

A blue-themed graphic featuring a world map in the background. Overlaid on the map are several yellow, 3D cube-like shapes of varying sizes, connected by dashed white lines. In the foreground, a black Arkoon SSL360 appliance is shown, with a smaller S20 Series unit stacked on top. A white dot on the top of the S20 unit is connected by a dashed line to the largest cube in the diagram. The background also features faint binary code (0s and 1s).

Appliances SSL360



La gamme des appliances Arkoon SSL360 est dédiée à la fonction de passerelle VPN SSL, et rend vos données et vos applications disponibles en toute simplicité et en toute sécurité.

Au travers d'un canal chiffré, le VPN SSL permet à des utilisateurs mobiles d'accéder à toute application (messagerie, Intranet, bureau déporté,...) par l'intermédiaire d'un navigateur Web.

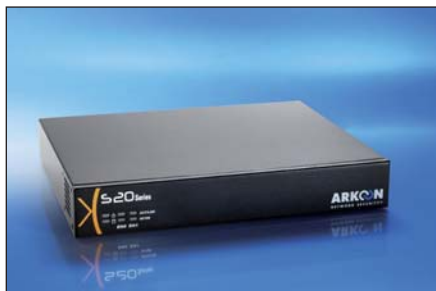


La gamme SSL360



Parce qu'elle simplifie la mise en place de réseaux privés virtuels, la technologie VPN SSL devient un composant clé des architectures de mobilité. Arkoon Network Security conçoit ses produits SSL360 avec la volonté de fournir le meilleur niveau de sécurité, de performance et de simplicité d'utilisation.

S20 Series



La famille S20 Series est destinée aux entreprises ayant des populations nomades de quelques dizaines d'utilisateurs.

Conçu pour permettre aux petites et moyennes entreprises de bénéficier de l'ensemble des fonctionnalités VPN SSL sur un produit d'entrée de gamme, le S20 est un concentré de technologie dans un produit mini tant par sa taille que par son prix.

S100 Series



Les appliances SSL360 S100 Series sont des appliances de forte capacité qui répondent aux besoins des entreprises dont la flotte des utilisateurs mobiles compte une centaines de personnes.

Le S100R restreint le nombre d'utilisateurs simultanés à 50, tandis que le S100U a une capacité de plus de 100 utilisateurs simultanés, sans restriction logicielle.

Les différents types d'accès aux applications



Une fois les utilisateurs identifiés et le tunnel SSL actif, les appliances SSL360 permettent d'accéder à des applications internes de l'entreprise selon 3 modes.

1. Le Reverse Proxy : pour les applications HTTP/HTTPS

Les appliances SSL360 intègrent la technologie SWA (Secure Web Agent) qui permet d'accéder de manière transparente à la totalité des applications Web :

- les standards Webmail comme OWA (en mode natif) et Lotus Domino iNotes,
- les Front-Ends de progiciels classiques comme les PGI ou les systèmes décisionnels,
- les applications Intranet spécifiques.

2. Les services "Webifiés"

Les applications de bureaux déportés (Terminal Server ou Citrix) ne sont pas des applications Web. L'appliance SSL360 propose des mécanismes qui permettent de rendre ces applications (et d'autres) disponibles en mode web, par l'intermédiaire d'une applet Java, d'un composant ActiveX ou d'une technologie similaire.

3. Le Virtual Passage : pour toutes les applications IP

Pour les applications complexes, pour lesquelles aucun mécanisme de "webification" n'est possible, la technologie Virtual Passage est la solution.

En effet, Virtual Passage est un composant qui s'installe automatiquement sur le poste nomade et qui permet l'accès en mode natif à toutes les applications du réseau interne de l'entreprise (messagerie, CRM, logiciel de gestion,...).

Pour l'utilisateur, tout se passe comme si son poste était physiquement sur le réseau interne de l'entreprise (allocation d'une adresse IP interne, utilisation des clients lourds pour accéder aux applications et ressources du réseau,...).

Parce que Virtual Passage répond aux mêmes usages que la technologie VPN IPSEC, mais sans intervention sur le poste mobile, il constitue une alternative aux déploiements de clients IPSEC sur les flottes nomades.

Usages, fonctionnements et bénéfices



Se connecter depuis n'importe où

Un simple navigateur Web permet de créer le tunnel VPN SSL (via un portail d'accès) et d'accéder à la plupart des applications.

En outre, le VPN SSL utilise le port TCP 443 (HTTPS) qui est autorisé par la plupart des firewalls. Un utilisateur nomade peut donc se connecter en VPN SSL depuis le réseau d'un partenaire ou d'un client sans modifier la configuration du pare-feu local.

BÉNÉFICES //////////////////////////////////////

- Vos données sont plus disponibles, en toute sécurité.

Créer des extranets sécurisés

L'accès au VPN SSL ARKOON se fait via un portail sécurisé qui peut être personnalisé en fonction des populations d'utilisateurs auxquelles il s'adresse.

Pour chaque portail, vous définissez :

- Le visuel et les messages d'accueil
- Les applications disponibles
- Les domaines d'authentification accessibles

BÉNÉFICES //////////////////////////////////////

- L'accès à vos données est contrôlé et adapté.

Alléger la tâche de l'administrateur

Le fonctionnement "sans client" permet aux entreprises de s'affranchir de toute intervention de l'administrateur réseau sur le parc d'ordinateurs nomades.

Que ce soit pour la configuration ou pour le support auprès des utilisateurs, l'intervention de l'administrateur est restreinte à l'appliance SSL360.

BÉNÉFICES //////////////////////////////////////

- Vos coûts d'administration de la mobilité sont réduits.

Profiter d'un unique fournisseur pour toutes les appliances de l'architecture de sécurité

Le VPN SSL est un élément d'une architecture qui met en œuvre un équipement de sécurité réseau.

L'environnement d'administration, de mise à jour et de support technique des appliances SSL360 est le même que celui des appliances ARKOON UTM FAST360.

BÉNÉFICES //////////////////////////////////////

- La cohérence de votre architecture de sécurité de est renforcée.



**Accédez
à vos données
où que vous soyez !**

La place du VPN SSL dans une architecture de sécurité

1. Contrairement à IPSec, SSL est un protocole applicatif qui nécessite la mise en œuvre d'un serveur Web pour constituer le portail d'accès et d'un reverse proxy pour le chiffrement des applications Web.

Recommandation : un serveur VPN SSL ne doit pas être intégré sur une appliance de sécurité UTM. La présence de services applicatifs ouverts vers l'extérieur serait de nature à compromettre l'équipement de sécurité réseau.

2. Le VPN SSL est un serveur d'accès et de chiffrement, il ne faut pas lui déléguer le rôle de sécurité réseau assuré par l'équipement UTM. Un serveur VPN SSL ne doit jamais se placer en coupure entre Internet et le réseau interne ou les serveurs de l'entreprise.

Recommandation : Les appliances Arkoon SSL360 sont des produits spécialisés, destinés à être isolés sur la DMZ d'un pare-feu pour tirer partie des fonctions de protection offertes par ce dernier : firewall, prévention et détection d'intrusions, antivirus...

Arkoon vous propose les gammes d'appliances complémentaires SSL360 et FAST360 (Appliance UTM) pour vous permettre de construire une architecture de sécurité et de mobilité homogène.

Caractéristiques techniques



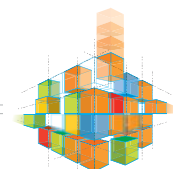
	S20R/ S20U	S100R/ S100U
Performance		
Débit VPN SSL (Mbps)	12	75
Nouvelles connexions VPN SSL / sec.	20	75
Nombre de pages / seconde	400	1 700
Nombre d'utilisateurs simultanés autorisés	10/Illimité	50/Illimité
Nouvelles connexions / sec.	500	1 000
Matériel		
Port console	1	1
Ports FastEthernet 10/100	2	2
Processeur	533 Mhz	2 Ghz
RAM	256 Mo	256 Mo
Carte Flash	128 Mo	128 Mo
Kit Rack	oui	oui
Portail d'accès		
Personnalisation des logos, thèmes, applications		oui
Gestion multiportails		oui
Support de plusieurs domaines d'authentification par portail		oui
Applications supportées		
Applications HTTP et HTTPS (Webmail, Standards, Spécifiques...): - Internet Explorer - Mozilla Firefox		Toutes selon préconisations d'Arkoon
Emulation du client via applet Java ou ActiveX		TSE RDP, CITRIX ICA, SSH, Telnet, VNC
Emulation du client en HTML dans le navigateur		FTP, partage de fichiers, voisinage réseau
Virtual Passage (toute application IP, TCP ou UDP)		oui
Navigateurs Web supportés		
Navigateurs Web Supportés		Internet Explorer 5.0 + ; Mozilla Firefox 1.0 + (Windows et Linux) ; Netscape 7.0 + (Windows et Linux) ; Opera 7.0

	S20R/ S20U	S100R/ S100U
Authentification		
Base interne d'utilisateurs (login et mot de passe)		oui
Annuaire externe LDAP, NT, Radius, Windows Active Directory		oui
Certificats électroniques X509 (sur carte à puce, clé USB)		oui
Modes d'authentification RSA SecurID supportés		Token code only ; PIN + Token (avec PIN défini par le système)
Autorisations		
Gestion des accès		Par utilisateurs et groupes, par domaines, par applications, par adresses IP
Configuration		
Interface Web Admin stand alone (SSL)		oui
Connexions à distance (LAN ou WAN)		oui
Mode console et ligne de commandes (SSH)		oui
Mise à jour système à distance		oui
Supervision		
Interface Web Admin stand alone (SSL)		oui
Supervision temps réel		Charge CPU et occupation mémoire
Connexions à distance (LAN ou WAN)		oui
Export de journaux et d'alertes (Syslog)		oui
Dimensions		
Format	Slim Desktop	1U
I/L/H (mm)	280/230/44	430/390/44
Poids	2 kg	10 kg
Environnement		
Température de fonctionnement	0 à 40 °C	0 à 40 °C
Humidité de fonctionnement	20 à 90%	20 à 90%
Température de stockage	0 à 70 °C	0 à 70 °C
Humidité de stockage	5 à 95%	5 à 95%
Alimentation	100/240 V	100/240 V
Fréquence	48 - 63 Hz	48 - 63 Hz
Puissance électrique max	45 W	250 W
Certifications	CE/FCC/UL	CE/FCC

Retrouvez l'ensemble de nos produits et leurs fiches détaillées sur :
www.arkoon.net

ARKOON

1, Place Verrazzano
CS 30603
69258 Lyon Cedex 09 - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.net



ADAPTIVE SECURITY