Accès externes pour un tiers

But de l'instruction :

Le but de cette instruction est de détailler les modalités de mise en œuvre d'un accès externe au réseau informatique de l'IFP pour une entité tierce.

Champ d'application :

Filiales, Partenaires, Fournisseurs, Mainteneurs

Objet de la révision :

Création du document

Rédaction nom / visa	Vérification nom / visa	Approbation nom / visa
date : 22/12/09 Thierry Bôle	date : 22/12/09 Myriam Viretto Elisabeth Merlen Christophe Favre	date d'application : 29/12/09 Bruno Bordet

SOMMAIRE

A Demande initiale

1 Étude de la faisabilité sur la mise en place d'un accès

Dans tous les cas, un échange préalable est nécessaire pour bien identifier avec le demandeur (en relation éventuellement avec la société tierce) ses besoins et pour vérifier si la mise en place d'un accès externe est pertinent, viable et s'il répond aux exigences de sécurité IFP décrites dans ce document.

Il est indispensable que la mise en place de l'accès externe s'accompagne d'une maquette et d'une validation entre les 2 parties avant sa mise en production pour bien s'assurer de la bonne adéquation entre les besoins du demandeur avec la solution mise en place.

2 Formalisation du besoin

Lorsqu'un besoin est identifié et nécessite la mise en place d'un accès externe pour un tiers, une demande officielle doit être adressée à la DSIT (équipe IFP-Sécurité). Cette demande précisera les informations suivantes :

- nom de la société tierce ou de la filiale ;
- nature des données à échanger, à accéder, volumétrie estimée et leur niveau de confidentialité (le nom du propriétaire des données le cas échéant) ;
- nature de l'accès (permanent, temporaire) et sa durée (date de fin du contrat) ;
- criticité de l'accès (en terme de disponibilité) ;
- référence du contrat liant l'IFP avec ce tiers et engagements de confidentialité existants ;
- délai souhaité de mise en œuvre de l'accès ;
- contact IFP et contact dans la société tierce ;
- toutes informations et documents complémentaires utiles.

3 Validation de la demande

Seules les personnes suivantes sont habilitées à solliciter un accès externe pour un tiers :

- le responsable d'application (après la validation du correspondant d'application) s'il s'agit de l'accès d'un tiers à une application dans le cadre d'un contrat de TMA;
- le responsable du projet s'il s'agit d'une interconnexion mise en œuvre dans le cadre d'un projet ;
- le directeur de la DSIT dans le cadre d'un contrat d'administration et de développement à distance;
- toute personne IFP avec validation par son directeur (dans le cadre d'un contrat de maintenance à distance).

Cette demande devra être adressée à la DSIT (équipe IFP-Sécurité) qui instruira la demande en relation avec le service Architecture. Cette demande pourra être traitée soit dans le cadre d'une évolution mineure soit dans le cadre du récurrent en fonction de l'impact et la charge induite.

S'il s'agit d'un accès permanent avec des flux entrants directement dans le système d'information IFP (sans poste de rebond), une validation supplémentaire du RSSI sera nécessaire.

B Mise en œuvre

Les accès les plus couramment mis en œuvre le sont :

- dans le cadre d'un contrat de maintenance (Tierce Maintenance Applicative ou mainteneur d'un logiciel, d'un matériel) ;
- dans le cadre d'un contrat d'administration (infogérance..) ou d'une prestation de développement à distance ;
- dans le cadre d'échange de données ou d'accès à certaines ressources informatiques IFP (avec une filiale, un client un fournisseur ou un mainteneur).

Les conditions d'accès dans ces différentes situations sont décrites ci-après.

1 Pour un accès du type "Maintenance"

1.1 Exigences contractuelles

Le contrat établi avec le tiers doit spécifier les engagements attendus en terme de confidentialité sur les données accédées et échangées. Ceux-ci sont formalisés par la Direction Juridique et adaptés au cas par cas.

1.2 Visibilité "minimale"

Le moyen privilégié sera la solution VPN SSL permettant un accès sécurisé aux ressources informatiques IFP via l'URL https://webnet.ifp.fr/tma.

Le prestataire accédera ainsi directement aux machines nécessaires où il se connectera à un poste de rebond avec l'ensemble des outils dont il aura besoin.

Les ressources accédées en interne seront limitées au strict minimum (filtrage par adresse destinataire et par protocole).

Le compte créé et mis à disposition du tiers devra respecter les règles de gestion des comptes informatiques (cf. instruction F06-I12 : Règles de gestion des comptes informatiques de l'IFP) avec des restrictions notamment sur les ordinateurs permettant son utilisation et limités au périmètre d'intervention.

1.3 Modalités d'ouverture de l'accès

L'interconnexion mise en place sera par défaut à l'état "désactivé". Son ouverture pourra être sollicitée par le contact IFP indiqué lors de la demande de mise en place de l'accès.

La durée de l'ouverture de cet accès ne pourra excédée 2 jours.

Le délai de traitement pour l'ouverture de l'accès est le délai contractuel pour le traitement et la réalisation d'une demande standard adressée à l'assistance informatique. Celui-ci couramment constaté est de l'ordre de 4h maximum.

La sollicitation de l'ouverture de l'accès sera réalisée en adressant le message suivant à l'assistance informatique :

> Bonjour,
>
> Conformément au workflow défini avec IFP-Securité de la DSIT, je sollicite l'ouverture ponctuelle de l'accès pour la société xxxx.
>
> Cette demande n'est pas soumise à validation, elle sera traitée directement car elle a déjà été validée initialement (la règle est déjà présente mais à l'état désactivé).
>
> Cet accès sera valide pour la durée du **xx/xx/xxxx au xx/xx/xxxx** (cette durée ne pourra pas excéder 2 jours).
>
> Après le traitement de la demande, le ticket sera placé dans la file d'attente d'IFP-Sécurité qui en assurera le suivi et assurera la fermeture de l'accès.

1.4 Niveaux de service associés

La solution proposée du VPN SSL (via Internet) ne permet pas de garantir un niveau de bande passante ni un temps de latence minimum.
Cette solution ne pourra être validée par les 2 parties qu'après maquettage pour vérifier qu'elle réponde bien au besoin.

1.5 Fin de mise à disposition de l'accès

La durée de l'accès est strictement limitée à la durée du contrat et de la prestation.

2 Pour un accès dans le cadre d'un contrat d'administration ou de développement à distance

2.1 Exigences contractuelles

Le contrat établi avec le tiers doit spécifier les engagements attendus en terme de confidentialité sur les données accédées et échangées. Ceux-ci sont formalisés par la Direction Juridique et adaptés au cas par cas.

2.2 Visibilité "minimale"

L'accès au réseau IFP depuis le réseau du tiers se fera, de préférence, soit :

- via la solution VPN SSL permettant un accès sécurisé aux ressources informatiques IFP via l'URL https://webnet.ifp.fr/tma. Dans ce cas, les données restent présentes et hébergées sur des postes IFP ;

- via un canal sécurisé (VPN) transitant par Internet pour réduire les coûts tout en assurant un niveau de sécurité acceptable. Dans ce cas, les données sont échangées et accédées depuis les postes du prestataire ;

- via une ligne spécialisée et une interconnexion dédiée.

Les ressources accédées en interne seront limitées au strict minimum (filtrage par adresse destinataire et par protocole).

Le compte utilisé par le tiers pour se connecter sur les équipements IFP devra respecter les règles de gestion des comptes informatiques (cf. instruction F06-I12 : Règles de gestion des comptes informatiques de l'IFP) avec des restrictions notamment sur les ordinateurs permettant son utilisation et limités au périmètre d'intervention.

2.3 Niveaux de service associés

Les solutions proposées du VPN SSL et du tunnel VPN IPSEC (via Internet) ne permettent pas de garantir un niveau de bande passante ni un temps de latence minimum.

Celle impliquant la mise en place d'un tunnel VPN peut se retrouver vite pénalisante pour des volumes importants de données à échanger et/ou des applications interactives très sensibles à la latence.

Cette solution ne pourra être validée par les 2 parties qu'après maquettage pour vérifier qu'elle réponde bien au besoin.

2.4 Fin de mise à disposition de l'accès

La durée de l'accès dépend de la prestation assurée par le tiers et est limité à la durée du contrat .

3 Pour des échanges de données ou un accès aux ressources informatiques internes IFP (hors maintenance)

3.1 Exigences contractuelles

Le contrat établi avec le tiers doit spécifier les engagements attendus en terme de confidentialité sur les données accédées et échangées. Ceux-ci sont formalisés par la Direction Juridique et adaptés au cas par cas.

Dans le cas d'une filiale, il n'y aura pas d'exigence contractuelle.

3.2 Visibilité "minimale"

L'interconnexion pourra se faire soit:

- via un canal sécurisé (VPN) transitant par Internet pour réduire les coûts tout en assurant un niveau de sécurité acceptable. Dans ce cas, les données sont échangées et accédées depuis les postes de l'entité tierce ;

- via une ligne spécialisée et une interconnexion dédiée.

Le compte utilisé par le tiers pour se connecter sur les équipements IFP devra respecter les règles de gestion informatiques (cf. instruction F06-I12 : Règles de gestion des comptes informatiques de l'IFP) avec des restrictions notamment sur les ordinateurs permettant son utilisation.

3.3 Niveaux de service associés

La solution du tunnel VPN via Internet ne permet pas de garantir un niveau de bande passante ni un temps de latence minimum. Elle peut se retrouver vite pénalisante pour des volumes importants de données à échanger et/ou des applications interactives très sensibles à la latence.

La solution retenue ne pourra être validée par les 2 parties qu'après maquettage.

3.4 Fin de mise à disposition de l'accès

La durée de l'accès est liée à la durée du besoin.

C Vérification/ Audit

Il est indispensable d'effectuer une revue annuelle des accès externes mis en œuvre pour des tiers et de s'assurer de leur utilité et que le contrat liant l'IFP à ce tiers est toujours en vigueur. Cette revue est effectué par IFP-Sécurité.

Il est aussi important de vérifier que les accès pour un contrat de type "Maintenance "sont bien mis à l'état désactivé par défaut.