

PROJET SYDONIA
Closes Techniques
Installations Clients VPN

Pré requis site client

Suite aux différents tests effectués lors de la mise en place du site pilote, veuillez trouver ci-dessous les pré requis techniques définis pour la mise en place des clients VPN.

Prise en charge de l'installation :

SYSCOM prend en charge les installations initiales du client VPN.

On entend par « installation initiale » l'installation du client CheckPoint SecureClient, sa configuration pour l'établissement d'une connexion VPN vers le Firewall du SMAI et le test de connexion de l'application SYDONIA au serveur.

L'installation initiale concerne également les instructions données aux utilisateurs pour l'utilisation du client SecureClient.

Tout autre installation ou réinstallation nécessaire suite à un problème hardware du poste de travail (changement disque dur ou autre composant obligeant un reformatage et réinstallation du système d'exploitation) ne sera pas considérée comme « installation initiale » et fera l'objet d'une prestation supplémentaire.

Chaque client disposera des documents et sources nécessaires pour effectuer lui-même la réinstallation du client SecureClient.

Connexion Internet :

- Optimo 125 - 250 - 500 - 1000
- Numéris 64 ou 128

Les connexions à Internet de poste isolé en modem analogique ne seront pas supportées

Partage de connexion à Internet :

Les connexions à Internet sont en général gérées soit par un simple Modem-router ADSL, soit par un Firewall soit par un simple proxy.

Dans tous les cas, ce moyen de connexion à Internet devra impérativement implémenter les normalisations suivantes :

Les postes passant par un Proxy http ou ftp ne sont pas pris en charge.

- VPN Pass Through (IPSec, L2TP, PPTP)
- Fonction NAT / NAT / Dynamic NAT

Modem-router ADSL testés et validés :

- ADSL Modem-router Planet ADE 3000 / ADE 3100 / ADE4000
- Linksys WAG54P
- Netgear DG814

Firewall testés et validés :

- Firewall ASTARO
- Firewall PIX CISCO
- Firewall Checkpoint
- SonicWall

Pour tout autre équipement, **SYSCOM** fera des tests de connexion VPN. Si ces connexions s'avèrent impossibles, le client devra se mettre en conformité d'après les éléments donnés ci-dessus.

Adressage IP du réseau :

Si l'adressage IP du réseau respecter la norme RF1918, les adresses suivantes sont autorisées

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

A l'exception de :

10.30.20.0 / 255.255.255.0
192.168.102.30 / 255.255.255.255

Poste client VPN SecureClient :

Les postes sur lesquels sera installé le client VPN SecureClient devront fonctionner sous Windows 2000 SP4 ou Windows XP SP1 ou SP2 (**Windows XP fortement conseillé**)

Si des applications Firewall (type ZoneAlarme ou autre) sont installés sur les postes de travail, ces derniers devront être désinstallés.

Ces postes doivent absolument avoir un accès direct à Internet (au travers d'un Firewall ou d'un modem-router). Les postes passant par un Proxy http ou ftp ne sont pas pris en charge.

Les postes de travail devront fonctionner sur un système ne présentant pas de dysfonctionnement majeur (plantage système, blocage, erreur système). Si des problèmes d'installation interviennent lors de la configuration du poste, **SYSCOM** ne prendra en aucun cas en charge la reconfiguration ou réinstallation du poste client. A la demande du client, cette prestation pourra faire l'objet d'une étude et d'un devis de mise en conformité du poste.

Dans le cas où l'installation du client SecureClient s'avère impossible, une fiche « Incident d'installation » sera rédigée.



Note importante : Les intervenants **SYSCOM** devront pouvoir disposer soit des informations permettant l'accès aux équipements Firewall ou modem-router du site, soit de disposer de l'intervenant sur ces éléments si des modifications de paramètres sont nécessaires.

Laurent ALLUYN
lalluyn@syscom.nc
Mobilis : 76.70.25