

Technical Overview

Arkoon SmartSSL

Version 1.0 – Juillet 2011



Smart SSL

SOMMAIRE

1 - Introduction	- 3 -
2 - Contexte	- 4 -
2.1 <i>Etat des lieux</i>	- 4 -
2.3 – <i>Les enjeux, SmartSSL vs VPN SSL « classique ».....</i>	- 6 -
3.1 <i>Architecture globale</i>	- 10 -
3.2 <i>Les composants</i>	- 11 -
3.2.1 <i>L'agent SmartSSL</i>	- 11 -
3.2.2 <i>Le serveur.....</i>	- 14 -
3.2.3. <i>L'appliance FAST360</i>	- 18 -
3.3 - <i>Monitoring et supervision de la solution</i>	- 19 -
3.4 – <i>Compatibilité des services Web</i>	- 20 -
4. Caractéristiques de l'offre	- 21 -
4.1 – <i>Les versions</i>	- 21 -
4.2 - <i>Mode de licence</i>	- 22 -
5. Questions / Réponses	- 23 -

Siège social

1 place Verrazzano - 69009 Lyon

Tél. +33 (0)4 72 53 01 01

Fax +33 (0)4 72 53 12 60

S.A. au capital de 4 605 019 € RCS Lyon



1 - Introduction

Le développement des besoins en matière de nomadisme d'entreprise est caractérisé par une croissance soutenue du taux d'équipements d'appareils mobiles - ordinateurs portables, Smartphone, Tablettes - personnels ou professionnels. Associé à ces changements d'usage mais aussi liés aux besoins de productivité, il est nécessaire pour toute entreprise de permettre l'accès à ses ressources IT quels que soient l'environnement, l'heure et le lieu où se trouvent les collaborateurs. Le dilemme consiste alors à devoir concilier l'ensemble de ces besoins avec le souci permanent de la sécurité des données. Comment ne pas être contraint de définir de lourdes et coûteuses stratégies d'accès à l'information ? Comment ne pas devoir investir lourdement dans des infrastructures matérielles complexes à mettre en œuvre et à maintenir ? **Arkoon Network Security** propose au travers de son offre **SmartSSL** une solution novatrice qui permet d'harmoniser en toute simplicité et en totale sécurité ce qui jusqu'à maintenant constituait un véritable challenge pour tout décideur IT.

SmartSSL a été conçu pour apporter une réponse efficace à la problématique d'accès aux applications de l'entreprise en toute sécurité, transparence et simplicité pour les utilisateurs en situation de mobilité.

Ce document a pour objectif de décrire la solution **SmartSSL**, quels en sont les enjeux et comment ce nouveau service permet de les adresser.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



2 - Contexte

2.1 Etat des lieux

Le développement d'Internet, sa complexification, le développement d'applications Web de nouvelle génération (Web 2.0) ont conduit à l'évolution des types de menaces et l'apparition de nouvelles vulnérabilités.

Les attaques traditionnelles sur les réseaux portaient auparavant sur la faiblesse des implémentations du protocole TCP/IP (*ping of death, land attack, etc.*), où encore sur la faiblesse des applications (*buffer overflow*) permettant des attaques de type « déni de service » ou de prise de contrôle à distance « *remote code execution* ».

Si ces failles sont aujourd'hui toujours présentes, leur nombre a néanmoins fortement diminué, réduisant ainsi la surface d'attaque disponible.

Pour parvenir à leur fin, les cybercriminels ont donc du s'adapter :

S'ils exploitaient par le passé des ports de communication spécifiques – bloqués aujourd'hui par le plus basique des firewalls - ils utilisent dorénavant les protocoles autorisés sur l'ensemble des firewalls au regard de la popularité de leur usage (HTTP, SSL, DNS, SIP...) et privilégient désormais les attaques sur les applications (*Microsoft Office* par exemple) ou les plugins des navigateurs (*Adobe Flash, Acrobat Reader...*).

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



La généralisation du navigateur comme plateforme applicative universelle a donc conduit à de nouvelles tendances dans les menaces :

- **Vulnérabilité de contenu** : les navigateurs exécutent localement du code envoyé par des sources non connues et pouvant provoquer une infection de la machine locale par différents types de malware ;
- **Tromperie de l'utilisateur** : L'utilisateur peut être trompé par un site malveillant cherchant la plupart du temps à lui faire divulguer des informations personnelles ou encore effectuer des opérations à son insu (*Phishing, Clickjacking...*) ;
- **Tromperie du navigateur** : Le navigateur peut également être trompé lors de sa connexion aux sites demandés par l'utilisateur (*DNS Rebinding, Pharming*) ;
- **Rebond** : le navigateur est constamment amené à suivre des liens en provenance de pages web sans en maîtriser le risque. Il peut ainsi servir de passerelle entre plusieurs sites web et s'exposer à des vulnérabilités de type Intranet Scanning ;
- **Vulnérabilités des sites Web** : Aujourd'hui, ces vulnérabilités sont exploitées par rebond à partir d'un site malveillant : XSS (*Cross Site Scripting*), CSRF (*Cross Site Request Forgery*) ;

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975




2.3 – Les enjeux, SmartSSL vs VPN SSL « classique »


Les systèmes d'informations sont dorénavant ouverts par nécessité et de plus en plus d'entreprises ont besoin de publier des applications vers l'extérieur. Le succès de la mise en œuvre d'une connexion distante via SSL sera assuré à partir du moment où un certain nombre d'exigences seront satisfaites :

① Les connexions doivent être chiffrées :

Avec un équipement SSL traditionnel :


 Les connexions seront chiffrées par l'utilisation du protocole SSL; L'équipement doit proposer les algorithmes les plus forts.


Avec SmartSSL :

 Les connexions seront chiffrées par l'utilisation du protocole SSL. L'algorithme AES est utilisé avec des clés de chiffrement de 256 bits (AES 256);

② Les connexions doivent être universelles :

Avec un équipement SSL traditionnel :

 Le serveur SSL doit être compatible avec les postes distants sous Linux, Windows, Mac OS, Tablettes, PDA ...

 Le portail SSL accepte-t-il des connexions depuis Internet Explorer? Firefox ? Safari ? Google Chrome ? De quelles versions ?

Avec SmartSSL :

 SmartSSL est disponible sous Linux, Windows, Mac OS x, iPad, iPhone

Un navigateur virtuel est utilisé par application. Il est défini par l'administrateur et garantit la compatibilité avec l'application distante.

→ SmartSSL est pratiquement la seule solution en mesure de répondre à ces besoins.

③ L'ouverture de mon SI ne doit pas permettre la fuite de données :

Avec un équipement SSL traditionnel :



Impossible à garantir ... « enregistrer sous », « enregistrer une copie de... » sont des fonctions qui ne peuvent être bloquées avec une solution SSL classique ;

Avec SmartSSL :



Le navigateur s'exécute dans un environnement totalement virtualisé et donc sécurisé. Aucune interaction n'est possible avec le poste de travail. Un fichier ouvert ne pourra pas sortir de la fenêtre du navigateur utilisé.

→ Seul SmartSSL permet de garantir par concept la fuite des données.

④ Comment garantir la sécurité de la connexion si celle-ci s'effectue depuis un poste de travail non contrôlé par l'entreprise (hôtel, cyber café, machine personnelle ...) ?

Avec un équipement SSL traditionnel :



Le serveur SSL doit pouvoir contrôler si le poste distant possède la dernière version AV, le dernier service Pack, si le FW personnel est actif, si

| ...

Avec SmartSSL :



L'utilisation du navigateur virtuel et son mode d'exécution garantissent l'étanchéité totale entre la connexion distante et le poste potentiellement infecté (backdor, virus, cheval de Troyes ...) ou ouvert (absence de firewall personnel, d'anti-virus ...);

➔ SmartSSL permet d'éviter d'avoir à exécuter l'ensemble de ces contrôles. Les solutions SSL traditionnelles se devront d'avoir une base de données de fonctions logicielles, de versions et de signatures très conséquente (et surtout à jour !) pour garantir l'accès en toute sécurité et en toutes circonstances.

⑤ Quel est le risque de compromission ou d'infection de mes serveurs consultés lorsque la connexion SSL sera établie ?

Avec un équipement SSL traditionnel :



Comment éviter une attaque des serveurs par rebond ?



Le poste distant, s'il est infecté, ne va-t-il pas contaminer les serveurs ?

Autant de fonctions de contrôle du poste distant que le serveur SSL se doit posséder.

Avec SmartSSL :




Seuls les dépôts d'affichage transitent via la connexion SSL. Aucun fichier ni code malicieux ne peut-être véhiculé.




→ SmartSSL permet grâce à l'utilisation d'un navigateur virtuel de s'assurer de l'intégrité des données et serveurs accédés.

⑥ Quel sera le niveau de performances de mon équipement ?

Avec un équipement SSL traditionnel :

 Le niveau de performances sera directement lié aux caractéristiques matérielles du serveur SSL choisi. Elles ne pourront en aucun cas être étendues.

Avec SmartSSL :

 Les performances de SmartSSL sont associées au dimensionnement des serveurs virtualisés Arkoon Cloud Datacenter qui assurent les connexions distantes. Ces serveurs sont sous surveillance permanente et associés à des tableaux de bord qui permettent de connaître le niveau de performance des services et les ajuster si nécessaire.

→ Le dimensionnement des serveurs Arkoon Cloud Datacenter et le principe de fonctionnement de SmartSSL autorisent même la lecture de fichiers vidéo distants avec une fluidité remarquable.

⑦ Comment permettre un accès multi-site à mes données avec une maintenance de mon infrastructure SSL réduite à son strict minimum ?

Avec un équipement SSL traditionnel :

 Autant de boîtiers physiques sont nécessaires que de points d'entrée aux réseaux distants.

 Les boîtiers SSL doivent être constamment maintenus à jour pour

garantir la compatibilité des connexions distantes

Avec SmartSSL :



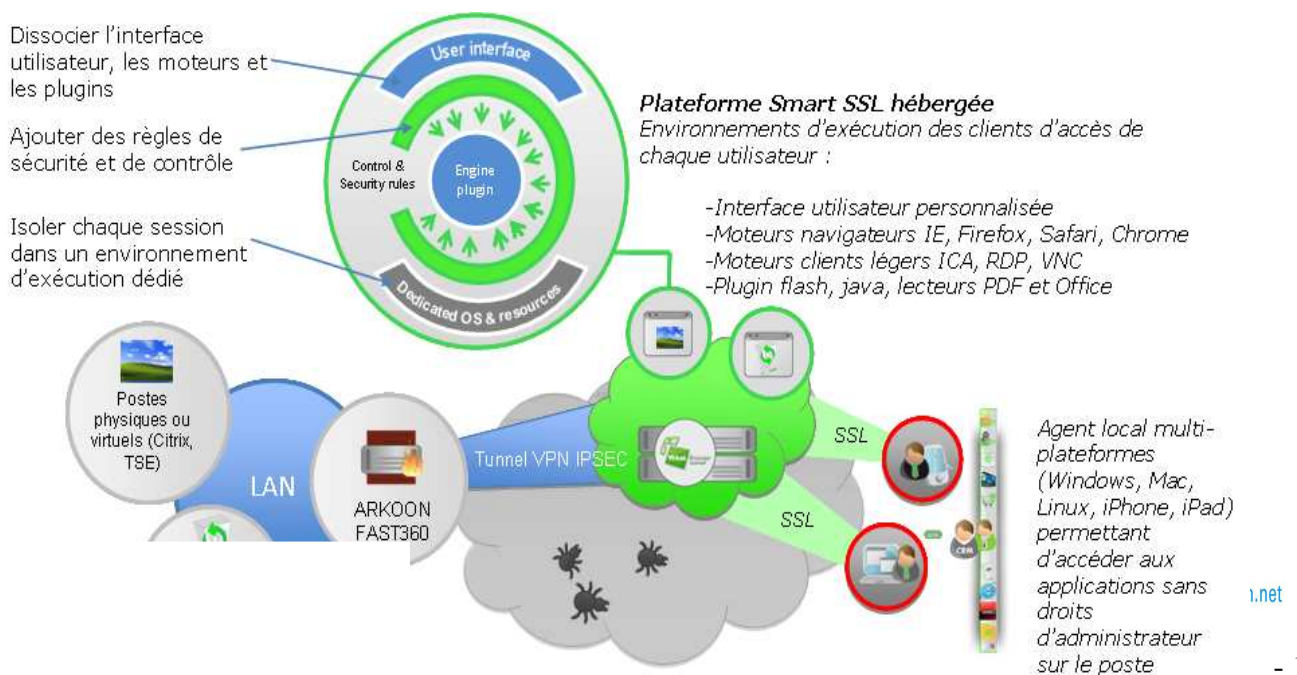
Une licence « flottante » permet depuis une seule option logicielle SmartSSL d'un équipement FAST360 d'accéder à de multiples sites distants. Aucune mise à jour n'est nécessaire par l'administrateur des systèmes. Elles sont assurées par Arkoon sur les serveurs du Cloud Datacenter

➔ SmartSSL est la seule solution du marché qui autorise des accès multi-sites sans aucune infrastructure matérielle locale.

3.1 Architecture globale

Principe de fonctionnement

Arkoon SmartSSL est un client logiciel qui se connecte via le protocole SSL à un serveur de présentation. Ce dernier, hébergé dans le *Cloud Datacenter* Arkoon monte à son tour un tunnel VPN IPSEC avec le réseau de l'entreprise dans lequel se trouvent les serveurs et applications accédés:



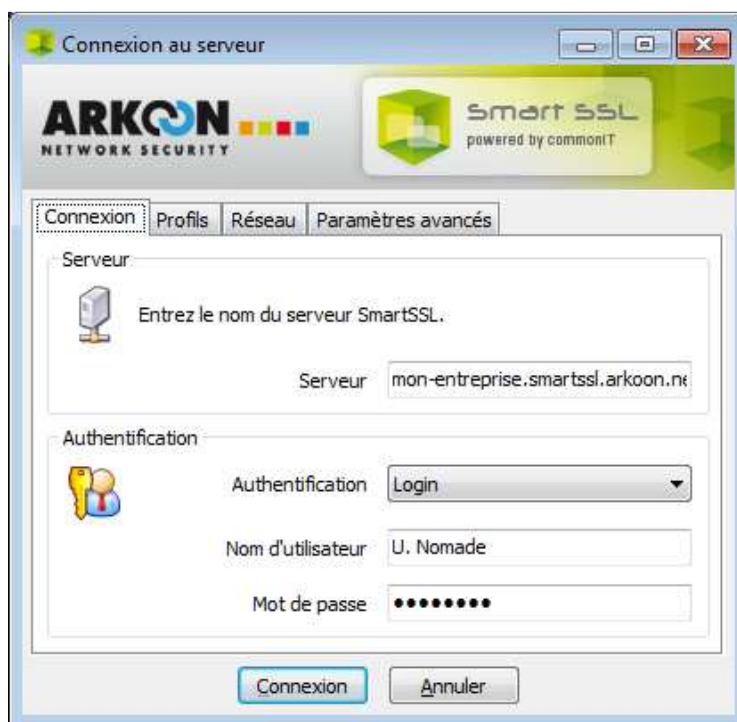
3.2 Les composants

Trois composants principaux sont à considérer dans une topologie SmartSSL :

- 1 Le client SmartSSL ou « agent » SmartSSL
- 2 Le portail de configuration du serveur *Cloud Datacenter Arkoon* sur lequel l'administrateur définit les applications accessibles
- 3 L'appliance Arkoon FAST360 qui protège les serveurs joints par les utilisateurs nomades ;

3.2.1 L'agent SmartSSL

L'agent est le composant logiciel exécuté sur le poste de l'utilisateur. Il est chargé de réaliser la connexion au serveur et de l'affichage déporté du navigateur :



Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975

 www.arkoon.net

- La connexion au serveur est sécurisée par une connexion SSL.
- La connexion au serveur sert à authentifier l'utilisateur, ouvrir les sessions, récupérer les informations de configuration, ...
- L'affichage déporté est réalisé en utilisant le protocole open source NX (NoMachine) et un serveur X local (embarqué seulement sur l'*agent* sous Windows car non nécessaire sur OSX et Linux).

L'agent SmartSSL est décliné sous différentes versions :

- **l'Agent** : version Windows (2000, XP, Vista, 7), Linux, Mac OS
- **l'Agent Portable**: version pour clé USB sans installation ni droit d'administrateur sur le poste
- **l'iAgent**: version iPhone et iPad disponibles sur Apple Store (gratuit)

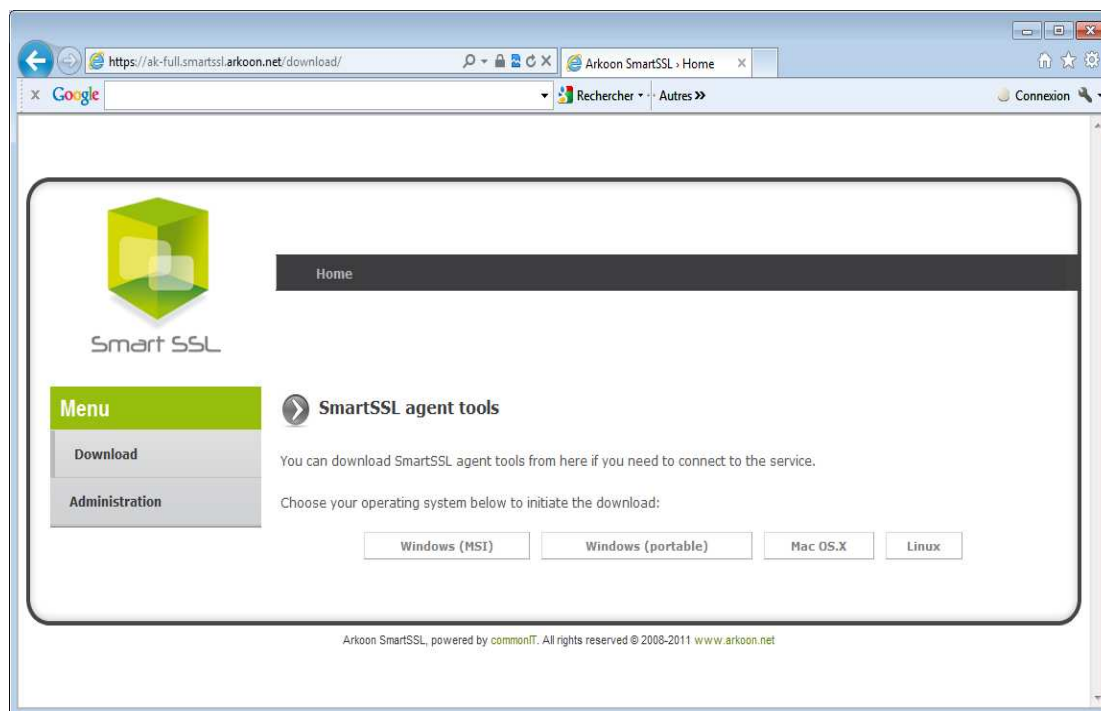
L'agent, dans sa version installable ou portable, pourra être téléchargé depuis n'importe quel accès Internet sur le portail défini pour la société :

Exemple : <http://mon-entreprise.smartssl.arkoon.net>

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975





NB : Aucune configuration particulière n'est à définir sur cet agent. Seuls, l'adresse du portail, le nom de l'utilisateur et son mot de passe sont à renseigner.

Afin de permettre à l'utilisateur une optimisation du fonctionnement de cet agent, certains paramètres peuvent être précisés :

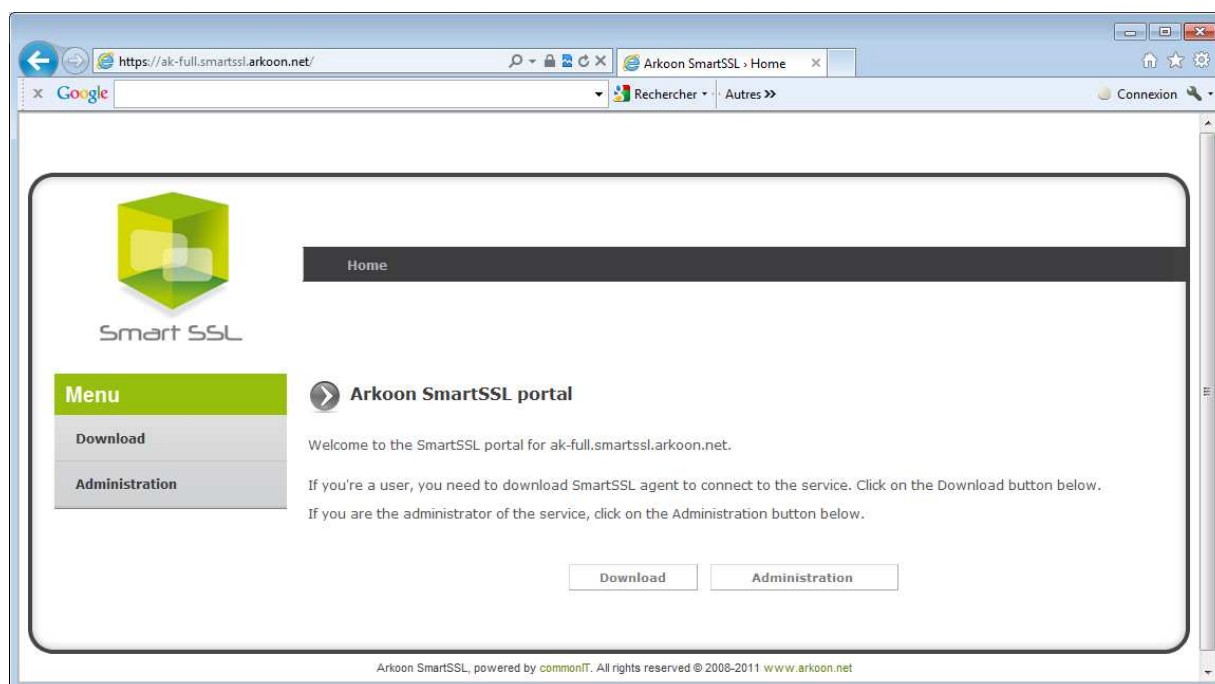
- L'onglet « **Profil** » permet de mémoriser l'ensemble des paramètres de connexion de façon à éviter à l'utilisateur de devoir saisir à chaque connexion les valeurs nécessaires à la montée des tunnels.
- La section « **Réseau** » du client permet l'optimisation de la vitesse de connexion en précisant éventuellement le débit de la ligne Internet utilisée. Il est également possible à cet endroit de spécifier l'utilisation d'un proxy qui serait présent sur le réseau local depuis lequel la connexion est demandée.

- Les « **paramètres avancés** » permettront de choisir la langue utilisée sur le client (Anglais / Français) ainsi que les options associées à la compression des images et des vidéos qui pourraient être consultées.

3.2.2 Le serveur

La partie serveur de la solution est utilisée pour gérer les différentes instances de la solution *SmartSSL*. Elle est hébergée par Arkoon qui assure la mise en œuvre et l'exploitation de l'infrastructure en garantissant le plus haut niveau de sécurité et de disponibilité.

C'est à partir de n'importe quel navigateur web, via une connexion sécurisée (https) que l'administrateur configure et supervise la solution :



Gestion des sessions

Siège social
1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975



Les sessions du navigateur virtuel sont la clé de voute de la configuration du serveur.

NB : Une session correspond à une machine virtuelle sur les serveurs SmartSSL et est unique pour chaque utilisateur.

- Pour chaque session, l'administrateur définit :
 - Les utilisateurs ayant le droit d'accéder à cette session
 - Les applications web (un ensemble d'URL) accessibles depuis cette session
 - Le profil du navigateur (appelé Template), c'est-à-dire son moteur de rendu (emulation IE, Firefow etc.) et ses différents plugins (flash et java notamment)
 - Les droits d'usage et de comportement du navigateur : autoriser ou non les téléchargements, les impressions, l'archivage des cookies, des historiques, ...

Gestion des utilisateurs:

- Les différents utilisateurs de *SmartSSL* sont authentifiés sur une base locale de comptes ou sur un serveur externe (AD, LDAP) relayé par l'appliance FAST360;
- Chaque utilisateur pourra, si l'administrateur l'y autorise, retrouver ses éléments d'archivage de sessions (favoris, cookies, etc.) à chaque connexion d'une session données ;
- L'administrateur de la solution peut autoriser ou non le transfert de fichiers depuis le serveur distant vers la machine locale qui effectue la connexion SSL. Lors de chaque téléchargement

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975



www.arkoon.net

(upload/download), les fichiers passent par une zone dédiée à l'utilisateur sur le serveur. Dans ce cas, l'utilisateur a toujours accès à sa zone d'échange quel que soit le poste qu'il utilise (ce qui peut être utile en situation de mobilité).

NB : L'administrateur peut également, s'il le souhaite, autoriser des transferts de fichiers transparents.

Gestion des applications

- L'administrateur définit les applications qui devront explicitement être isolées dans des sessions spécifiques du navigateur (et donc dans des machines virtuelles cloisonnées) ;
- Les différentes sessions de *Virtual Browser* sont lancées dans un environnement OpenVZ permettant d'isoler les applications les unes des autres dans des machines virtuelles différentes.

Gestion des bureaux distants (Microsoft RDP, Citrix ICA, VNC)

- L'administrateur définit dans cette section quelles sont les applications qui seront autorisées à être exécutées sous Microsoft Terminal Server, Citrix ICA ou encore RealVNC ;

Gestion des navigateurs

Pour chaque session, l'administrateur associe un profil de navigateur.

- Dans le profil du navigateur, l'administrateur sélectionne :
 - Le moteur de rendu utilisé (Firefox 3.0/3.5, IE6, IE7, Chrome, Safari) et les plugins associés ;
 - Si l'impression et le téléchargement (upload/download) de fichiers sont autorisés ;

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



www.arkoon.net

Remarques concernant la sécurité des navigateurs :

- Les composants des navigateurs sont mis à jour régulièrement et automatiquement.
- Le navigateur est lancé dans un environnement virtuel OpenVZ propre et redémarré à chaque ouverture de nouvelle session.
- Le navigateur virtuel bénéficie d'une interface renforcée permettant d'empêcher un accès au système local.
- Les informations de l'utilisateur (cookies, bookmark, ...) sont présentes dans un répertoire monté par le serveur dans l'environnement virtuel.

The screenshot shows the Arkoon SmartSSL web interface. The browser address bar displays https://ak-full.smartssl.arkoon.net/vb_config/sessions/. The page features a navigation menu with 'Home', 'Configuration', 'Authentication', and 'Monitoring'. The 'Configuration' section is active, showing a 'Select Session to Change' page. A table lists sessions with columns for Name, Description, Session configuration, Applications, Groups, and Actions.

Name	Description	Session configuration	Applications	Groups	Actions
Internet		default-browser	-	-	up down enable
Intranet		default-browser	-	vb-group1	up down disable
VB-DEMO		VB-DEMO	-	vb-group1	up down disable
COMPTA		IE7	COMPTA	vb-group1	up down disable

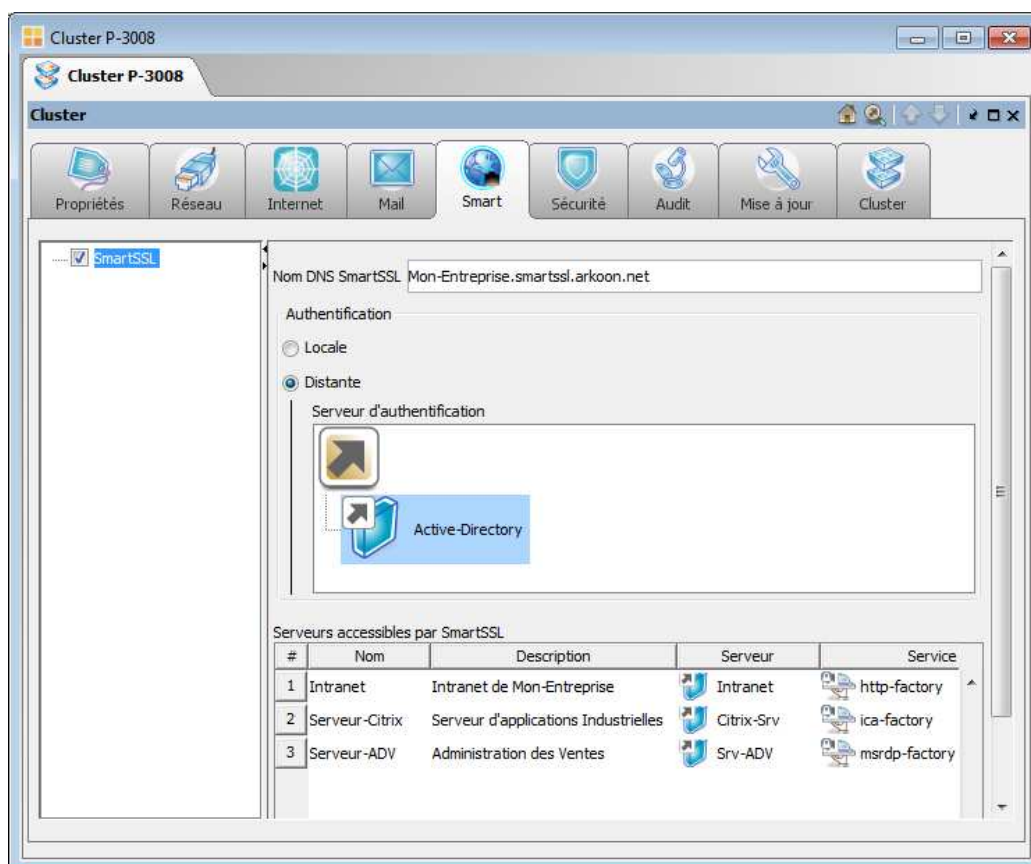
4 Sessions

3.2.3. L'appliance FAST360

L'appliance FAST360 permet d'établir le lien entre la partie serveur de la solution et les ressources clients.

Les mécanismes suivants sont mis en œuvre :

- Création d'un tunnel IPSEC entre l'appliance FAST360 et le serveur SmartSSL: le tunnel est monté automatiquement par l'activation de la fonction dans Arkoon Manager ;
- Synchronisation de la base utilisateur entre le FAST360 et le serveur SmartSSL ;
- Relaying des flux d'authentification pour l'accès aux ressources (proxy Socks) ;
- Règles de flux pour autoriser explicitement l'accès aux ressources internes de l'entreprise ;



Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975

www.arkoon.net

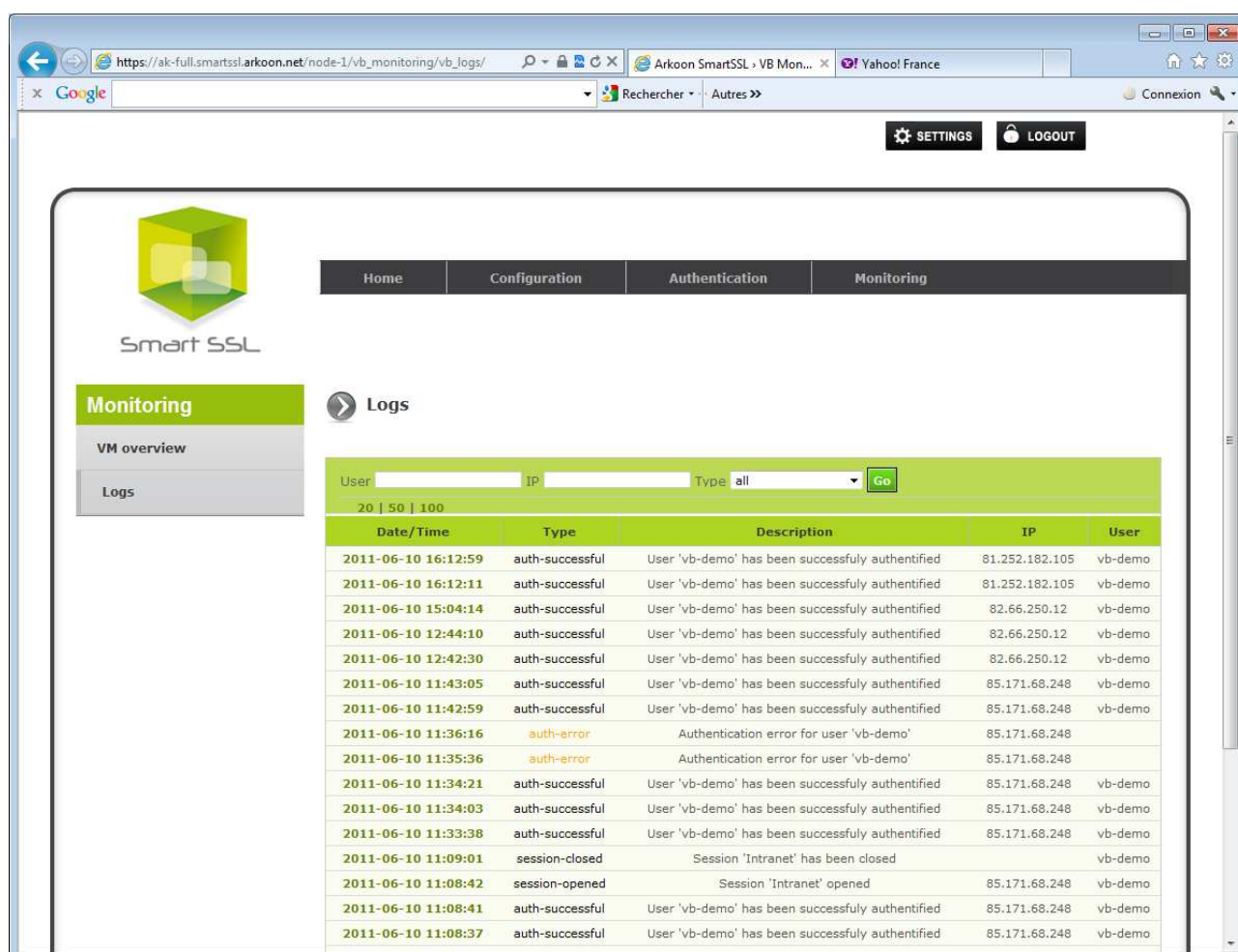
Les tunnels IPsec constitués auront les caractéristiques suivantes :

- Authentification des entités par certificats X509
- Algorithmes de chiffrement : AES
- Longueur des clés : 256 bits
- Hachage : SHA1

3.3 - Monitoring et supervision de la solution

SmartSSL permet une supervision générale de l'activité de ses connexions utilisateurs ;

- Depuis le portail <http://mon-entreprise.smartssl.Arkoon.net>:



The screenshot shows the SmartSSL monitoring interface. At the top, there are navigation tabs: Home, Configuration, Authentication, and Monitoring. The 'Monitoring' tab is active. Below the navigation, there is a 'Monitoring' sidebar with options for 'VM overview' and 'Logs'. The main content area displays a 'Logs' section with a search bar for User, IP, and Type, and a 'Go' button. Below the search bar, there is a table with the following data:

Date/Time	Type	Description	IP	User
2011-06-10 16:12:59	auth-successful	User 'vb-demo' has been successfully authenticated	81.252.182.105	vb-demo
2011-06-10 16:12:11	auth-successful	User 'vb-demo' has been successfully authenticated	81.252.182.105	vb-demo
2011-06-10 15:04:14	auth-successful	User 'vb-demo' has been successfully authenticated	82.66.250.12	vb-demo
2011-06-10 12:44:10	auth-successful	User 'vb-demo' has been successfully authenticated	82.66.250.12	vb-demo
2011-06-10 12:42:30	auth-successful	User 'vb-demo' has been successfully authenticated	82.66.250.12	vb-demo
2011-06-10 11:43:05	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:42:59	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:36:16	auth-error	Authentication error for user 'vb-demo'	85.171.68.248	
2011-06-10 11:35:36	auth-error	Authentication error for user 'vb-demo'	85.171.68.248	
2011-06-10 11:34:21	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:34:03	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:33:38	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:09:01	session-closed	Session 'Intranet' has been closed		vb-demo
2011-06-10 11:08:42	session-opened	Session 'Intranet' opened	85.171.68.248	vb-demo
2011-06-10 11:08:41	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo
2011-06-10 11:08:37	auth-successful	User 'vb-demo' has been successfully authenticated	85.171.68.248	vb-demo

- Depuis les journaux d'activité IP dans Arkoon Monitoring de votre équipement FAST360.

3.4 – Compatibilité des services Web

L'architecture de SmartSSL consiste à dédier une instance virtuelle par session web sur le serveur.

De cette manière l'entreprise peut définir pour chaque application la version du navigateur qui sera utilisée. Par exemple, si une application de l'intranet n'est compatible qu'avec le moteur Firefox 3.0 utilisant le plugin java JRE 1.6, tous les utilisateurs exécuteront automatiquement ce navigateur sans même s'en rendre compte, quel que soit le terminal utilisé.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975



4. Caractéristiques de l'offre

4.1 – Les versions

SmartSSL se décline en deux versions : **SmartSSL Light** & **SmartSSL Full**.

La version « **Light** » de SmartSSL autorise jusqu'à 3 applications maximum accessibles à distance et exécutables en simultané :

- 1 application de type http / https
- 2 applications de type RDP (Citrix et/ou Microsoft TSE ou VNC)

Exemple :

- 1 application de type Intranet (http)
- + 1 application Microsoft TSE
- + 1 application Citrix ICA

Ou encore :

- 1 application Intranet (HTTPS)
- + 1 application Microsoft TSE
- + 1 application VNC

La version « **Full** » de SmartSSL autorise un nombre d'applications non restreint.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



4.2 - Mode de licence

SmartSSL est disponible sur toute appliance FAST360 de la série NPA, XLarge ou Performance en versions 5.0/22 et supérieures.

Cette option logicielle est définie par modèle d'apppliance FAST360 utilisé, tout comme peut l'être un service de sécurité « antivirus », Antispam ou filtrage d'URL avancé pour 1 an ou 3 ans.

Chaque modèle d'apppliance compatible propose ainsi un nombre maximal d'utilisateurs SmartSSL simultanés (utilisateurs déclarés).

Série NPA	S150	S250	M500	M1000	L1800	L2500	L3200
Nb utilisateurs déclarés	15	35	70	150	250	300	350
Licence Flottante (150 U)	-	-	-	-	√	√	√

Série Performance	P-1206	P-1808	P-2508	P-3008
Nb utilisateurs déclarés	70	150	250	300
Licence flottante (150 U)	-	√	√	√

Série XLarge	A2200	A5200
Licence flottante (150 U)	√	√

Le mode 'licence flottante' autorise un nombre maximal d'utilisateurs déclarés qui seront répartis sur plusieurs appliances FAST360 (entreprises multisites).

5. Questions / Réponses

Q. Qu'est ce qu'une « SANDBOX » ?

R. Une Sandbox, littéralement « bac à sable », consiste à réserver et à dédier une partie de la mémoire d'un ordinateur pour y faire exécuter une application. Le problème d'une Sandbox, contrairement au concept initial où cet espace se voulait totalement imperméable, est qu'il n'est pas vraiment dissociable du système hôte.

Un très bon article présente cette technologie et ses failles: <http://www.infoworld.com/d/security-central/does-sandbox-security-really-protect-your-desktop-105>

Une Sandbox se trouve ainsi être vulnérable. La technologie du Navigateur Virtuel utilisée par SmartSSL est la seule qui puisse garantir le niveau de sécurité attendu.

Q. Sur la machine depuis laquelle je vais monter la connexion SSL, dois-je disposer de droits de type « administrateur » afin d'y installer l'agent ?

R. Les simples droits « Utilisateur » suffisent pour installer le client SmartSSL.

Q. Le module 'Serveur' est hébergé et exploité par Arkoon. Comment me garantissez-vous la sécurité de mes données et la disponibilité de l'accès ?

R. La sécurité étant depuis plus de 10 ans le cœur de métier d'Arkoon, toutes les mesures visant la protection du centre d'hébergement sont mises en œuvre. La disponibilité des connexions est assurée par des équipements installés en mode Haute Disponibilité et des liens Internet redondants.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



Q. Peut-on permettre aux utilisateurs de surfer sur Internet depuis SmartSSL?

R. L'administrateur pourra, par configuration, permettre aux utilisateurs de ressortir vers Internet. Pour ce faire l'administrateur configurera sur le FAST360 une redirection transparente des flux web vers le proxy interne de l'Appliance de sécurité FAST360 Arkoon ou encore celui d'une Virtual Edition Web&Mail Arkoon.

La conception de SmartSSL (étanchéité du poste de travail avec le navigateur virtuel) permettra à l'utilisateur l'utilisation de sa propre ligne ADSL ou accès Internet pour surfer, même si une connexion vers les ressources de l'entreprise est en cours.

Q. Je suis administrateur et je dois accéder à un serveur en SSH. Comment puis-je procéder ?

R. Très simplement : il faudra pour cela établir une connexion 'Bureau déporté' (RDP, ICA, VNC) avec un poste du réseau local pouvant accéder en SSH au serveur à atteindre.

Q. Combien de temps faut-il pour déployer de manière opérationnelle une solution SmartSSL ?

R. Toute l'infrastructure hébergée étant opérationnelle, le déploiement de la solution se résume aux opérations de configuration du module 'Serveur' et du FAST360 à travers une interface graphique très simple. En moyenne, la solution peut être totalement paramétrée en configurée en moins d'une demi-journée.

Q. Est-il possible d'autoriser malgré tout des transferts de fichiers ou des impressions depuis une connexion SmartSSL ?

R. Oui, seul l'administrateur décide de cette possibilité dans l'interface d'administration. Ces zones d'échanges, pourront être configurées par utilisateur par utilisateur.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 € RCS Lyon 428 173 975



Q. Est-il possible de personnaliser le portail d'accès ou les navigateurs virtuels ?

R. Oui, les thèmes des navigateurs pourront être modifiés suivants 8 modèles différents prédéfinis. Le contenu de ces navigateurs pourra faire également l'objet d'une personnalisation en ajoutant ou supprimant des boutons présentés par défaut : page précédente, suivante, impression, stop etc ...

Les icônes représentant chacune des sessions accessibles par l'utilisateur pourront être téléchargées à souhait et être modifiées par l'administrateur.

Siège social

1 place Verrazzano - 69009 Lyon
Tél. +33 (0)4 72 53 01 01 - Fax +33 (0)4 72 53 12 60
S.A. au capital de 4 605 019 €RCS Lyon 428 173 975



www.arkoon.net