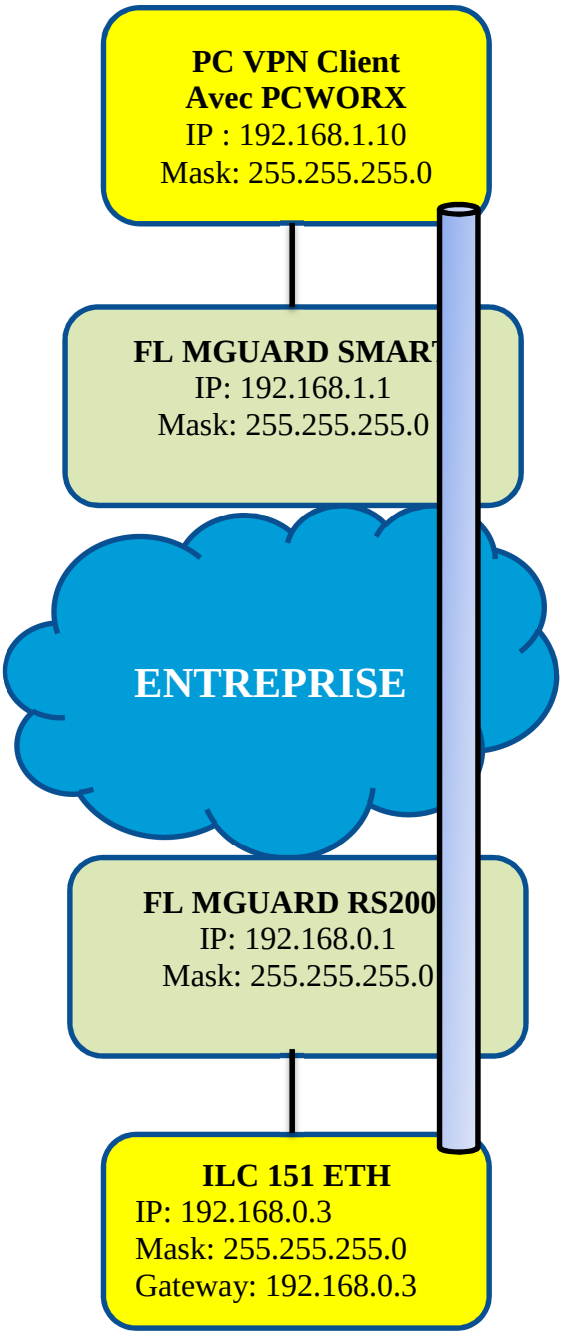
FL MGUARD

Liaison VPN IPsec PSK

Version : 1

But du manuel :

Ce guide vous permettra de mettre en œuvre une liaison VPN IPsec avec « Preshared Secret Key » entre un PC et un automate programmable de réseaux différents grâce à l'utilisation de deux routeurs avec pare feu intelligent de type FL MGUARD.



Annexes :

Annexe 1 : Versions Logicielles et matérielles utilisées pour ce manuel

Matériels :

Fabricant	référence	Type	Version Hardware	Version Firmware
INNOMINATE	2700639	FL MGUARD SMART2 VPN	00003000	7.4.1
INNOMINATE	2700642	FL MGUARD RS2000 VPN	00003200	7.4.0
PHOENIX CONTACT	2700974	ILC151ETH	HW00	FW400

Logiciels :

Fabricant	lien	Type	Version
PHOENIX CONTACT		PCWORX	
SHREW	https://www.shrew.net/download/vpn	ShrewSoft VPN Client	V2.2.2
INNOMINATE	https://fr.cloud.mguard.com/	Secure Cloud	

Annexe 2 : Révision document

Version en cours : 1

Version	Date	Opérateur	Commentaires
1	27/05/2015	JF.FOUARD	Création

Architecture :

PC Client réseau local LAN1 :
Adresse IP : 192.168.1.10
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.1.1 (adresse locale du MGUARD1)

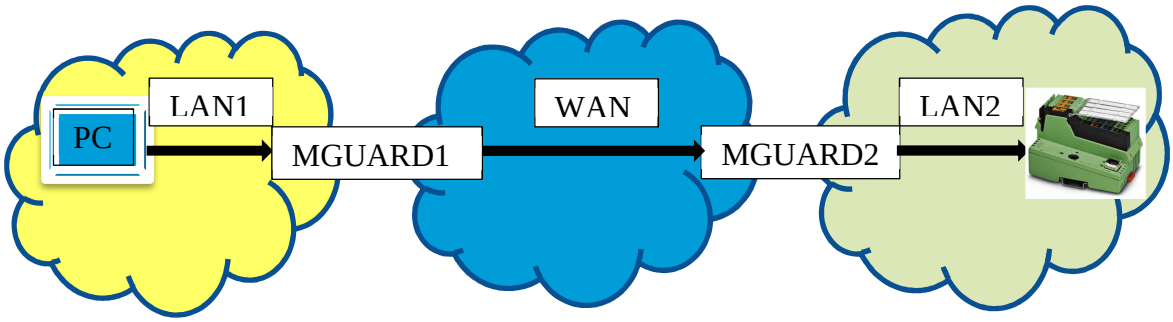
MGUARD1 réseau local LAN1 :
Adresse IP : 192.168.1.1
Masque de sous-réseau : 255.255.255.0

MGUARD1 réseau WAN :
Adresse IP : 10.1.80.100
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 10.1.80.101 (adresse WAN du MGUARD2)

MGUARD2 réseau local LAN2 :
Adresse IP : 192.168.0.1
Masque de sous-réseau : 255.255.255.0

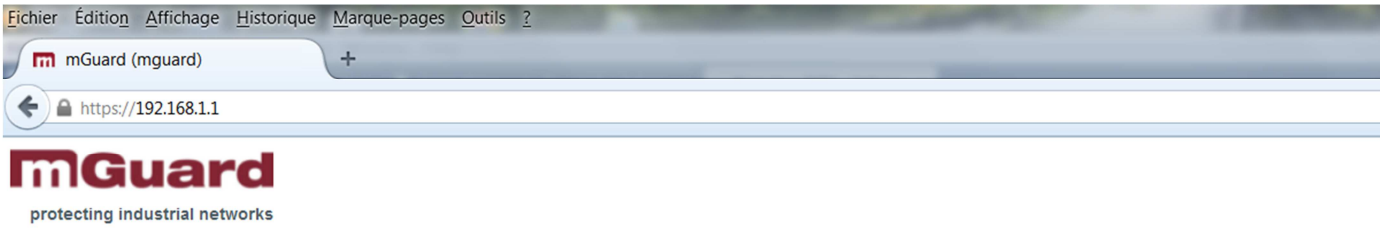
MGUARD2 réseau WAN :
Adresse IP : 10.1.80.101
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 10.1.80.100 (adresse WAN du MGUARD1)

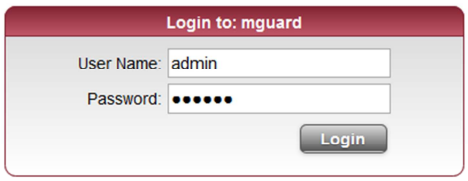
ILC150ETH réseau local LAN2 :
Adresse IP : 192.168.0.3
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.0.1 (adresse locale du MGUARD2)



Configuration du MGUARD SMART2 VPN

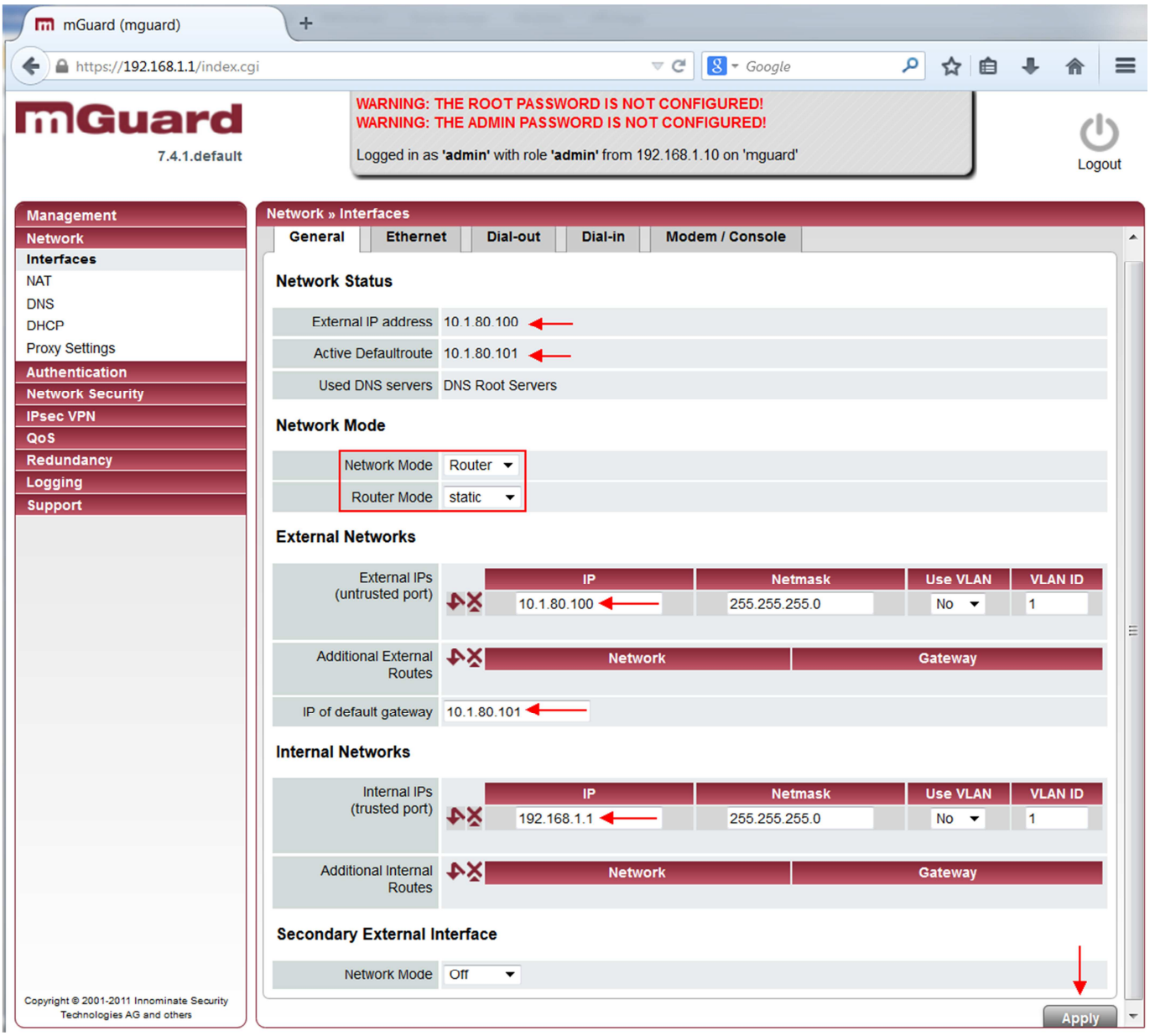
Via n'importe quel explorateur Windows, se rendre sur l'adresse IP LAN du MGUARD : https://192.168.1.1 ou WAN https://1.1.1.1 puis entrer l'utilisateur « admin » et le mot de passe « mGuard ».
Tous ces paramètres sont les paramètres par défaut et modifiables.





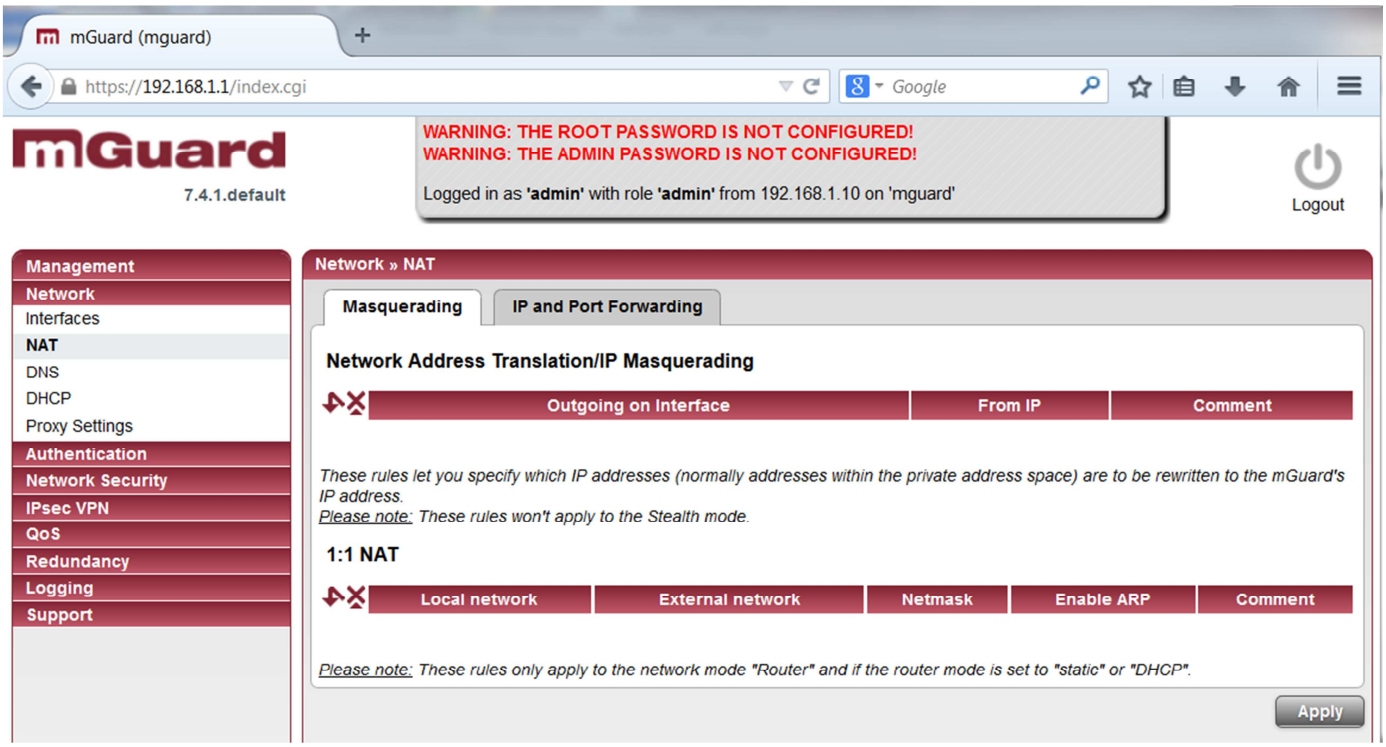
Si le MGUARD dispose déjà d'une adresse IP inconnue ou qu'il n'est plus accessible, utiliser la procédure de remise en configuration usine, deux séquences de 6 appuis à fréquence constante sur le bouton « Reset ».

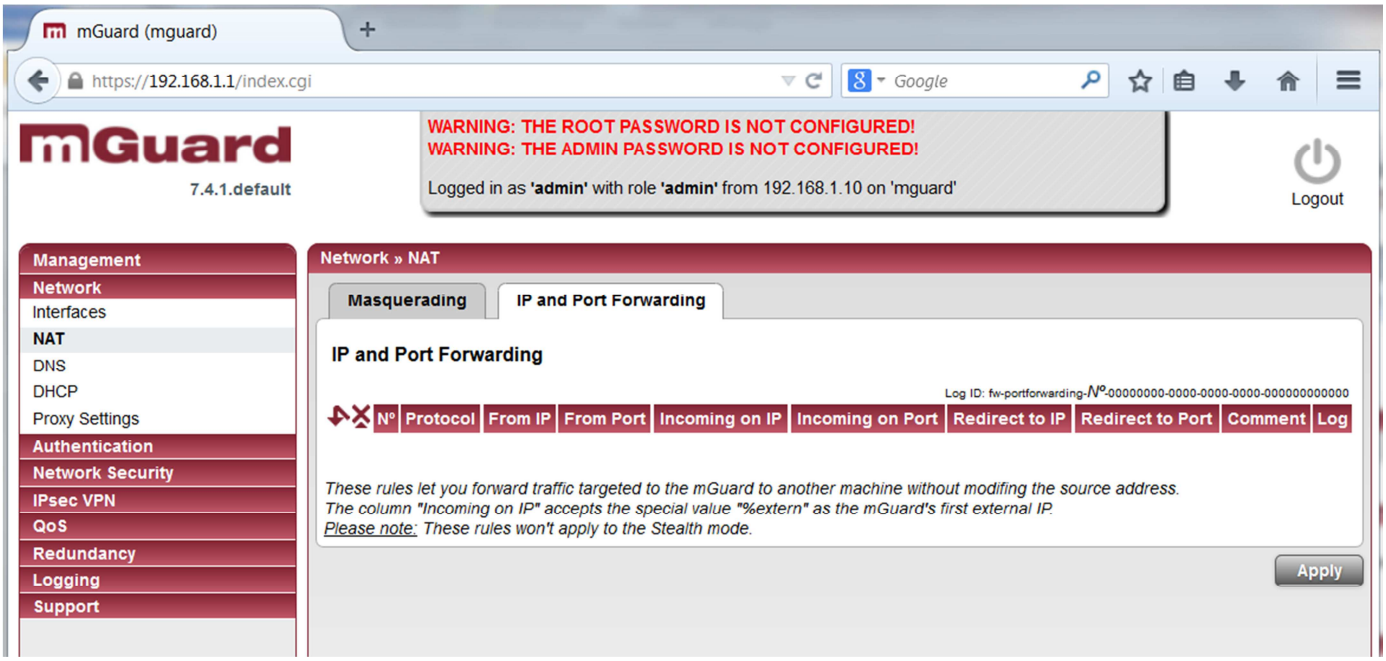
Dans le menu « Network/Interfaces/Général » penser à changer le « Network Mode » en mode routeur car initialement paramétré en « Stealth ».



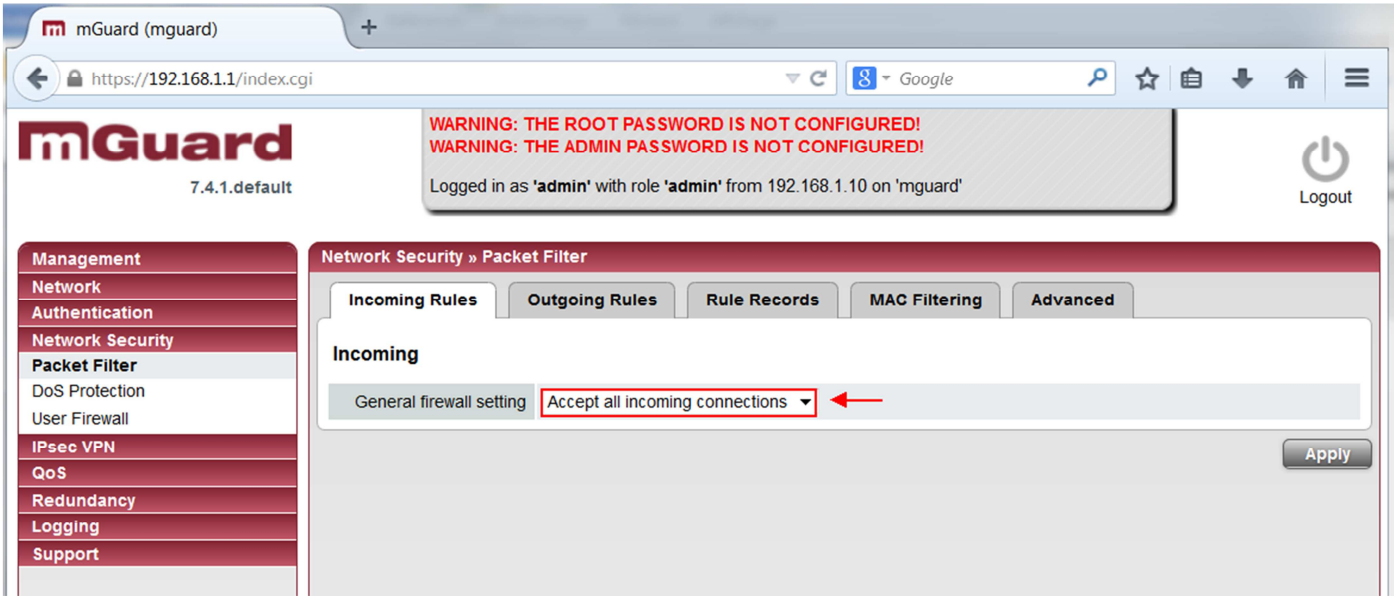
Renseigner les adresses IP sur le modèle de l'architecture.
Nous rappelons qu'il est important de valider toute modification par le bouton « Apply » avant de changer de page sous peine de les perdre.

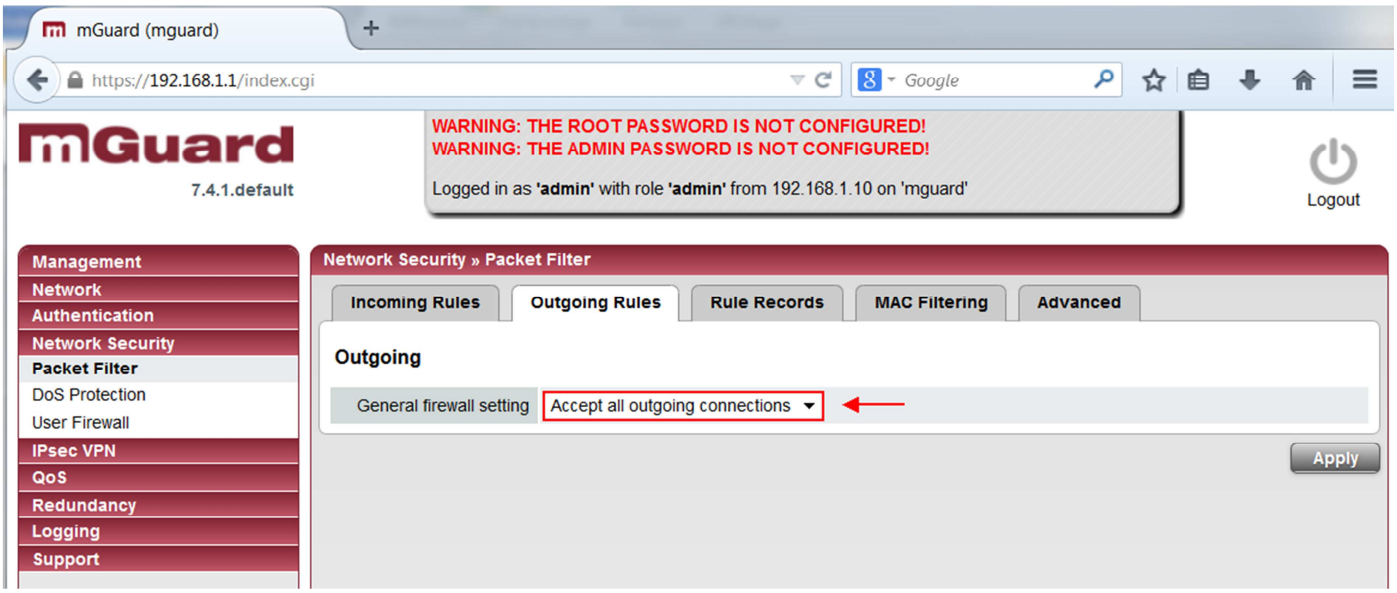
Dans les menus « Network/NAT/Marquerading » et « Network/NAT/IP and Port Forwarding » assurez-vous qu'aucun paramétrage ne soit effectif. En effet quand l'authentification par « Pre-Shared Secret Keys est utilisé il ne faut pas activer le « Network Adress Translation ».



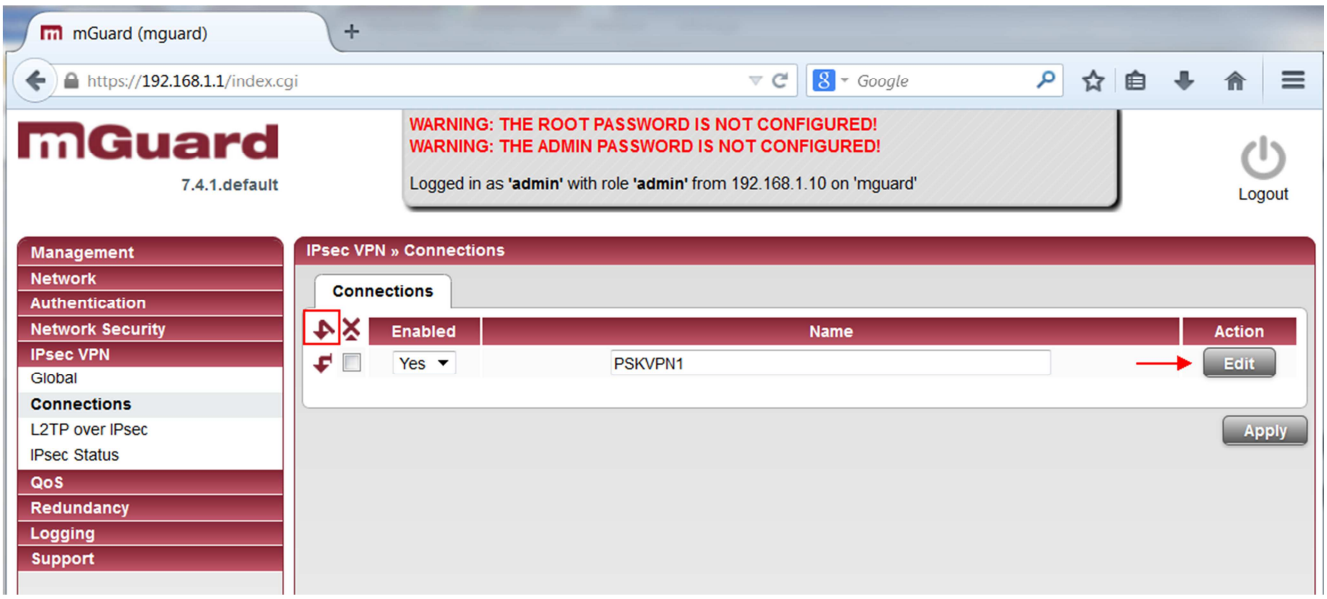


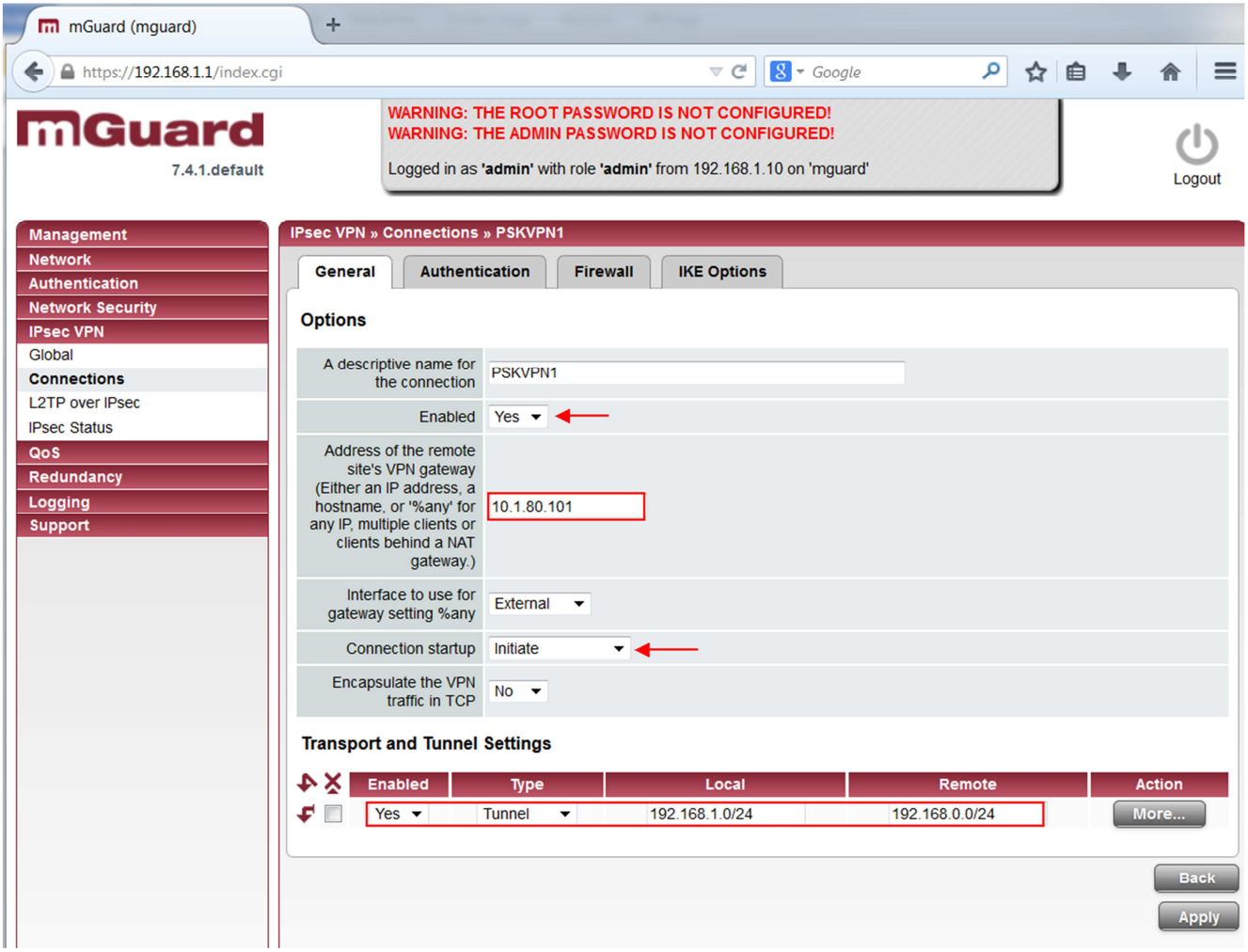
Dans les menus « Network security/Packet Filter/Incoming rules » et « Network security/Packet Filter/Outgoing rules » vérifiez que les règles de Firewall permettent tout trafic entrant et sortant.



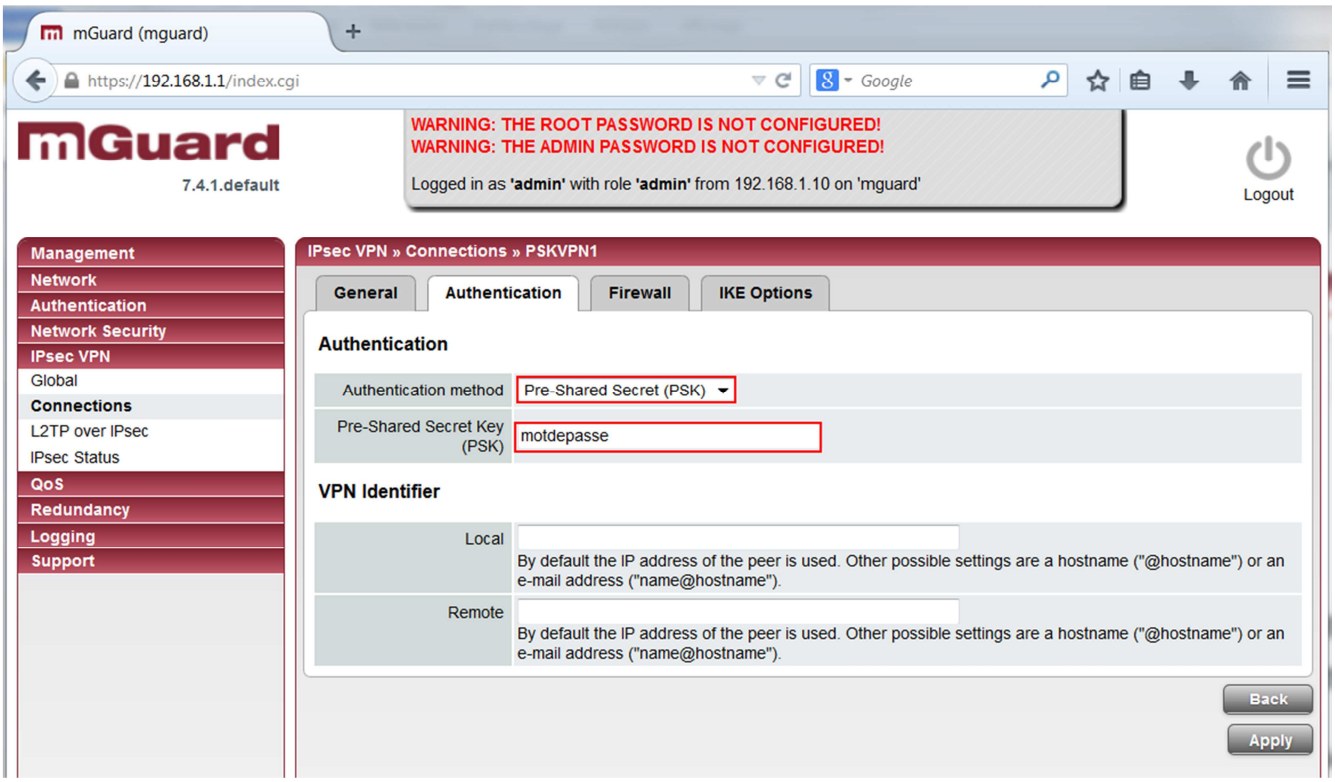


Dans le menu « IPsec VPN/Connections » créez une connexion VPN en sélectionnant la flèche encadrée puis appuyez sur la touche Edit pour faire apparaître les paramètres à renseigner.

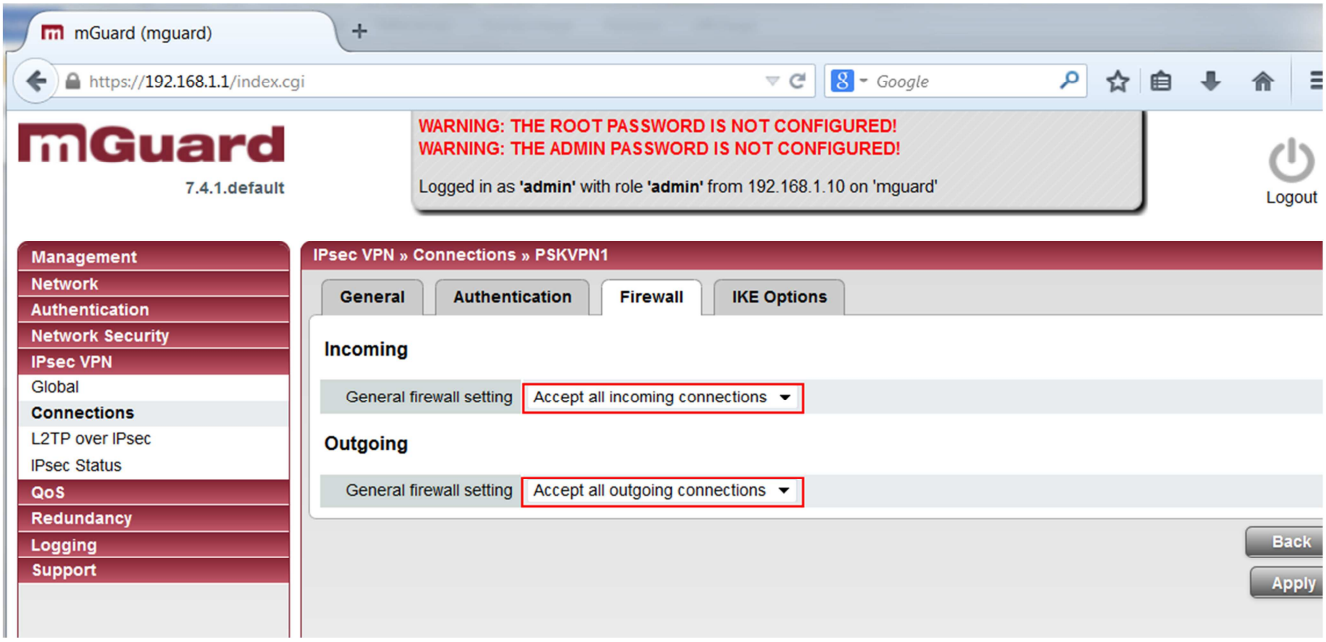




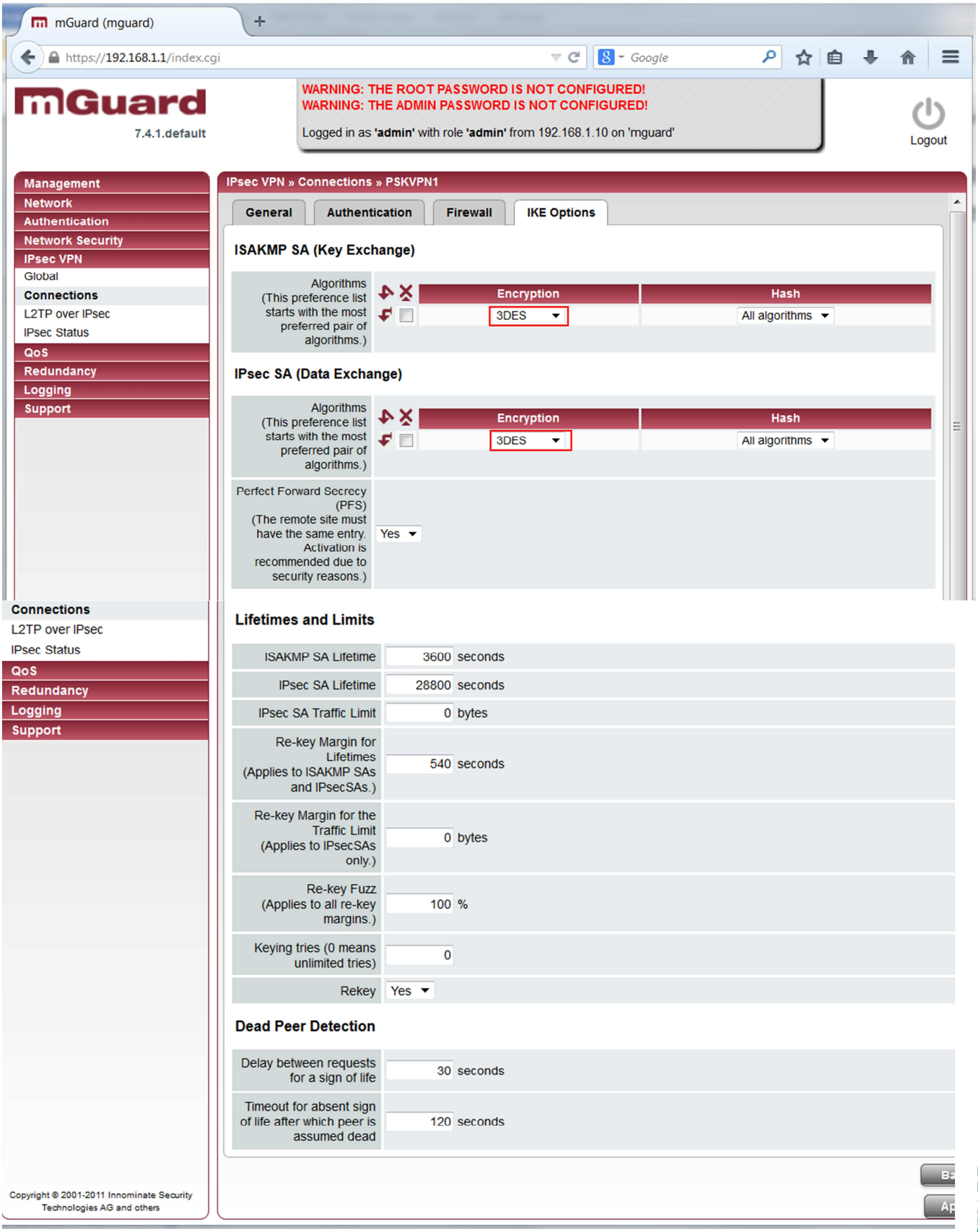
Dans l’onglet « Authentication » Sélectionner la méthode d’authentification par Pre-shared Secret Key.



Dans l’onglet « Firewall » autorisez toutes les connections entrantes et sortantes.

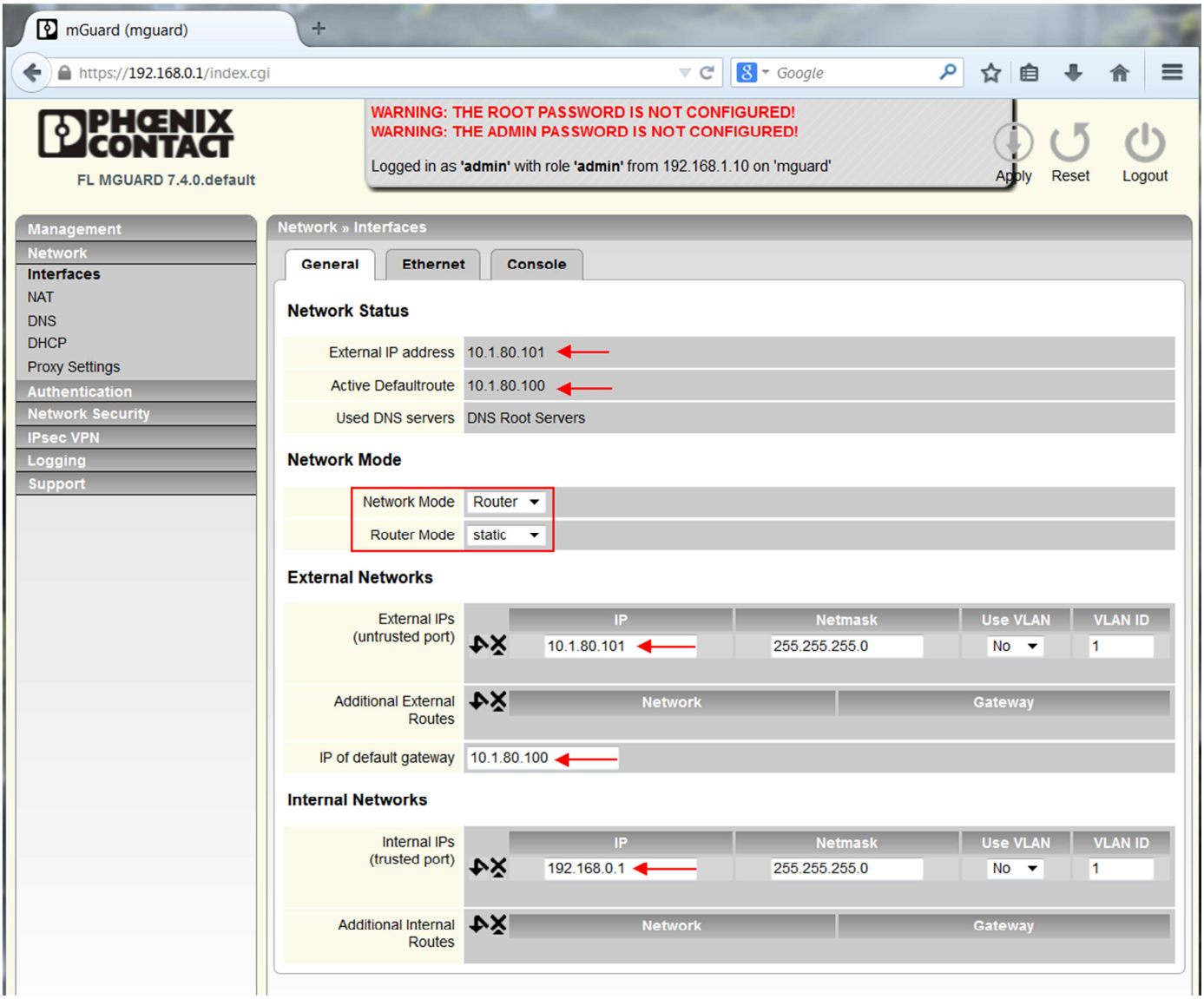


Dans l’onglet « IKE Options » préférez l’encryptage « 3DES ».

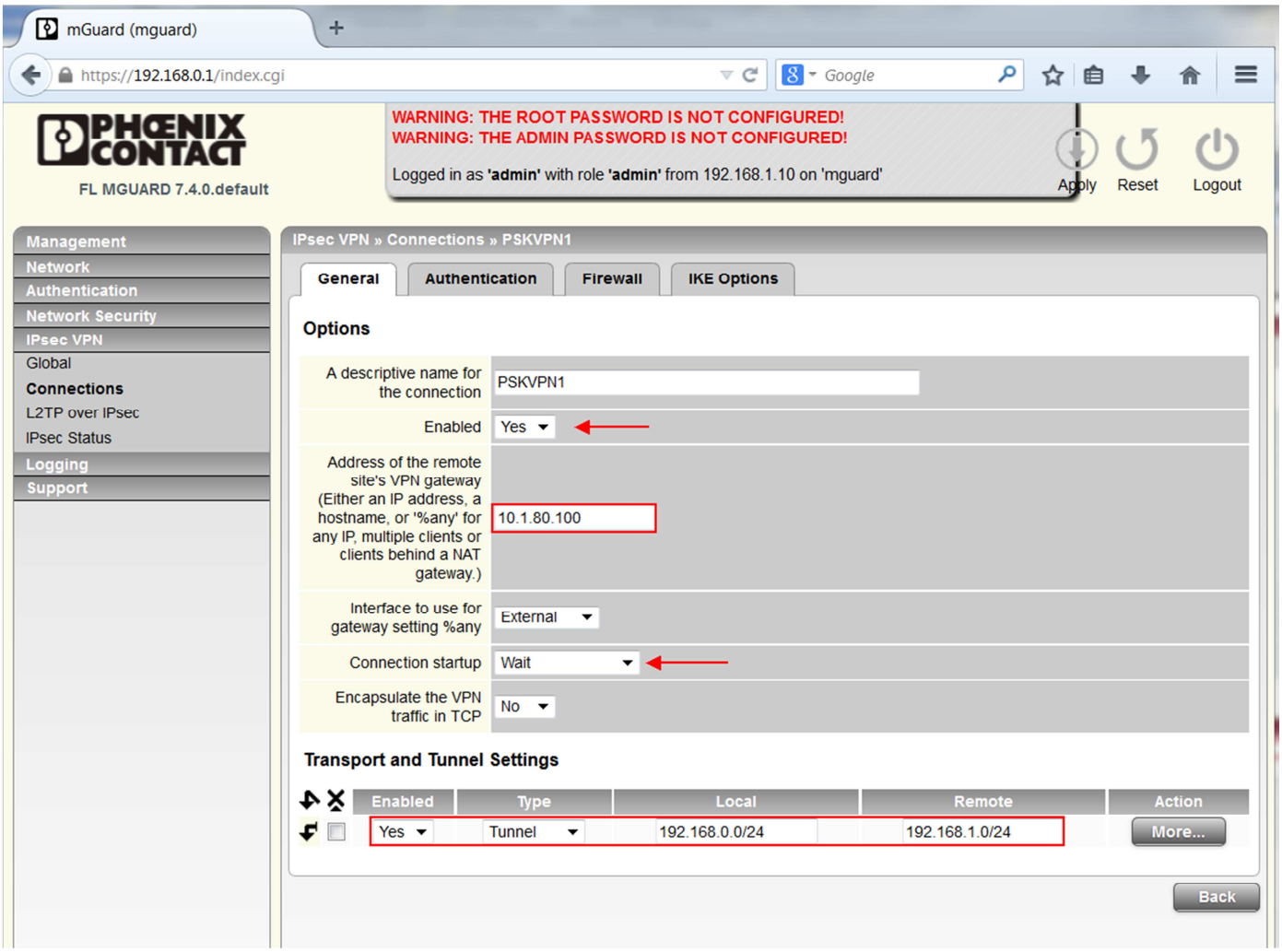


Configuration du MGUARD RS2000 VPN

Tous les paramètres sont identiques à l'exception des menus impliquant les adresses IP comme suit :



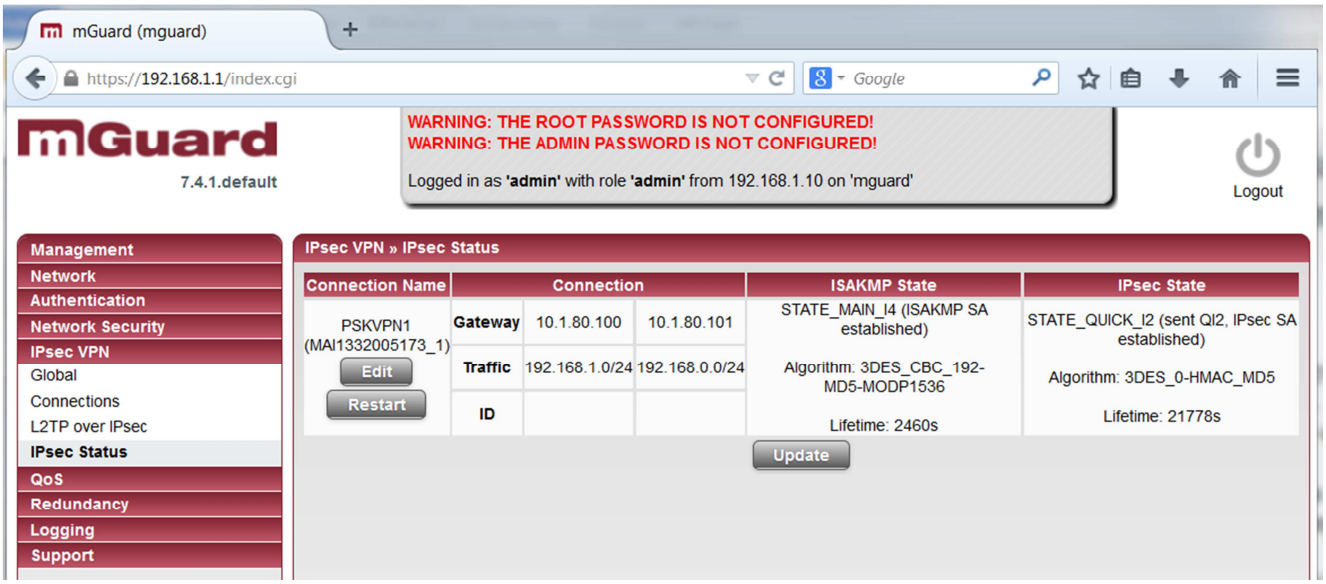
Concernant le MGUARD en attente, spécifiquement en PSK, il faut absolument préciser l'adresse IP du site initiateur distant sans utiliser le sigle %any.

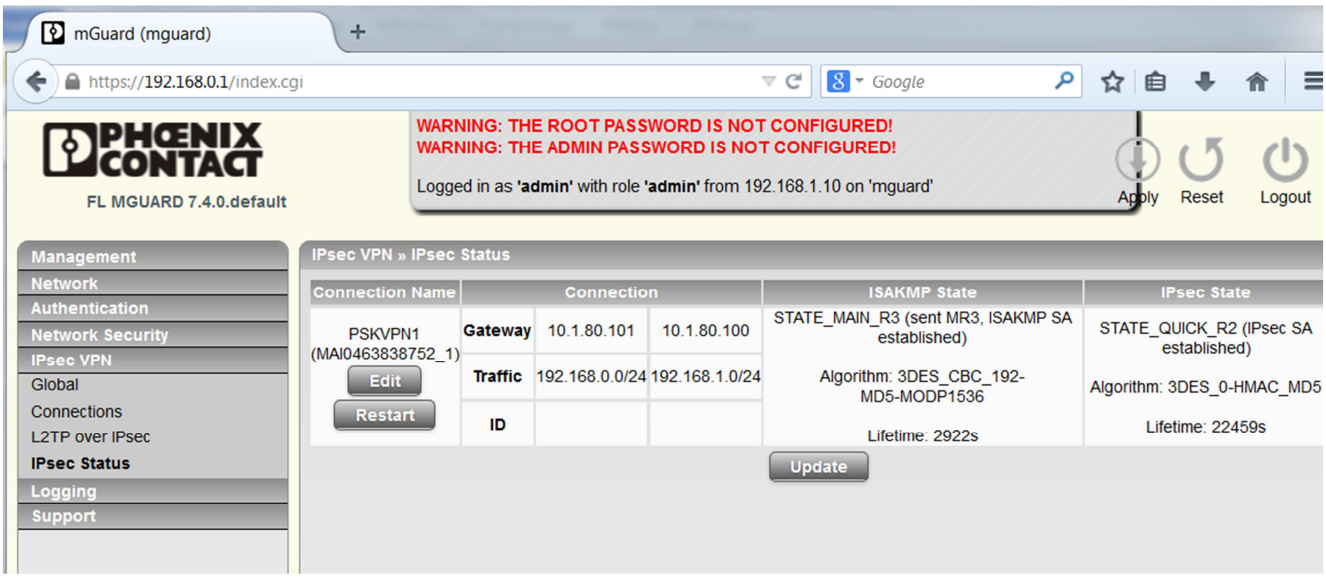


Mise en service de la communication

Dans le cas où vous êtes connectés au réseau d'entreprise via des « Proxys » il vous faudra ajouter au moins une route car le système ne sait gérer qu'une passerelle.
Dans la fenêtre « Invite de commandes » utilisez la commande « route » comme suit :
C:\route add 192.168.0.0 mask 255.255.255.0 192.168.1.1 metric 3
Il faut alors enlever la passerelle d'adresse 192.168.1.1 dans l'IPV4 de la carte réseau afin de garder toutes les fonctionnalités d'accès à l'extérieur via le réseau d'entreprise.

Une fois la commande acceptée l'on peut observer les Statuts VPN depuis le menu « IPSec VPN/IPSec Status » des deux MGUARD :



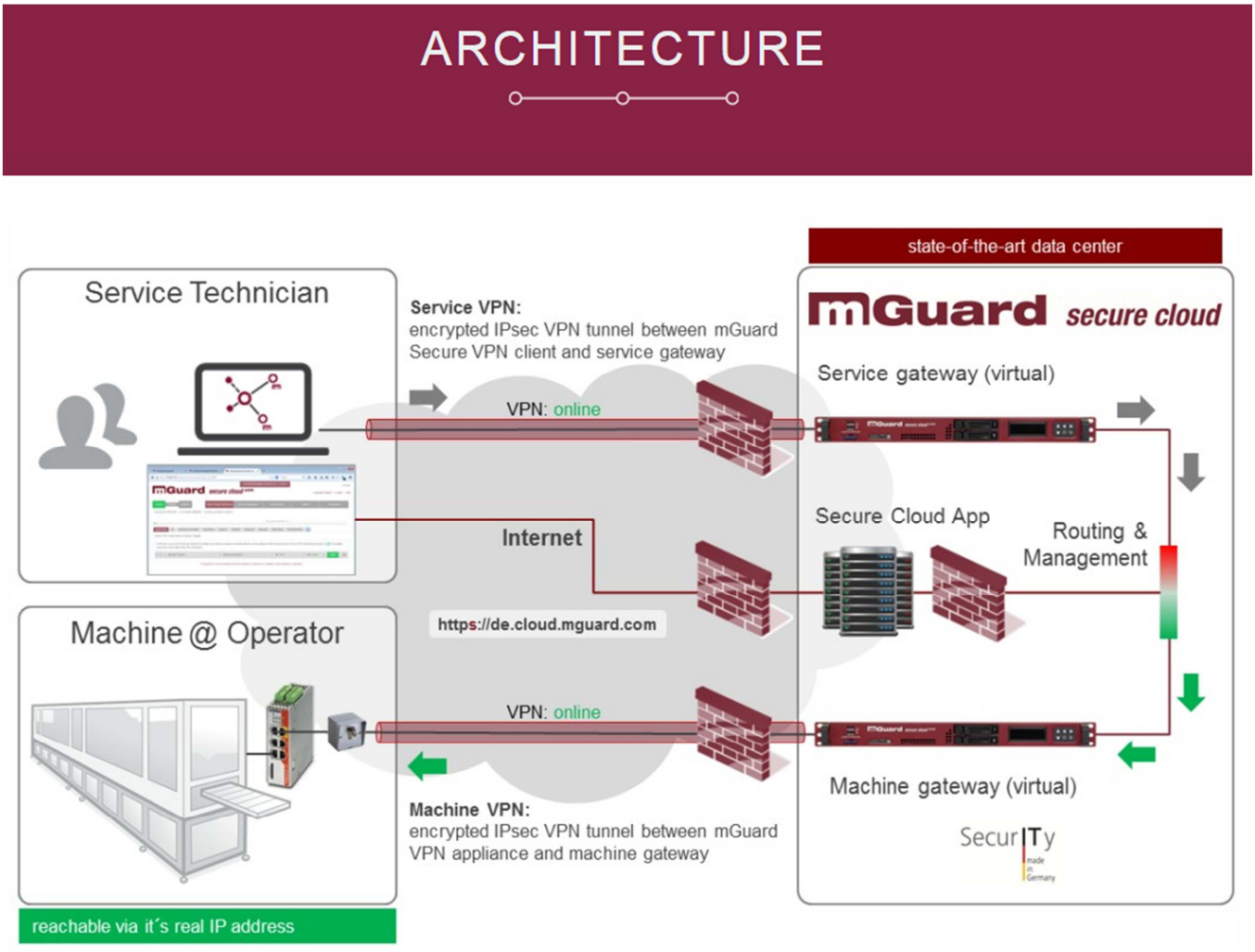


MGUARD Secure Cloud

Une autre solution consiste à utiliser en tant qu'assistance à la mise en service de la communication, le Cloud d'innominate.

C'est un portail qui permet de configurer une communication distante simplement avec un niveau de sécurité optimal.

L'architecture implique des connections sortantes depuis la station de travail ainsi que des machines distantes, ce qui facilite la gestion des différentes politiques de sécurité.
Le schéma ci-dessous illustre bien ce fait :



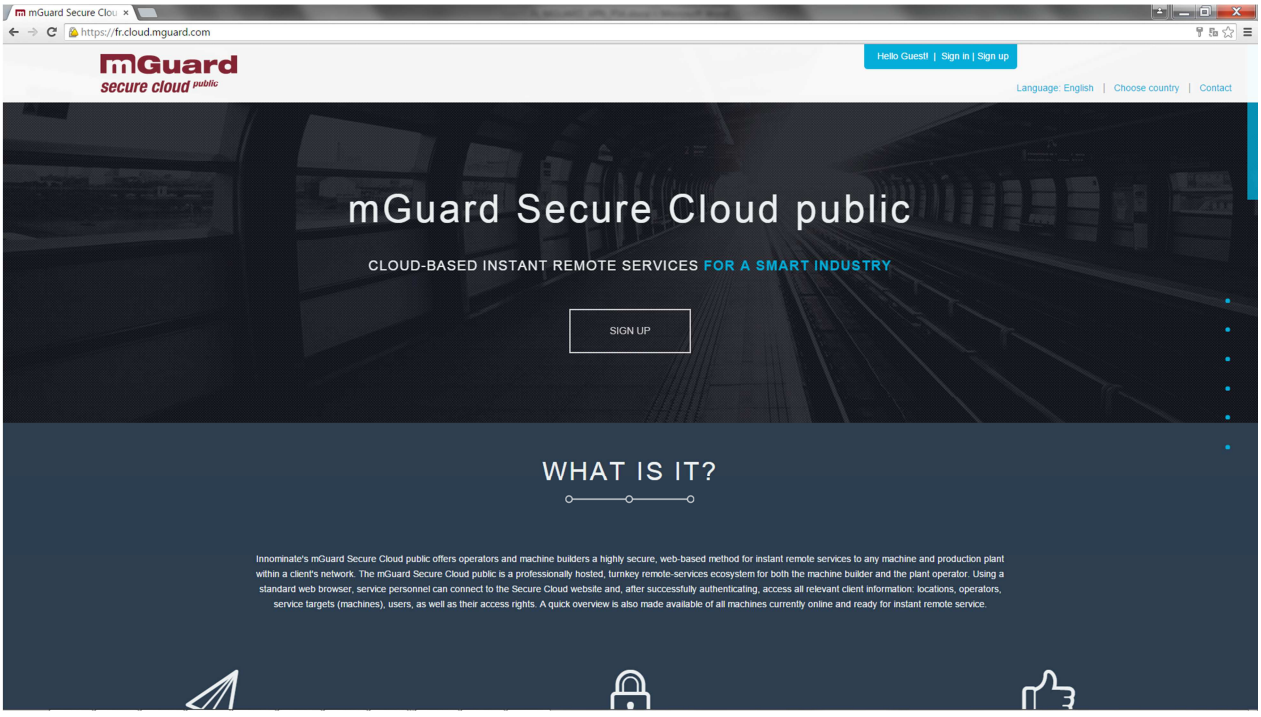
Le portail fournit aux tenants et aboutissants les fichiers de configuration des tunnels IPsec VPN avec certificats, ce qui évite toute programmation. Une fois les connections sortantes validées il suffit depuis le portail d'assurer la jonction.

Trois formules sont disponibles permettant une prise en main progressive et adaptée aux différentes applications :

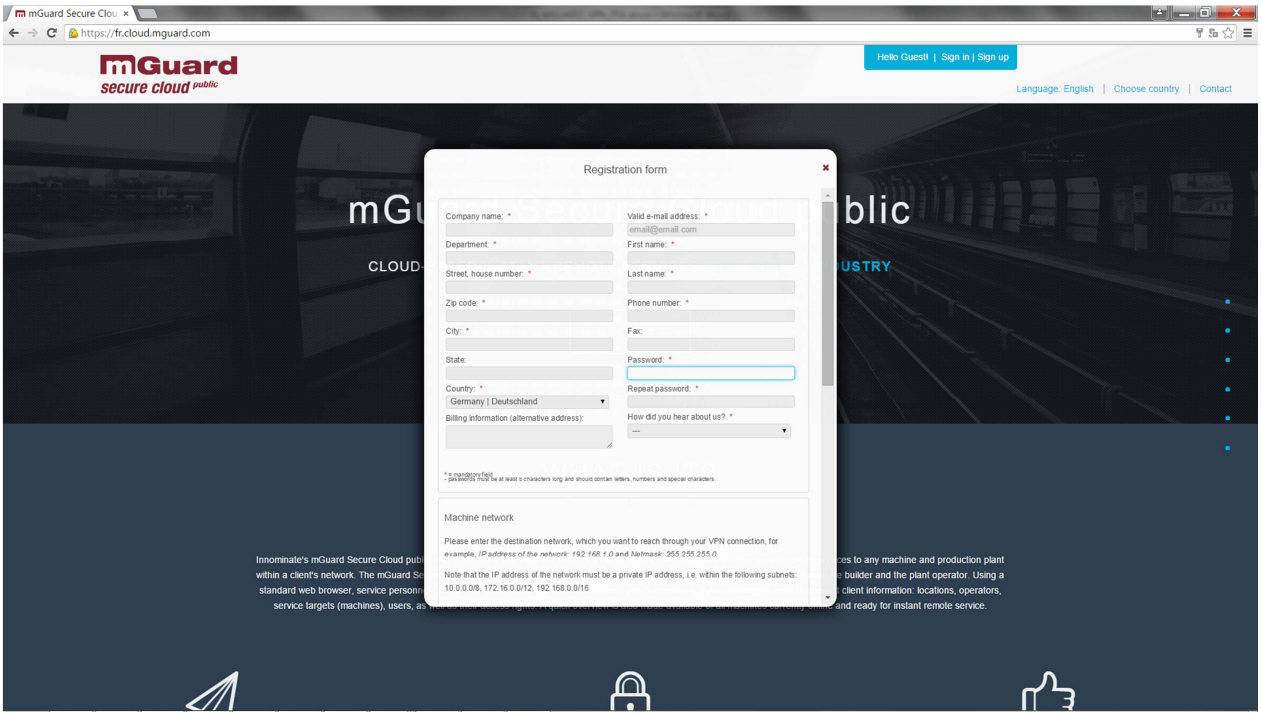
EDITIONS DISPONIBLES

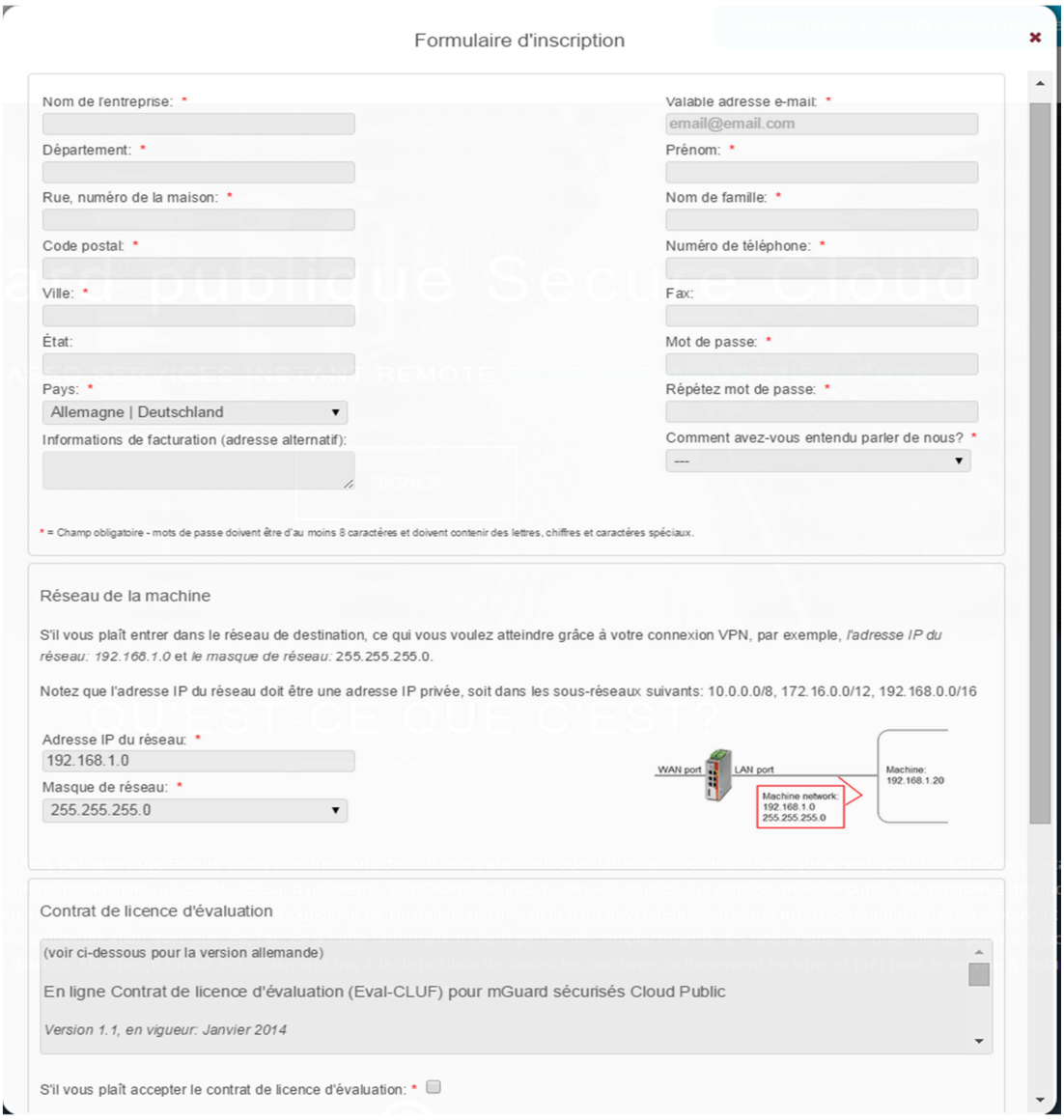
EVAL 30 jours gratuitement	BASE gratuit	PREMIUM Payant
SPÉCIFICATIONS:	**SPÉCIFICATIONS:**	**SPÉCIFICATIONS:**
Nombre d'utilisateurs: illimité	Nombre d'utilisateurs: illimité	Nombre d'utilisateurs: illimité
Nombre de machines: 1	Nombre de machines: Illimité	Nombre de machines: dépendante licence
Nombre de séances d'utilisateurs simultanés: 1	Nombre de séances d'utilisateurs simultanés: 1	Nombre de séances d'utilisateurs simultanés: 1
Bande passante par connexion de service garanti: Non	Bande passante par connexion de service garanti: Non	Bande passante garantie par raccordement au service:
Garantie de disponibilité: Non	Garantie de disponibilité: Non	Disponibilité garantie: 98% 1 Mbit / s
Volume de transfert par raccordement au service: 1 Go / mois	Volume de transfert par raccordement au service: 1 Go / mois	Volume de transfert par raccordement au service: illimité
Niveau Hébergement: Mission critique	Niveau Hébergement: Faible	Niveau Hébergement: Mission critique
Service de clients VPN: mGuards, logiciel IPsec	Service de clients VPN: mGuards, logiciel IPsec	Service de clients VPN: mGuards, logiciel IPsec
Clients VPN machine: mGuards	Clients VPN machine: mGuards	Clients VPN machine: mGuards
Hotline: téléphone, e-mail	Hotline: e-mail	Hotline: téléphone, e-mail
CARACTÉRISTIQUES	**CARACTÉRISTIQUES**	**CARACTÉRISTIQUES**
Modèle d'autorisation: Enhanced	Modèle d'autorisation: standard	Modèle d'autorisation: Enhanced
Reporting: Oui	Reporting: Oui	Reporting: Oui
Signaler filtrage: Oui	Signaler filtrage: Non	Signaler filtrage: Oui
Rapport exportation: Oui (CSV, XLS, PDF)	Exporter le rapport: Non	Rapport exportation: Oui (CSV, XLS, PDF)

Ce portail est accessible en renseignant suivant la zone géographique dans votre navigateur internet l'adresse suivante (cas de la France) : [https://**fr**.cloud.mguard.com/](https://fr.cloud.mguard.com/)
Nous recommandons l'utilisation de Firefox (V17.0 ou plus), Google Chrome (V28.0 ou plus), Apple Safari (V5.1.7 ou plus) voire Internet Explorer 10 minimum.

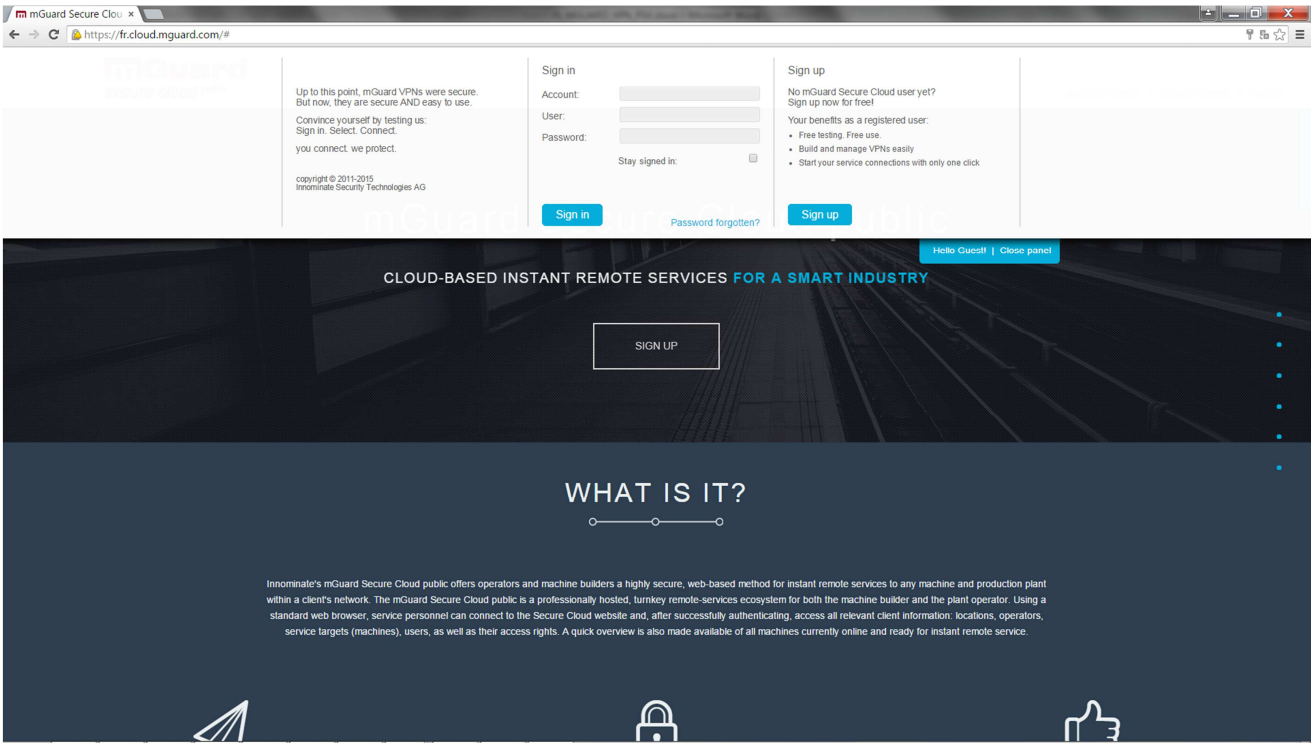


Dans un premier temps et afin de bénéficier de l'offre gratuite valable pendant 30 jours il est nécessaire de remplir un formulaire en cliquant sur la zone « SIGNER » :



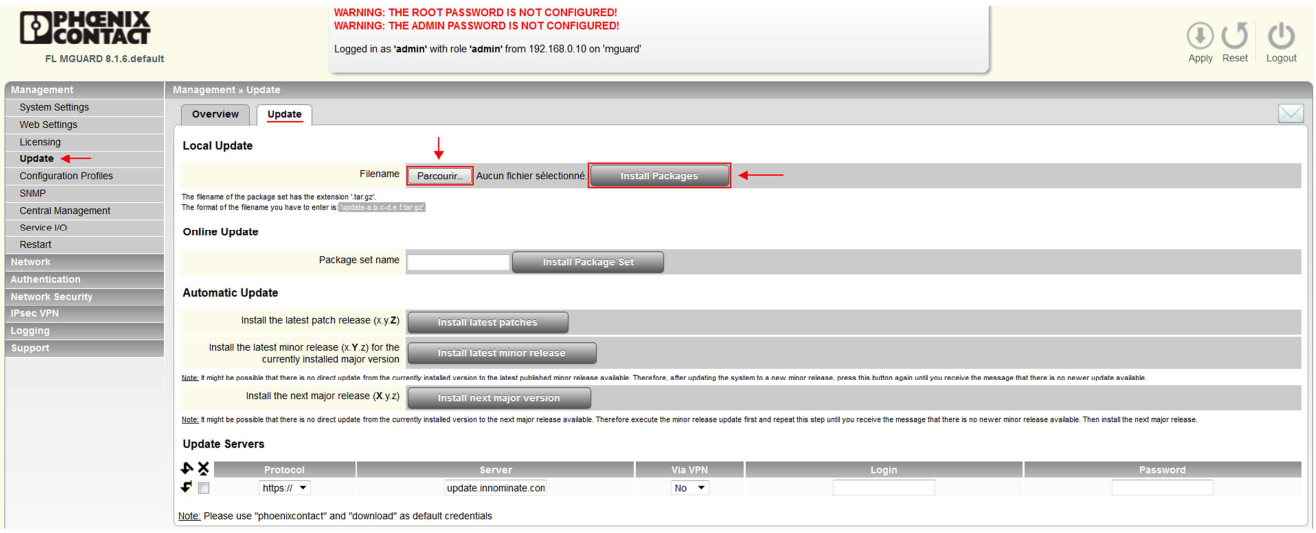


Une fois ce formulaire renseigné vous devrez confirmer par réponse à un mail reçu les clauses du contrat afin de transformer la formule « EVAL » en une formule « BASE » ou « PREMIUM ».
Enfin pour vous connecter à votre compte il vous faudra renseigner les paramètres « Compte », « Utilisateur » et « mot de passe » fournis dans le mail de confirmation.



Notez que tous les équipements mGuard connectés au portail doivent impérativement avoir la version Firmware 7.5 minimum.

La Mise à jour du Firmware est téléchargeable sur notre site https://www.phoenixcontact.com/online/portal/fr dans l'onglet « Téléchargements » du produit concerné. C'est un fichier compressé de type « update-a.b.c-d.e.f.tar.gz ».
Dans le mGuard aller dans le menu « Management/Update » comme suit :



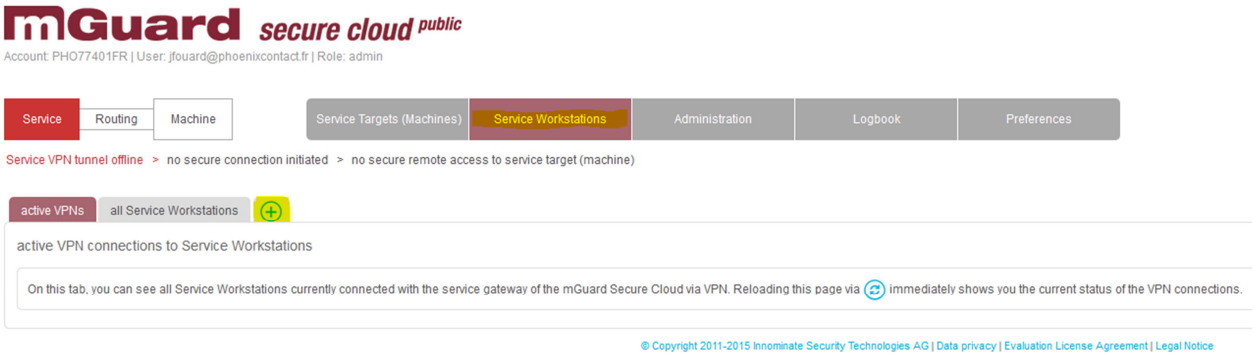
Dans « Local Update » appuyer sur « Parcourir » et sélectionner le fichier « update-a.b.c-d.e.f.tar.gz » puis « Install Packages ».

A la première connexion au portail vous obtenez :

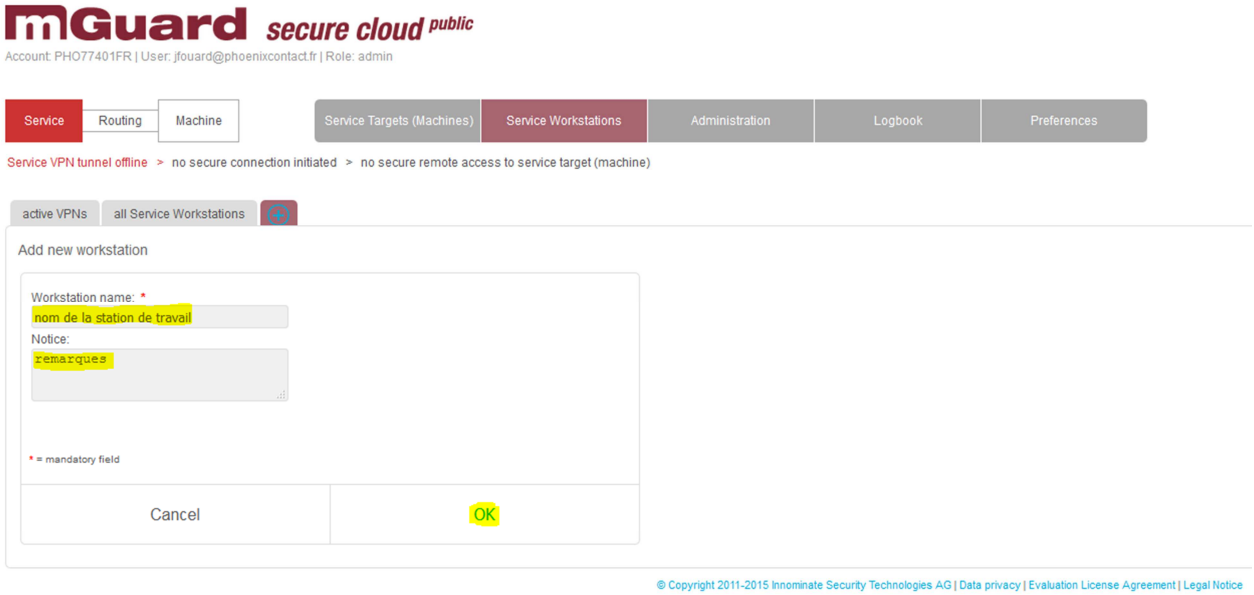
Les services principaux sont présentés en deux parties :

- Station de travail
- Machines

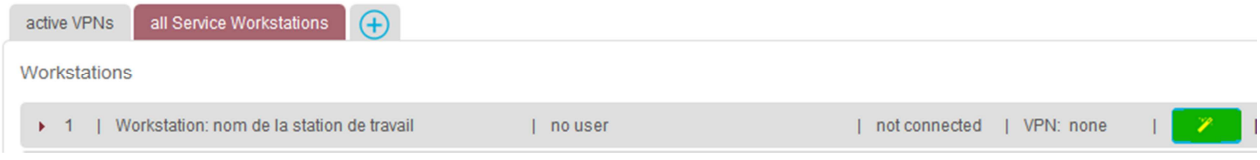
Il est préférable de commencer par la station de travail comme suit :



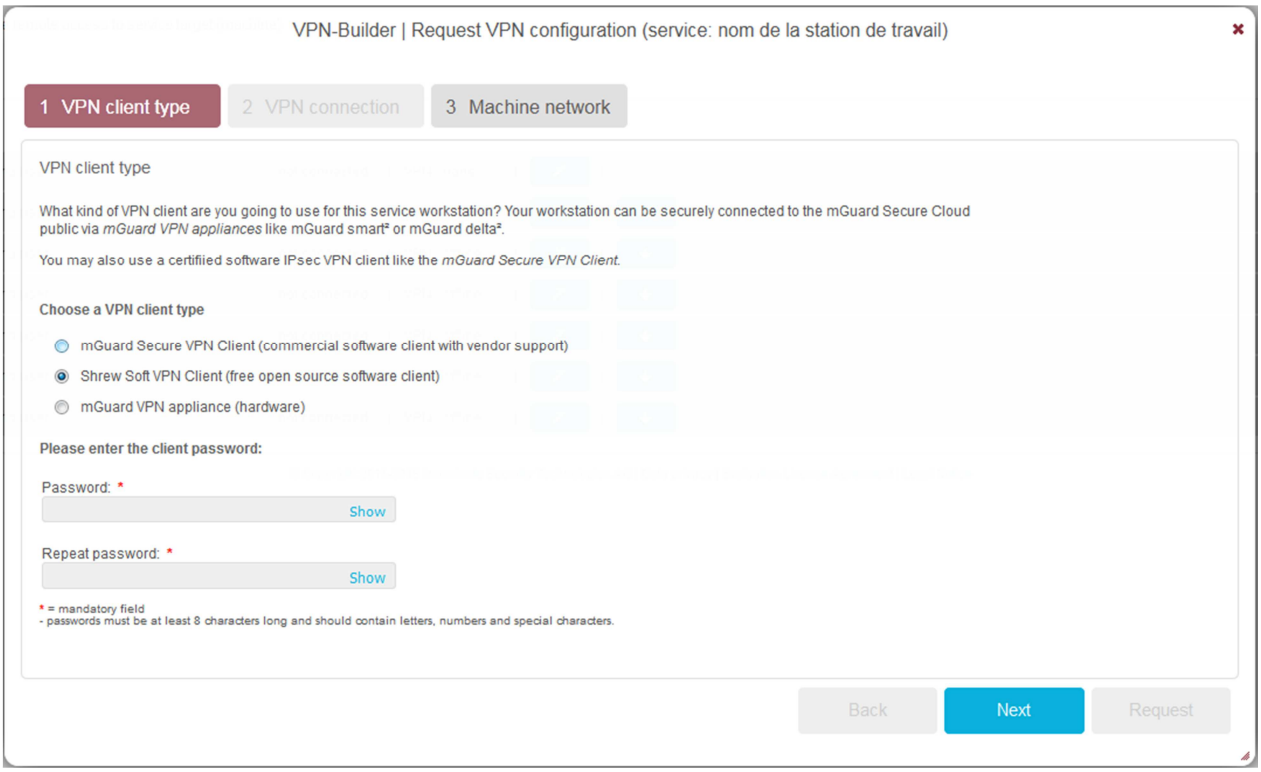
Sélectionner l'onglet marqué d'un « + » pour ajouter une nouvelle station de travail :



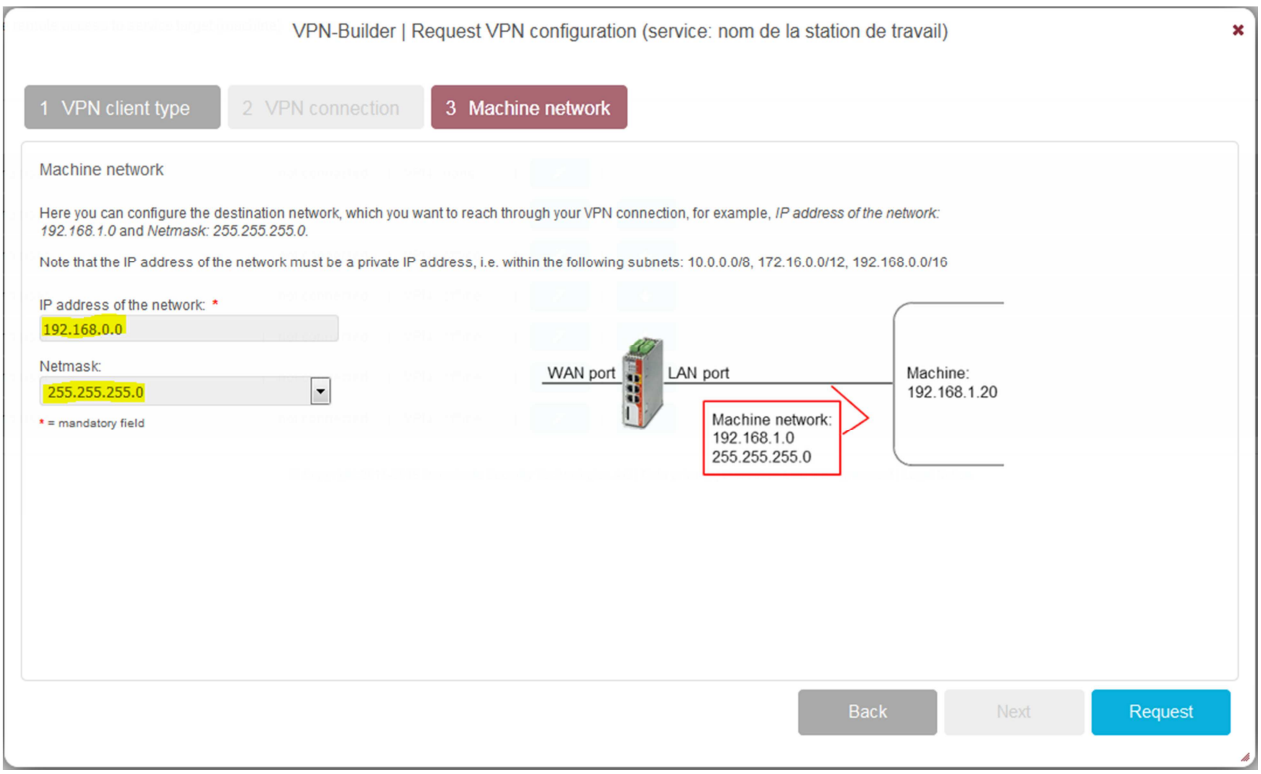
Après avoir renseigné le nom et d'éventuelles remarques et validé, vous ajoutez à la liste existante une nouvelle station que vous pourrez paramétrer par l'appui sur l'icône stylet :



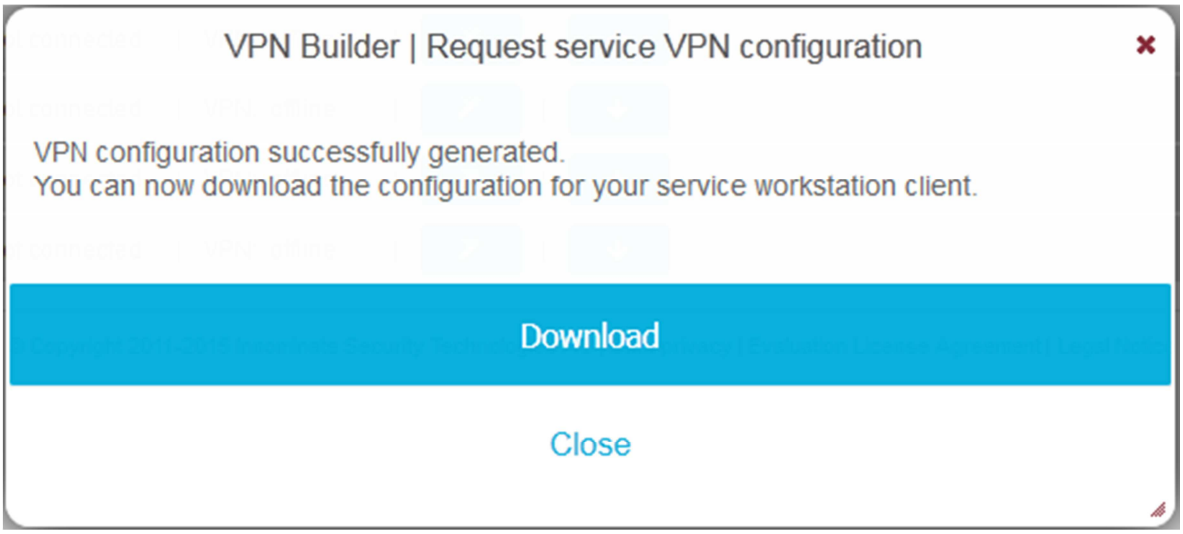
Vous obtenez alors la feuille de renseignement présentant les trois types de clients VPN possibles :



Après avoir obligatoirement renseigné le mot de passe si le choix s'est porté par exemple sur un client VPN logiciel :

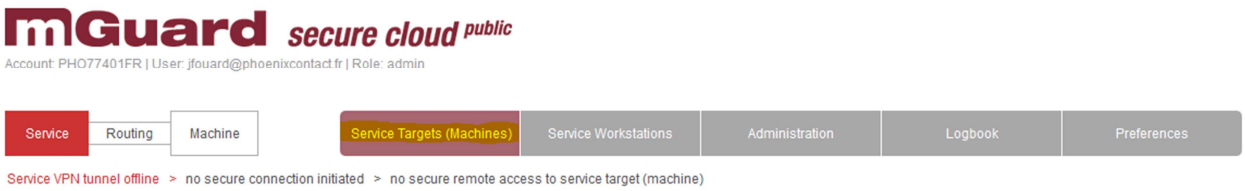


L'appui sur la touche « Request » permet de télécharger le fichier de configuration pour le VPN client Shrewsoft dans notre exemple.

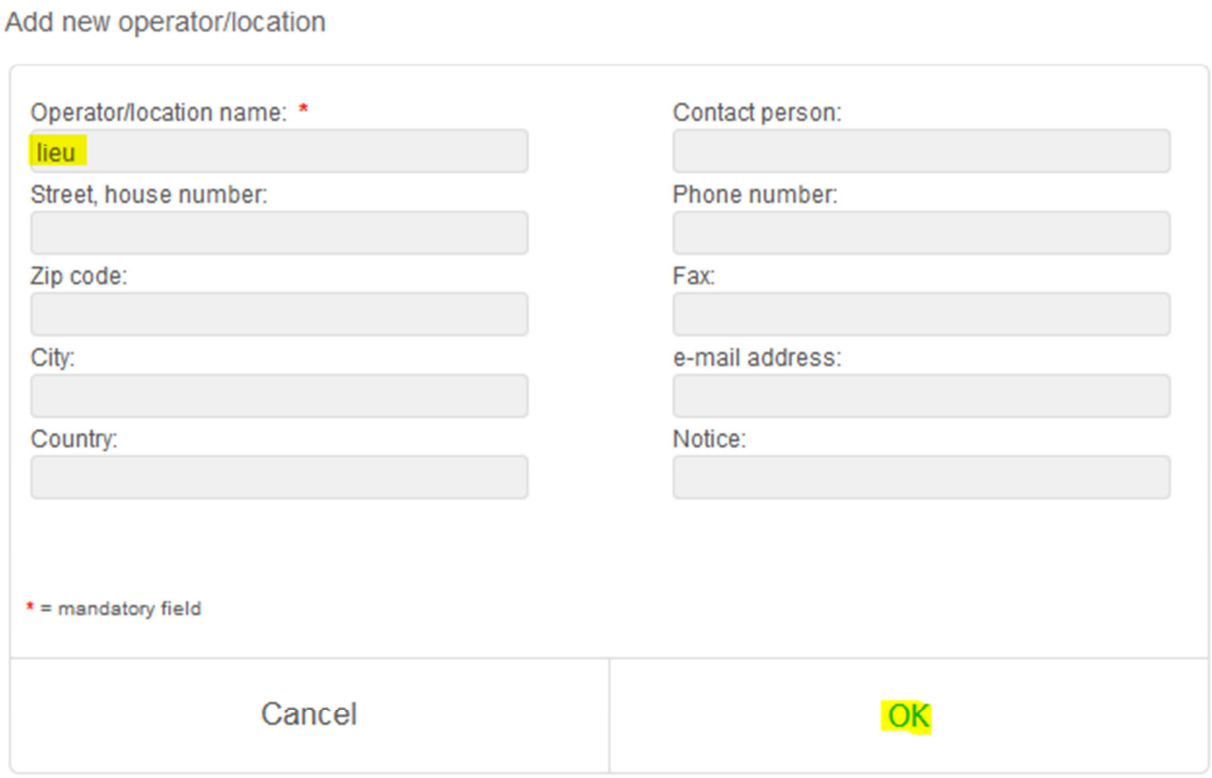


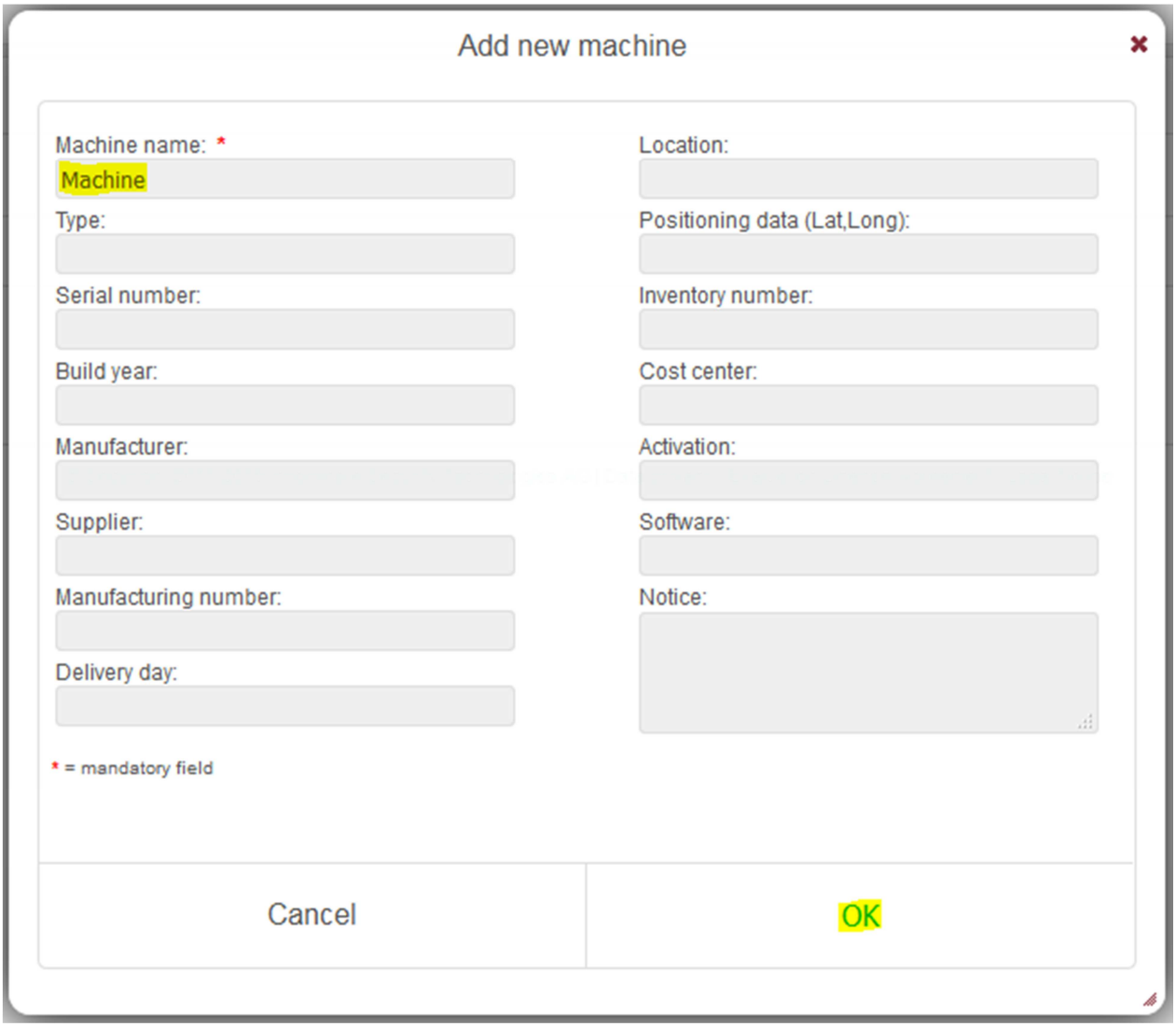
Vous obtenez un fichier de type *.vpn exploitable via le logiciel VPN client Shrewsoft en renseignant le mot de passe choisi.

Vous pouvez maintenant passer à l'étape suivante en sélectionnant la cible « Machines » :

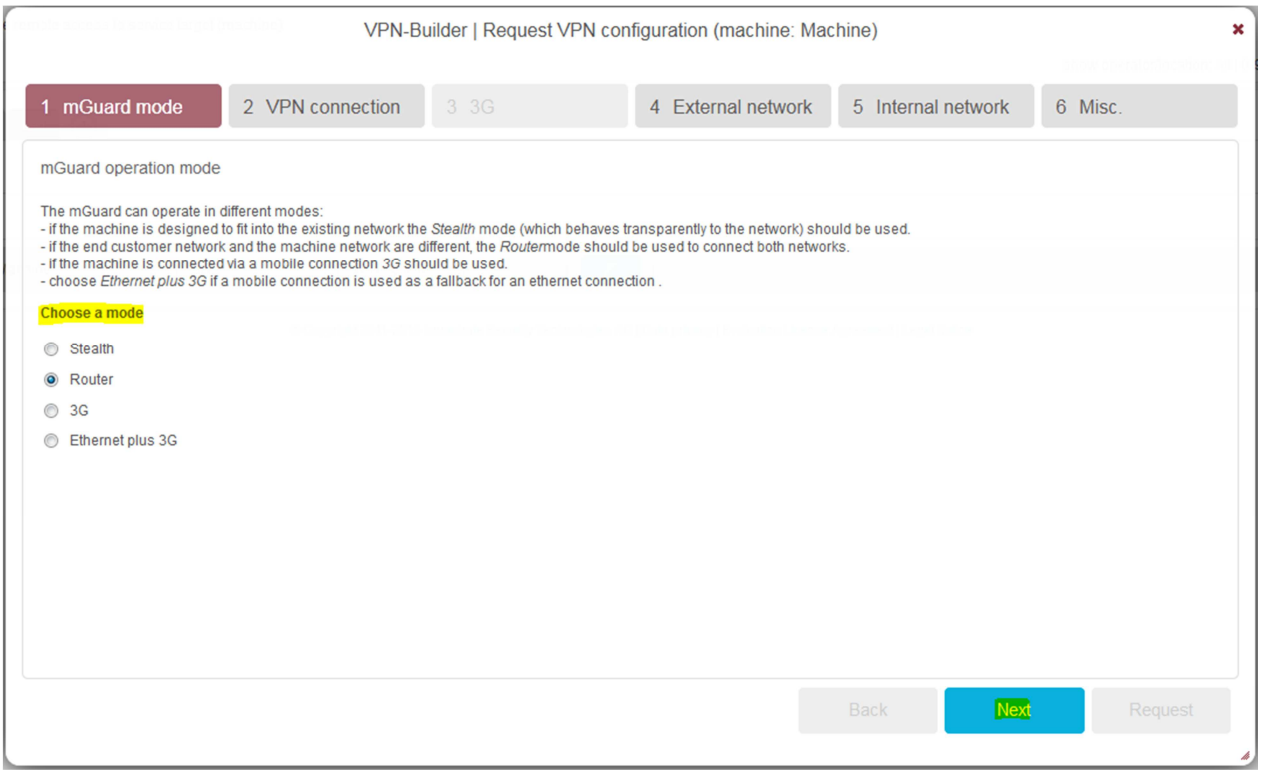


Sélectionner l'onglet marqué d'un « + » pour ajouter une nouvelle Machine, opération qui se fait en deux temps, « Lieu » et « Machine » :

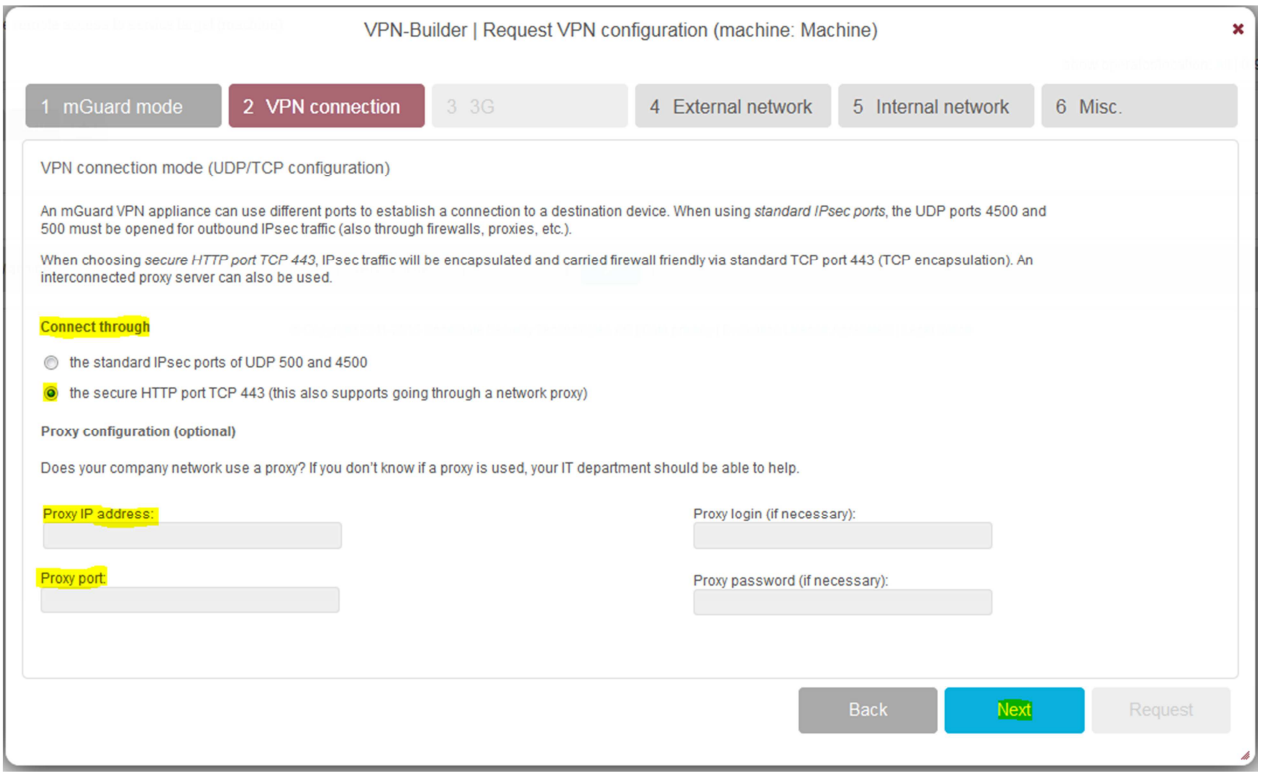




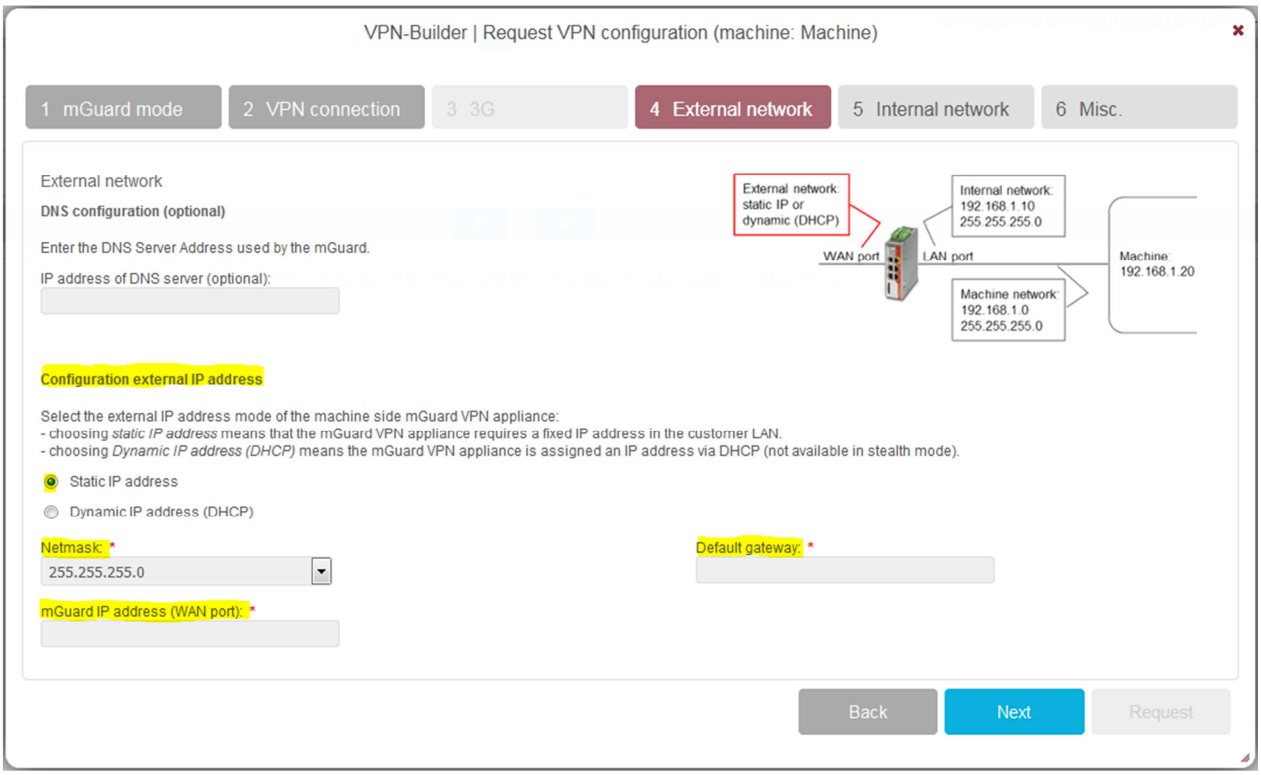
Vous ajoutez à la liste existante une nouvelle machine que vous pourrez paramétrer par l'appui sur l'icône stylet :

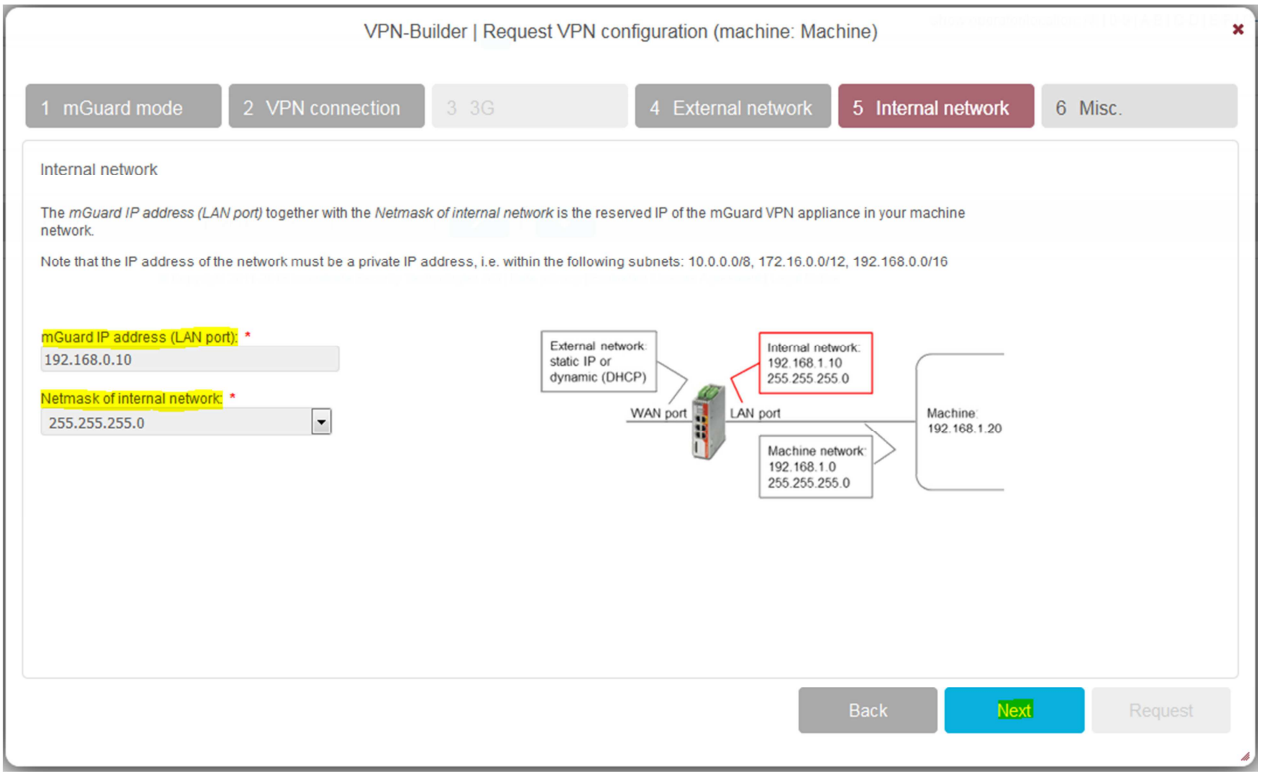


Différentes étapes permettent de renseigner les caractéristiques principales de fonctionnement du mGuard afin de télécharger son fichier de configuration.

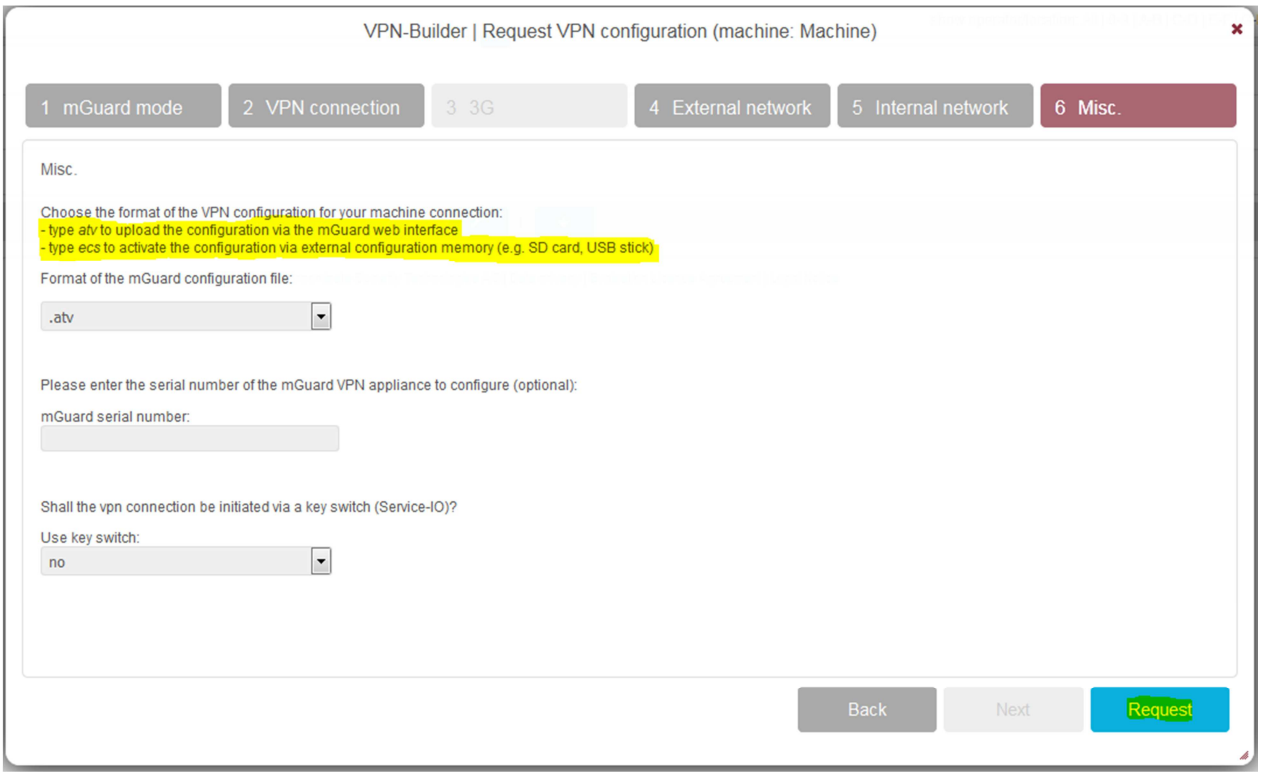


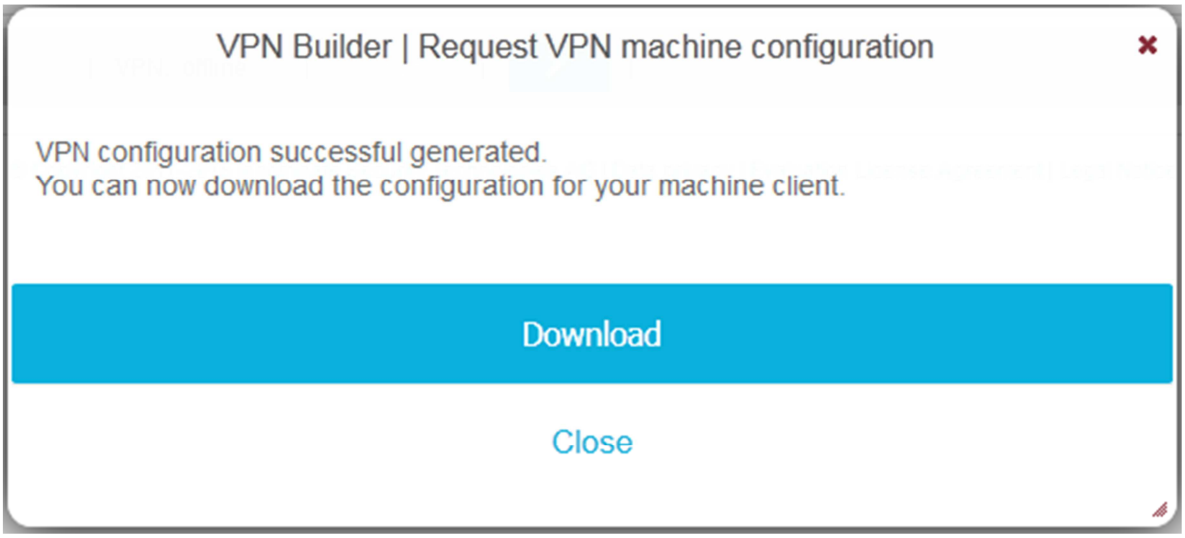
La connexion VPN offre le choix d'utiliser les ports standards IPsec (500 et 4500) ou des ports sécurisés notamment en présence de serveurs proxys. Dans ce cas il sera nécessaire de renseigner au minimum l'adresse IP ainsi que le port du proxy.





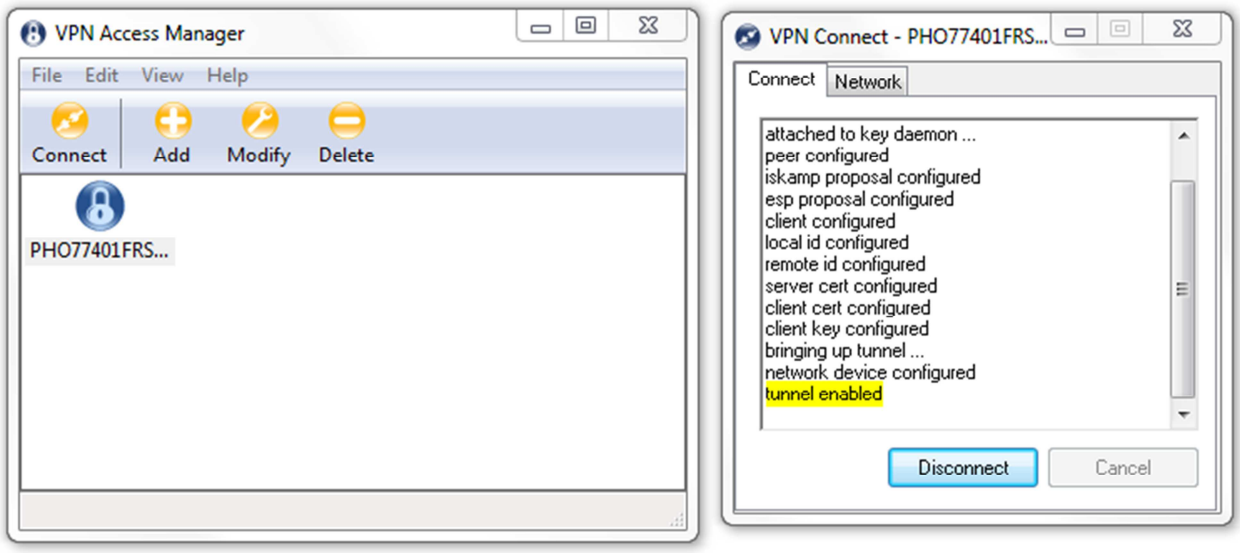
Une fois les paramètres du réseau externe comme du réseau interne renseignés, il est demandé de préciser l'extension du fichier de configuration pour cibler soit directement le mGuard soit une carte SD enfichable ultérieurement dans le routeur :





Vous obtenez un fichier de type *.atv téléchargeable directement dans le mGuard ou de type *.ecs téléchargeable dans une carte SD qui sera ensuite enfichée dans le mGuard.

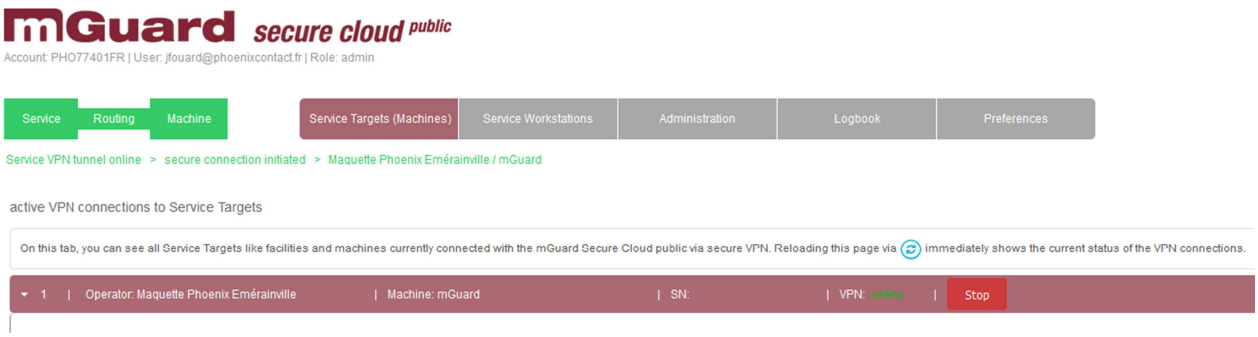
Vous pouvez maintenant passer à l'étape suivante en activant le tunnel VPN depuis le logiciel Shrewsoft avec le fichier téléchargé :



Quand le tunnel VPN entre la stationde travail et le cloud vous obtenez :

Appuyer alors sur la touche « Start » pour finaliser la connexion entre la station de travail et la machine sélectionnées.

Vous obtenez alors le visuel « Service/Routing/Machine » totalement vert qui confirme la réunion des deux connexions sortantes :



Vous pouvez alors à tout moment décider de gérer comme bon vous semble la liaison VPN.