disponible dans le Google Play Store et l'Apple Store).

CLIENTS VPN SSL

- Le réseau VPN SSL défini sur le serveur est considéré comme un réseau interne ⇒ Il ne doit pas chevaucher un réseau interne existant
- Le réseau VPN SSL est découpé en sous-réseaux de /30 :
 - Le premier est utilisé par le serveur
 - Un sous-réseau est utilisé pour chaque client
- Exemple : 192.168.100.0/24 ⇒ 63 clients maximum
 - Serveur [192.168.100.0] .1 | .2 | .3] /30
 - Client 1 [192.168.100.4] .5 | **.6** | .7] /30
 - Client 2 [192.168.100.8] .9| **.10**] .11] /30
 - Client 3 [192.168.100.12] .13| **.14**] .15] /30
 - ...

7

Les clients VPN SSL font partie d'un même réseau défini au niveau du firewall. Ce réseau est considéré comme un réseau interne protégé et il ne doit par conséquent pas chevaucher un réseau interne existant.

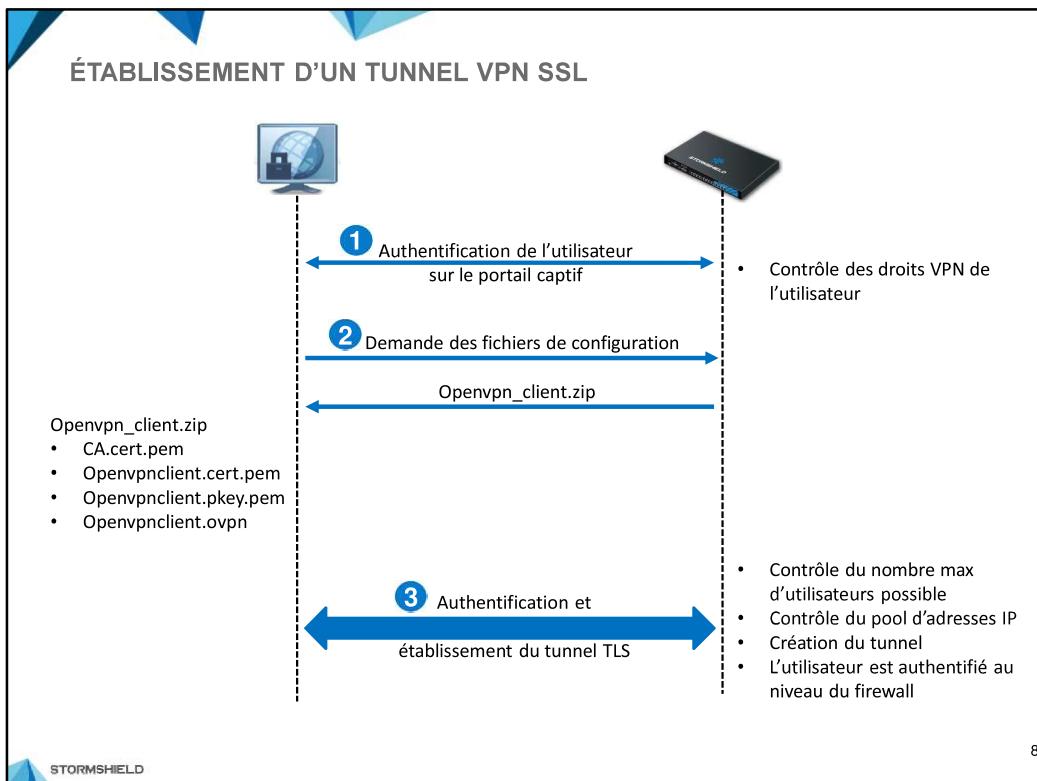
Pour son fonctionnement interne, le serveur se réserve le premier sous-réseau de /30 issu du réseau VPN SSL (une interface « tun0 » est créée et porte la première adresse IP du réseau. Cette interface n'est visible que via une ligne de commande). Les sous-réseaux de /30 suivants sont utilisés par les clients.

Par exemple, si le réseau 192.168.100.0/24 est utilisé par le service VPN SSL, le premier client VPN SSL utilise le deuxième sous-réseau de /30 :

- Adresse réseau : 192.168.100.4
- Adresse de l'interface du tunnel côté serveur : 192.168.100.5
- Adresse de l'interface du tunnel côté client : 192.168.100.6
- Adresse de diffusion : 192.168.100.7

Ainsi, le nombre maximum de clients VPN SSL sur ce réseau est de 63 (64 sous-réseaux de /30, dont un utilisé par le serveur).

Ce comportement est explicitement défini dans la solution OpenVPN.



La mise en œuvre du tunnel VPN SSL s'effectue en 3 étapes principales :

1. Le client VPN SSL authentifie l'utilisateur via le portail captif. Durant cette étape, le firewall vérifie si l'utilisateur authentifié possède les droits lui permettant d'ouvrir un tunnel VPN SSL.
2. Si l'authentification réussit, le client envoie une requête pour récupérer les fichiers de configuration renvoyés par le firewall dans un dossier compressé « `openvpn_client.zip` ». Le dossier contient les fichiers suivants :
 - Le certificat de l'autorité de certification (**CA.cert.pem**),
 - Le certificat du client et sa clé privée (**openvpnclient.cert.pem** et **openvpnclient.pkey.pem**),
 - La configuration du client OpenVPN.
3. Le client lance le processus de mise en œuvre du tunnel TLS avec authentification par certificat à l'aide des certificats récupérés lors de l'étape précédente. Avant la mise en œuvre du tunnel, le firewall vérifie que le nombre maximal d'utilisateurs n'est pas encore atteint et qu'un sous réseau peut être réservé pour ce nouveau client. Si toutes les conditions sont vérifiées, le tunnel est mis en œuvre et l'utilisateur est considéré comme authentifié.

NOTE : Si le serveur VPN SSL est accessible via un port UDP et TCP, le client VPN SSL tente d'abord de mettre en œuvre le tunnel avec le protocole UDP et en cas d'échec, il effectue automatiquement une nouvelle tentative avec le protocole TCP.



STORMSHIELD

VPN SSL

CONFIGURATION D'UN TUNNEL

VPN SSL

STORMSHIELD

Programme du module

- ✓ Concepts et généralités
- ➔ Configuration d'un tunnel

PRÉREQUIS : ANNUAIRE, PORTAIL CAPTIF ET AUTHENTIFICATION

- Un annuaire interne ou externe doit être configuré
- Un profil du portail captif doit être rattaché à l'interface depuis laquelle les utilisateurs se connectent

Interface	Profile	Default method or directory
out	Internal	Directory (trainer.local)

- Une méthode d'authentification doit être configurée

Method
LDAP
Guest method
Sponsorship method

10

La première étape de mise en œuvre d'un tunnel VPN SSL est l'authentification de l'utilisateur via le portail captif, ce qui signifie que :

- un annuaire externe ou interne doit être configuré au niveau du firewall,
- un profil du portail captif doit être rattaché à l'interface depuis laquelle les utilisateurs se connectent,
- une méthode d'authentification doit être configurée.

Les méthodes d'authentification possibles pour le service VPN SSL sont les méthodes explicites qui nécessitent un couple identifiant/mot de passe, en l'occurrence LDAP (interne, externe ou Microsoft Active Directory), Kerberos et Radius.



PRÉREQUIS : L'AUTORITÉ DE CERTIFICATION VPN SSL

- PKI fournissant les certificats pour le serveur OpenVPN et les clients OpenVPN (le même certificat sera affecté à tous les clients OpenVPN) :



11

L'authentification entre le client et le serveur VPN SSL s'effectue par certificat. Pour cela, une autorité de certification racine (CA) existe dans la configuration usine de tous les firewalls Stormshield Network. Cette CA est nommée **sslvpn-full-default-authority**, et elle contient un certificat serveur (qui identifie le serveur VPN SSL) et un certificat client (qui identifie tous les clients; chacun d'entre eux étant alors différencié par un couple identifiant/mot de passe).

NOTE : Il est naturellement possible de créer une CA dédiée au VPN SSL sans recourir à la CA par défaut. La création des CA est présentée dans le niveau expert.

DROITS D'ACCÈS VPN SSL

Paramétrage par défaut

Paramétrage personnalisé

12

Pour autoriser un utilisateur à monter un tunnel VPN SSL, vous devez lui attribuer les droits correspondants dans le menu **Configuration ⇒ Utilisateurs ⇒ Droits d'accès**.

Il est possible de choisir un accès par défaut indépendamment de l'utilisateur connecté dans l'onglet **Accès détaillé** ⇒ colonne **VPN SSL**. Sélectionnez **Autoriser** dans le champ **Politique VPN SSL par défaut**

Cependant, une gestion plus fine des droits d'accès est préconisée en conservant la valeur de la politique VPN SSL par défaut « Interdire » et en ajoutant des utilisateurs ou des groupes d'utilisateurs dans l'onglet **ACCÈS DÉTAILLÉ ⇒ AJOUTER** avec les droits VPN SSL définis sur **Autoriser**.

RÈGLE DE FILTRAGE IMPLICITE POUR LE VPN SSL

SECURITY POLICY / IMPLICIT RULES

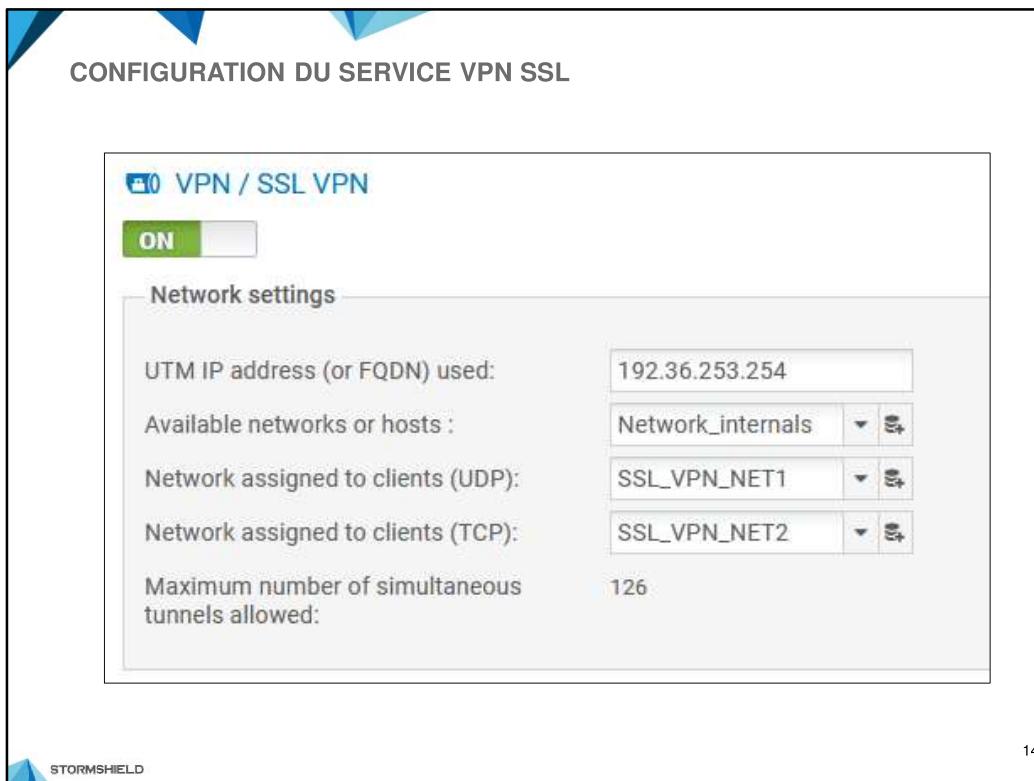
IMPLICIT FILTER RULES

Enabled	Name
<input checked="" type="checkbox"/> Enabled	Allow access to the PPTP server
<input checked="" type="checkbox"/> Enabled	Allow mutual access between the members of a firewall cluster (HA)
<input checked="" type="checkbox"/> Enabled	Allow ISAKMP (UDP port 500) and the ESP protocol for IPSec VPN peers.
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's DNS service (port 53).
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for modem interfaces (dialup)
<input checked="" type="checkbox"/> Enabled	Block and reinitialize ident requests (port 113) for ethernet interfaces
<input type="checkbox"/> Disabled	Allow protected interfaces (serverd) to access the firewall's administration server (port 1300)
<input checked="" type="checkbox"/> Enabled	Allow protected interfaces to access the firewall's SSH port
<input checked="" type="checkbox"/> Enabled	Allow interfaces associated with authentication profiles (Authd) to access the authentication portal and SSL VPN.
<input checked="" type="checkbox"/> Enabled	Allow access to the firewall's web administration server (WebAdmin)
<input checked="" type="checkbox"/> Enabled	Allow "Bootp" requests with an IP address specified for relaying DHCP requests
<input checked="" type="checkbox"/> Enabled	Allow clients to reach the firewall SSL VPN service on the HTTPS port
<input checked="" type="checkbox"/> Enabled	Allow router solicitations (RS) in multicast or directed to the firewall
<input checked="" type="checkbox"/> Enabled	Allow requests to DHCPv6 server and DHCPv6 multicast solicitations
<input checked="" type="checkbox"/> Enabled	Do not log IPFIX packets in IPFIX traffic

13

Pour permettre aux clients VPN SSL d'accéder au portail d'authentification sur les interfaces associées aux profils d'authentification du firewall, la règle de filtrage implicite nommée **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces associées aux profils d'authentification (Authd)** doit être activée.

Si tel n'est pas le cas, il est impératif d'ajouter des règles de filtrage explicites dans la politique active autorisant les flux à destination de l'interface publique sur le port d'écoute du service.



Le service VPN SSL peut être configuré dans le menu **Configuration ⇒ VPN ⇒ VPN SSL**.

- Encadré **Paramètres réseaux** :
 - **Adresse IP (ou FQDN) de l'UTM utilisée** : il s'agit de l'adresse sur laquelle vont se connecter les clients VPN SSL (adresse publique la plupart du temps). Attention, la saisie d'un FQDN induit une résolution de noms via un service DNS,
 - **Réseaux ou hôtes disponibles** : machines ou réseaux auxquels les utilisateurs peuvent avoir accès une fois le tunnel établi (l'accès dépend néanmoins de la politique de filtrage active). Il est possible de choisir l'objet **Any**. Dans ce cas, tous les flux du client VPN passent par le tunnel et sont soumis aux opérations de filtrage et de NAT du firewall.
 - **Réseau assigné aux clients (UDP)** : réseau attribué aux clients nomades une fois le tunnel établi via le protocole UDP. La valeur minimale pouvant être choisie ici est un réseau de /29.
 - **Réseau assigné aux clients (TCP)** : réseau attribué aux clients nomades une fois le tunnel établi via le protocole TCP. La valeur minimale pouvant être choisie ici est un réseau de /29.
 - **Nombre maximal de tunnels simultanés autorisés** : paramètre non configurable dans la GUI. Il indique le nombre maximal de tunnels (clients) autorisés, c'est-à-dire le minimum entre le nombre de tunnels autorisés pour le modèle du firewall et le nombre de tunnels possibles calculé à partir du réseau assigné aux clients.

NOTE : les réseaux assignés aux client UDP et TCP doivent être différents.

CONFIGURATION DU SERVICE VPN SSL

The screenshot shows the 'VPN / SSL VPN' configuration page. It includes sections for 'DNS settings sent to client' (Domain name, Primary DNS server, Secondary DNS server), 'Advanced configuration' (UTM IP address for the SSL VPN (UDP), Port (UDP), Port (TCP), Interval before key renegotiation (seconds)), and 'Scripts to run on the client' (Script to run when connecting, Script to run when disconnecting). The 'Used certificates' section lists 'Server certificate: openvpnserver' and 'Client certificate: openvpncclient'. A small '15' is visible in the bottom right corner of the form area.

Comme vu précédemment, ce réseau est découpé en sous-réseaux de /30 dont l'un est utilisé par le serveur pour son fonctionnement interne, les autres étant utilisés par les clients. Ainsi, un réseau de /24 permet un maximum de 63 tunnels.

- Encadré **Paramètres DNS envoyés au client** :
 - **Nom de domaine** : il s'agit en général du domaine dont dépendent les réseaux accessibles par le client
 - **Serveur DNS primaire (et secondaire)**: interne à l'entreprise si le client doit pouvoir accéder à des ressources locales. Sinon, le choix d'un serveur public est autorisé.
- Encadré **Configuration avancée** :
 - **Adresse IP de l'UTM pour le VPN SSL (UDP)** : il s'agit de l'adresse à laquelle vont se connecter les clients du VPN SSL s'ils sont configurés pour utiliser l'UDP (adresse publique la plupart du temps).
 - **Port (UDP)** : port d'écoute UDP du service VPN SSL.
 - **Port (TCP)** : port d'écoute TCP du service VPN SSL.

NOTE : Attention, certains ports sont réservés à un usage interne et ne peuvent être sélectionnés. Ces ports sont smtp_proxy : 8081/TCP, ftp_proxy : 8083/TCP, pop3_proxy : 8082/TCP, ssl_proxy : 8084/TCP, http_proxy : 8080/TCP, loopback_proxyssl : 8085/TCP, firewall_srv : 1300/TCP, ldap : TCP/389, ldaps TCP/636, pptp : TCP/1723, TCP/4444, TCP/8087, smux_tcp : TCP/199, isakmp : UDP/500, isakmp_nat : UDP/4500, bootps : UDP/67, bootpc : UDP/68.

- **Intervalle avant renégociation clé (en secondes)** : période avant qu'une nouvelle session TLS ne soit renégociée.
 - **Utiliser les serveurs DNS fournis par le firewall** : lorsque cette option est choisie, le client VPN SSL ajoutera les serveurs DNS qui ont été récupérés via le tunnel VPN SSL à la configuration réseau du poste de travail du client.
 - **Interdire l'utilisation des serveurs DNS tiers** : lorsque cette option est choisie, le poste de travail du client utilisera uniquement les serveurs DNS qui ont été récupérés via le tunnel VPN SSL.
-
- Encadré **Script à exécuter sur le client** : permet de définir les scripts à exécuter lorsque le client se connecte et se déconnecte. Des exemples de scripts sont fournis de façon détaillée dans le document snentno_SSL_VPN_Tunnel.pdf accessible via <https://mystormshield.eu>.
 - Encadré **Certificats utilisés** : personnalise les certificats utilisés. Rappel : le certificat serveur permet d'identifier le serveur VPN SSL alors que le certificat utilisateur permet d'identifier les clients VPN SSL (chaque client sera ensuite identifié par son login). Si ces certificats sont modifiés, s'assurer qu'ils ont bien été émis par la même autorité de certification. Sinon, la configuration ne sera pas appliquée.
 - Encadré **Configuration** : le fichier de configuration peut être téléchargé au format OpenVPN.

FILTRAGE ET NAT

- Il est nécessaire de définir des règles de filtrage explicites pour la gestion du trafic provenant des tunnels :

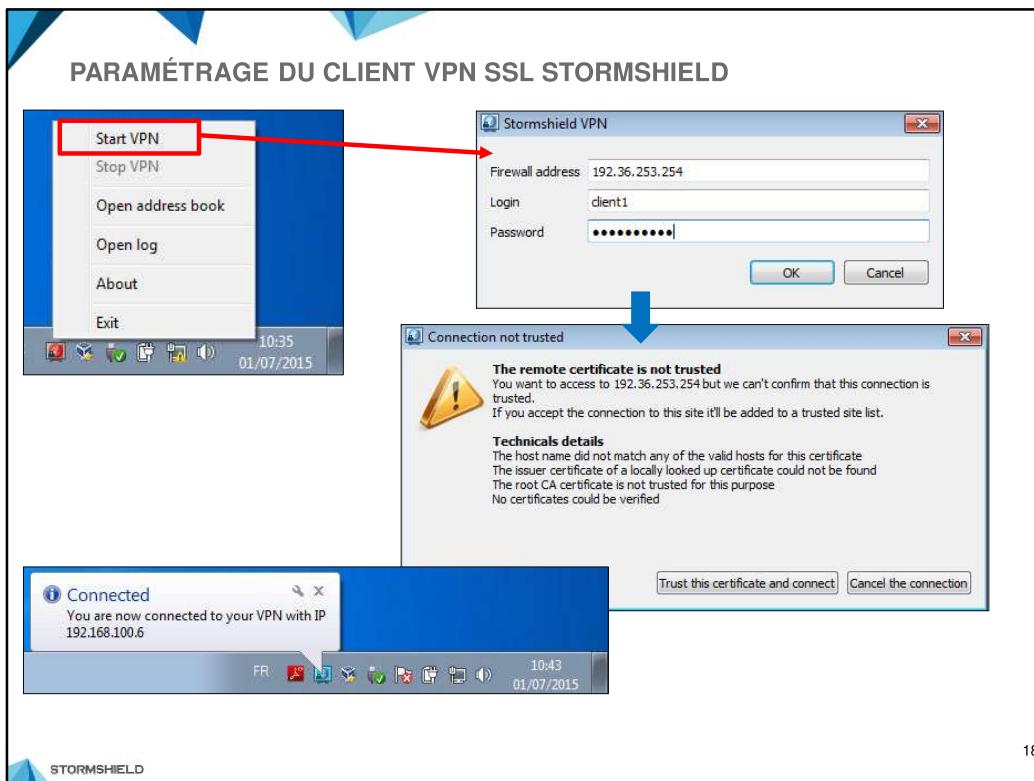
FILTERING NAT								
	Status	Action	Source	Destination	Dest. port	Protocol	Security insp...	Comments
1	on	pass	SSL_VPN_NET1 via SSL VPN tunnel	Network_internals	http		IPS	
2	on	pass	SSL_VPN_NET1 via SSL VPN tunnel	Internet	dns_udp http https		IPS	

- Une translation d'adresses peut être mise en œuvre si des clients doivent utiliser le VPN SSL pour accéder à Internet :

FILTERING NAT								
Original traffic (before translation)					Traffic after translation			
	Status	Source	Destination	Dest. port	Source	Src. port	Destin...	Dest. port
1	on	SSL_VPN_NET1 interface: sslvpn	Internet interface: out	Any	Firewall out	ephemeral fw	Any	

17

La règle de filtrage n°1 permet l'**initiation de connexions** à partir des clients VPN SSL et à destination de tous les réseaux internes (Network_Internal),
 La règle de filtrage n°2 permet l'**initiation de connexions** à partir des clients VPN SSL et à destination d'Internet ; dans ce cas, une règle de NAT doit également être ajoutée.



18

L'application VPN SSL Stormshield Network peut être téléchargée sur votre espace privé <https://mystormshield.eu> et sur le portail captif du firewall après authentification.

Une fois démarré, le client VPN SSL demande trois paramètres :

- l'adresse IP ou le FQDN du firewall à contacter,
- l'identifiant de l'utilisateur disposant des droits pour le VPN SSL,
- le mot de passe associé à l'utilisateur.

Une fenêtre indique que la connexion à ce site n'est pas sécurisée car le client ne fait pas confiance à la CA signataire du certificat serveur présenté par le portail captif du firewall. Il est donc possible de :

- afficher le certificat afin de connaître notamment la CA signataire,
- faire confiance à ce certificat, ce qui ajoute la CA aux autorités de confiance et permet de continuer la mise en œuvre du tunnel,
- annuler la connexion, ce qui interrompt la mise en œuvre du tunnel.

En cas d'échec lors de la création du tunnel, un clic-droit sur l'icône Stormshield Network VPN SSL permet d'afficher les journaux.

Une fois le tunnel établi, le poste client dispose d'une interface spécifique pour le tunnel VPN SSL, dont l'adresse IP fait partie de l'objet **Réseau assigné au client** dans la configuration serveur.



PARAMÉTRAGE DU CLIENT VPN SSL STORMSHIELD

	Déconnecté
	En cours de connexion
	Connecté

Connected as client1 on 192.36.253.254
Since 10:43 (414 s)
IP address: 192.168.100.6
In: 34,36 KB Out: 35,47 KB

10:50 01/07/2015

19

L'icône du client VPN SSL Stormshield qui apparaît dans la zone de notification de la barre de tâches de Windows possède un code couleur qui correspond à son état :

- Rouge : le client est déconnecté,
- Jaune : le client essaye d'établir le tunnel,
- Bleu : le client est connecté.

Lorsque le client est connecté, des informations sur la connexion apparaissent lorsque le curseur de la souris est positionné sur l'icône.



TUNNELS VPN SSL DANS LA GUI

User	Directory	VPN client IP address	Real IP address	Received	Sent
vpnuser	trainer.local	172.30.30.6	31.20.108.163	4.49 KB	6.64 KB

Name	IP address	Directory	Group	Expiry date	Auth. method
vpnuser	172.30.30.6	trainer.local		6d 23h 57m	OPENVPN

20

Dans la page de supervision du firewall, il est possible de consulter les tunnels VPN SSL ouverts dans le menu **Surveillance => onglet Tunnels VPN SSL**. Il est également possible de supprimer un tunnel en cliquant sur **Déconnecter cet utilisateur**, accessible en effectuant un clic droit.

Les utilisateurs connectés via un tunnel VPN SSL sont considérés comme authentifiés et peuvent être visualisés depuis le menu **Utilisateurs**. La colonne **VPN SSL** indique que le client VPN est authentifié via un tunnel VPN SSL.