RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

# Services canadiens d'identification criminelle en temps réel

## Lignes directrices techniques sur l'ITR à l'intention des organismes

| | |
|---|---|
| **Date :** | 10-02-2015 |
| **État :** | Final |
| **Version :** | 3.0 |
| **Classification :** | Non classifié |
| **Propriétaire :** | Solutions biométriques d'entreprise |
| **SGDDI :** | 19086 |

## REGISTRE DES MODIFICATIONS

| Nº de version | Date | Commentaires |
|---|---|---|
| 1.1 | 02-11-2005 | Ébauche initiale |
| 1.2 | 07-11-2005 | Modification visant à inclure les commentaires de l'équipe d'engagement envers les clients. |
| 1.3 | 18-11-2005 | Modifications visant à inclure les commentaires du rédacteur technique. |
| 1.4 | 20-06-2006 | Modifications relatives aux « exigences techniques de la phase 1 du projet d'ITR ». |
| 1.5 | 23-07-2006 | Révision du rédacteur technique du CCC. |
| 1.6 | 10-08-2006 | Révision de l'équipe du CCC. |
| 1.7 | 20-08-2006 | Révision du rédacteur technique du CCC. |
| 1.8 | 29-08-2006 | Révision du rédacteur technique du CCC. |
| 1.9 | 25-10-2006 | Révision du rédacteur technique du CCC.<br>Diffusion du document auprès des ressources en matière d'ITR.<br>Intégration des changements proposés à la version définitive. |
| 2.0 | 29-05-2008 | Ajout de l'information détaillée sur les connexions<br>de client à système au Réseau de la VCP. |
| 2.1 | 22-01-2009 | Mise à jour des sections sur les exigences fédérales et le CIPC. |
| 2.2 | 15-05-2009 | Remplacement du terme « SPOI » (point d'interface unique) par « PAU » (point d'accès unique). |

## ORIGINE ET APPROBATION DU DOCUMENT

| Approbations | Postes<br>(Les signatures réelles se trouvent sur une liste de vérification officielle livrable.) |
|---|---|
| **Accepté par** | Directeur général des SCICTR |
| **Accepté par** | Officier responsable, Soutien opérationnel et Services à la clientèle des SCICTR |
| **Accepté par** | Officier responsable, Solutions biométriques d'entreprise des SCICTR |
| **Centre stratégique** | Soutien opérationnel et Services à la clientèle des SCICTR |

## AVERTISSEMENT

Le présent document vise à fournir aux organismes un aperçu de l'infrastructure de réseau et de sécurité établie entre leurs propres installations informatiques et le Réseau des Services nationaux de police (RSNP) aux fins d'identification en temps réel (ITR).

Bien que la Gendarmerie royale du Canada (GRC) fournisse aux organismes des lignes directrices visant à les préparer à relier leur réseau au RSNP, elle n'offre aucune garantie quant à l'intégralité et à l'exactitude de cette documentation. Toutefois, l'utilisateur demeure en définitive responsable de l'adaptation des systèmes existants, de l'intégration des changements qui s'imposent et des résultats obtenus. La GRC, les Services des sciences judiciaires et de l'identité (SSJ&I) et les Services canadiens d'identification criminelle en temps réel (SCICTR) rejettent toute responsabilité et obligation, ainsi que les coûts, la perte d'efficacité ou toute autre perte financière, directe ou indirecte, découlant de tout usage fait par l'utilisateur de l'information présentée ici et de tout autre matériel du présent document.

La GRC n'offre aucune garantie, expresse ou implicite, et rejette en particulier toute garantie implicite de qualité marchande ou de valeur adaptative pour un usage précis. La GRC ne peut être tenue responsable de toute erreur ou omission qui a pu se produire au moment de la préparation des présentes lignes directrices et rejette expressément toute responsabilité, en vertu d'un contrat ou par négligence, envers un utilisateur direct ou tout autre emprunteur ou utilisateur, ou n'importe lequel de leurs clients.

En prenant possession du présent document, l'utilisateur accepte de s'abstenir d'en divulguer le contenu à une tierce partie sans avoir préalablement obtenu l'autorisation explicite écrite de la GRC.  L 'utilisateur du présent document reconnaît et accepte le présent avis et exonère la GRC, les SSJ&I et les SCICTR de toute responsabilité.

**TABLE DES MATIÈRES**

# 1 INTRODUCTION

## 1.1 OBJET

Le présent document vise à fournir aux organismes un aperçu de l'infrastructure de communications établie entre leurs propres installations informatiques et le Réseau des Services nationaux de police (**RSNP**) aux fins d'identification en temps réel (**ITR**). Il permet en outre aux organismes de se familiariser avec le modèle de connexion par point d'accès unique (**PAU**), ainsi qu'avec les options de connectivité réseau mises à leur disposition.

## 1.2 DESTINATAIRES

Le présent document s'adresse aux catégories d'organismes ci-dessous, y compris leurs options de connectivité réseau respectives.

**1.** Organismes d'application de la loi :

GRC; services de police provinciaux, municipaux et militaires qui traitent des empreintes digitales de criminels, de civils et de réfugiés; et organismes fédéraux ayant des pouvoirs d'exécution de la loi.

**2.** Organismes du gouvernement fédéral :

Travaux publics et Services gouvernementaux Canada, Agence du revenu du Canada et autres organismes fédéraux qui traitent des empreintes digitales à des fins civiles.

**3.** Entreprises privées :

Organisations du secteur privé accréditées à prendre des empreintes digitales à des fins civiles, etc.

## 1.3 OPTIONS DE CONNEXION AU RSNP

Le tableau qui suit récapitule tous les organismes concernés, ainsi que leurs options de connectivité réseau respectives :

**Tableau 1 :** Options de connexion au réseau d'ITR

| **Type d'organisme** | **Options de connexion au réseau d'ITR**[1] | | |
|---|---|---|---|
| | **SNP** | **Réseau de la VCP** | **Connexion Internet sécurisée** |
| **Organismes d'application de la loi** | Tous | Non disponible | Non disponible |
| **Organismes fédéraux** | Non disponible | Organismes fédéraux seulement[2] | Non disponible |
| **Entreprises privées** | Non disponible | Non disponible | Tous |

[1] La GRC évaluera au cas par cas les options de connexion réseau des organismes gouvernementaux provinciaux, municipaux et territoriaux.

[2] Les organismes fédéraux doivent se connecter au RSNP par le truchement d'un tunnel partagé qui emprunte le Réseau de la VCP.

## 2 POINT D'ACCÈS UNIQUE (PAU)

Le PAU est une fonctionnalité du réseau d'ITR qui permet à chaque organisme de bénéficier d'une connexion unique au RSNP. L'organisme peut ainsi communiquer directement par protocole de transfert de courrier simple (**protocole SMTP**) avec le serveur NIST (*National Institute of Standards and Technology*) des SNP (Services nationaux de police) grâce à l'option de connexion qu'il a choisie.

Le PAU d'un organisme peut être un dispositif de lecture électronique des empreintes (**DLEE**, p. ex. LiveScan ou CardScan) ou un serveur de messagerie centralisée relié à de multiples systèmes de LEE et d'autres systèmes protégés par le serveur ou le réseau de l'organisme. Se connectant directement au serveur NIST des SNP (**gestionnaire des flux de travaux**), le PAU de l'organisme constitue l'unique point de contact au RSNP de l'organisme.

Le modèle de connexion par PAU peut supposer l'intégration de DLEE à d'autres composants des systèmes hébergés par le serveur de messagerie centralisée situé sur le site de l'organisme. Le serveur de l'organisme pourra ainsi communiquer directement avec le gestionnaire des flux de travaux qui relie tous les DLEE et autres composants de systèmes qui se trouvent sur le site de l'organisme.

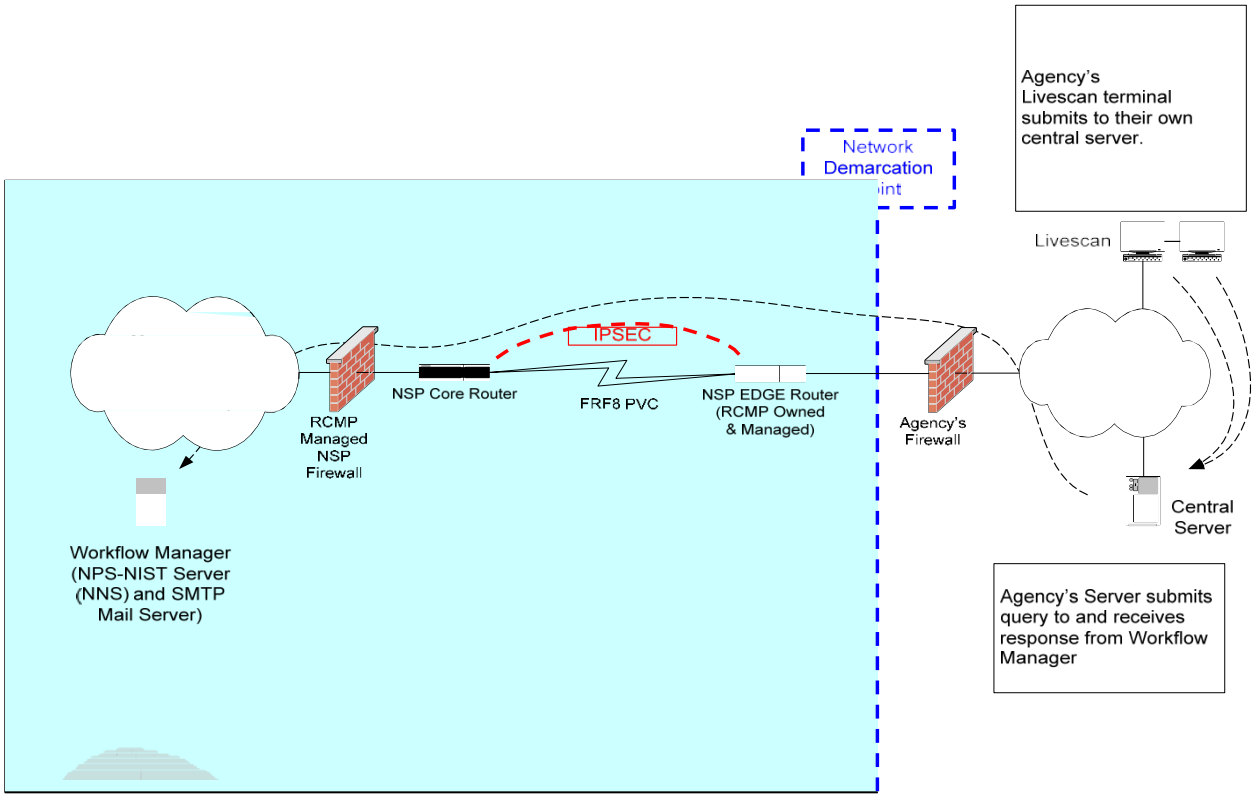
Tous les organismes qui souhaitent soumettre des transactions au gestionnaire des flux de travaux doivent adhérer au concept de connexion par PAU.

**Nota :** Pour de plus amples renseignements au sujet du concept de connexion par PAU, voir la **section 2** du document *Pratiques exemplaires de mise en œuvre des flux de travaux pour les dispositifs de lecture électronique des empreintes digitales à des fins civiles*.

# 3 POSTURE DE SÉCURITÉ DU RÉSEAU

## 3.1 ORGANISMES D'APPLICATION DE LA LOI – CONNEXION RÉSEAU DE SYSTÈME À SYSTÈME

Figure 1 - Organismes d'application de la loi – Connexion réseau de système à système




### 3.1.1 Aperçu

- Une connexion réseau de système à système facilite la mise en œuvre et l'utilisation du modèle de connexion par PAU.
- La connexion est établie par le truchement d'un circuit de posture de sécurité réseau (PSR) entre le serveur de l'organisme d'application de la loi et le gestionnaire des flux de travaux.

### 3.1.2 Exigences

- Le chiffrement de lien fourni par les routeurs gérés de la GRC (routeurs d'infrastructure de PSR et routeurs de périphérie) est nécessaire pour la séquence de traversée vers le circuit de communications à relais de trames. Les routeurs gérés de la GRC feront l'objet de certificats pour périphériques d'Entrust de la GRC.
- Le serveur de l'organisme sera établi au sein du réseau de l'organisme.
- Le serveur de l'organisme communiquera avec le gestionnaire des flux de travaux par protocole SMTP.

- La connexion PSR agit comme transporteur pour les communications entre le serveur de l'organisme et le gestionnaire des flux de travaux.
- Le système de la GRC déterminera que le serveur de l'organisme tente d'accéder au réseau à partir de sa propre adresse **IP** (protocole Internet) enregistrée auprès de l'Internet Assigned Numbers Authority (**IANA**) ou, s'il utilise la fonction de traduction d'adresses de réseau (**TAR**), à partir de l'adresse IP PSR attribuée par la GRC.
- La démarcation entre le réseau de l'organisme et la PSR est établie par le câble qui relie le routeur géré de la PSR de la GRC au pare-feu de l'organisme (ou au serveur de l'organisme, si celui-ci n'a pas installé de pare-feu).
- Toutes les données qui traversent les circuits du réseau étendu de la PSR sont cryptées par protocole IPSec entre le routeur périphérique géré de l'organisme et le routeur de cœur au sein de la PSR.

## 3.2 ORGANISMES D'APPLICATION DE LA LOI – RESPONSABILITÉS

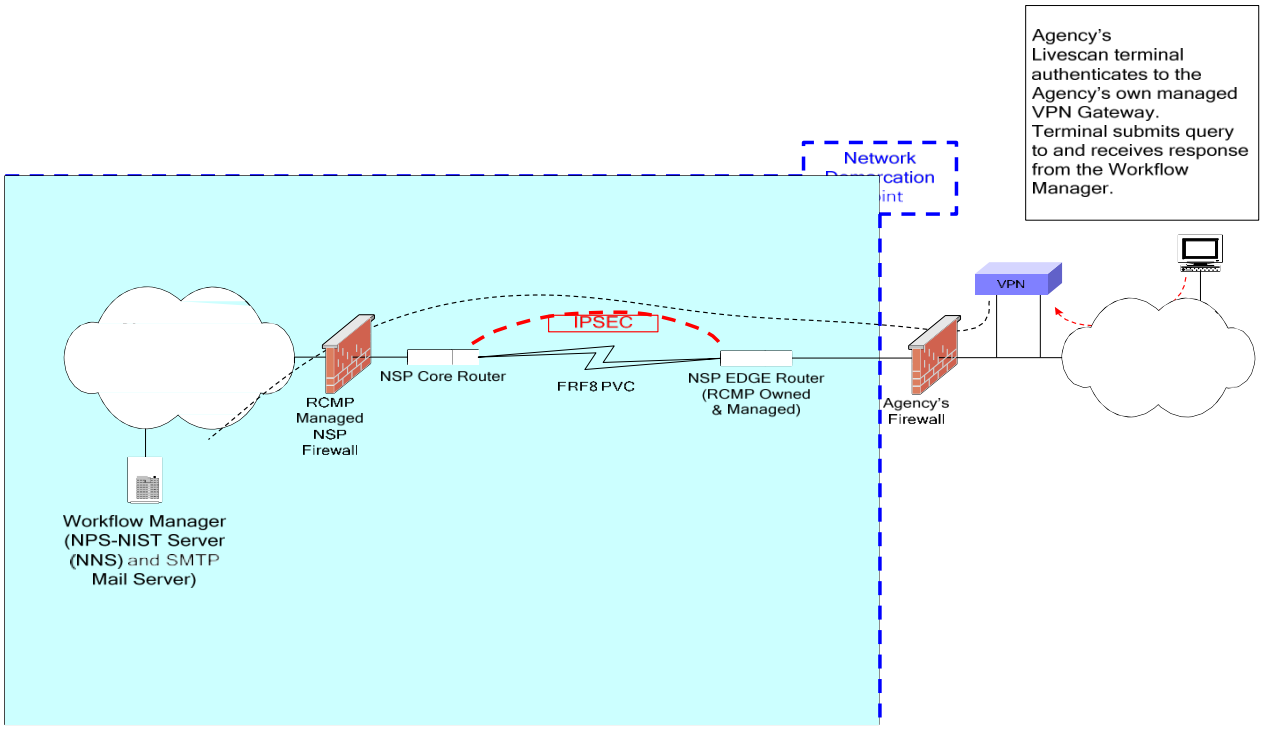
- Le serveur de l'organisme doit communiquer avec le gestionnaire des flux de travaux par protocole SMTP. Il incombe à l'organisme d'activer et de valider la fonction de messagerie SMTP de sa connexion.
- Il incombe à l'organisme de faire en sorte que ses différents emplacements puissent accéder aux services d'ITR en se servant de leur propre réseau étendu comme transporteur.
- Tous les services que la GRC fournit aux réseaux des organismes et qu'elle reçoit de ceux-ci doivent passer par un pare-feu de la GRC installé à Ottawa (Ontario).
- Toutes les modifications devant être apportées au pare-feu de l'organisme doivent être annoncées au moins deux semaines à l'avance. **Nota :** Il est important que l'organisme annonce à l'avance les modifications qu'il apportera à son au pare-feu, au cas où il changerait l'adresse IP reconnue par la PSR.
- L'organisme doit collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC au maintien, à la modification ou à la mise à niveau de son réseau à la suite de toute menace à la sécurité de l'information, évolution des normes technologiques ou transition à un nouvel équipement.
- L'organisme doit fournir les noms et les coordonnées d'une personne-ressource principale et d'une personne-ressource secondaire qui seront chargées de résoudre les problèmes techniques et fonctionnels (p. ex. coordonnées des responsables de la sécurité et du réseau).

### 3.2.1 Recommandation

- On recommande fortement à l'organisme de se procurer et d'installer un pare-feu conforme EAL-4.

## 3.3 ORGANISMES D'APPLICATION DE LA LOI – CONNEXION RÉSEAU DE CLIENT À SYSTÈME

Figure 2 - Organismes d'application de la loi – Connexion réseau de client à système – L'organisme fournit la connexion à un RPV de client à passerelle RPV.




### 3.3.1 Aperçu

- Une connexion réseau de client à système facilite la mise en œuvre et l'utilisation du modèle de connexion par PAU.
- La connexion est établie par le truchement d'un circuit de posture de sécurité réseau (PSR) entre le DLEE (p. ex. LiveScan ou CardScan) de l'organisme d'application de la loi et le gestionnaire des flux de travaux.

### 3.3.2 Exigences

- Le chiffrement de lien fourni par les routeurs gérés de la GRC (routeurs d'infrastructure de PSR et routeurs de périphérie) est nécessaire pour la séquence de traversée vers le circuit de communications à relais de trames. Les routeurs gérés de la GRC feront l'objet de certificats pour périphériques d'Entrust de la GRC.
- Le DLEE de l'organisme sera installé au sein du réseau de l'organisme.
- Le DLEE de l'organisme enverra des transactions électroniques au gestionnaire des flux de travaux par protocole SMTP et recevra des transactions électroniques de celui-ci par protocole **POP** (Post Office Protocol).
- La connexion PSR agit comme transporteur pour les communications entre le DLEE de l'organisme et le gestionnaire des flux de travaux.

- Le système de la GRC déterminera que le serveur de l'organisme tente d'accéder au réseau à partir de sa propre adresse IP enregistrée auprès de l'IANA ou, s'il utilise la fonction de TAR, à partir de l'adresse IP PSR attribuée par la GRC.
- La démarcation entre le réseau de l'organisme et la PSR est établie par le câble qui relie le routeur géré de la PSR de la GRC au pare-feu de l'organisme (ou au DLEE de l'organisme, si celui-ci n'a pas installé de pare-feu).
- L'organisme doit établir une session de travail cryptée lorsqu'il se branche à son RPV de client à passerelle.

## 3.4 ORGANISMES D'APPLICATION DE LA LOI – RESPONSABILITÉS

- Il incombe à l'organisme d'activer et de valider la fonction de messagerie SMTP et le protocole POP de son DLEE.
- Il incombe à l'organisme de faire en sorte que ses différents emplacements puissent accéder aux services d'ITR en se servant de leur propre réseau étendu comme transporteur.
- Tous les services que la GRC fournit aux réseaux des organismes et qu'elle reçoit de ceux-ci doivent passer par un pare-feu de la GRC installé à Ottawa (Ontario).
- Toutes les modifications devant être apportées au pare-feu de l'organisme doivent être annoncées au moins deux semaines à l'avance. **Nota :** Il est important que l'organisme annonce à l'avance les modifications qu'il apportera à son au pare-feu, au cas où il changerait l'adresse IP reconnue par la PSR.
- L'organisme doit collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC au maintien, à la modification ou à la mise à niveau de son réseau à la suite de toute menace à la sécurité de l'information, évolution des normes technologiques ou transition à un nouvel équipement.
- L'organisme doit fournir les noms et les coordonnées d'une personne-ressource principale et d'une personne-ressource secondaire qui seront chargées de résoudre les problèmes techniques et fonctionnels (p. ex. coordonnées des responsables de la sécurité et du réseau).
- L'organisme doit établir une session de travail cryptée lorsqu'il branche son DLEE à son RPV de client à passerelle.

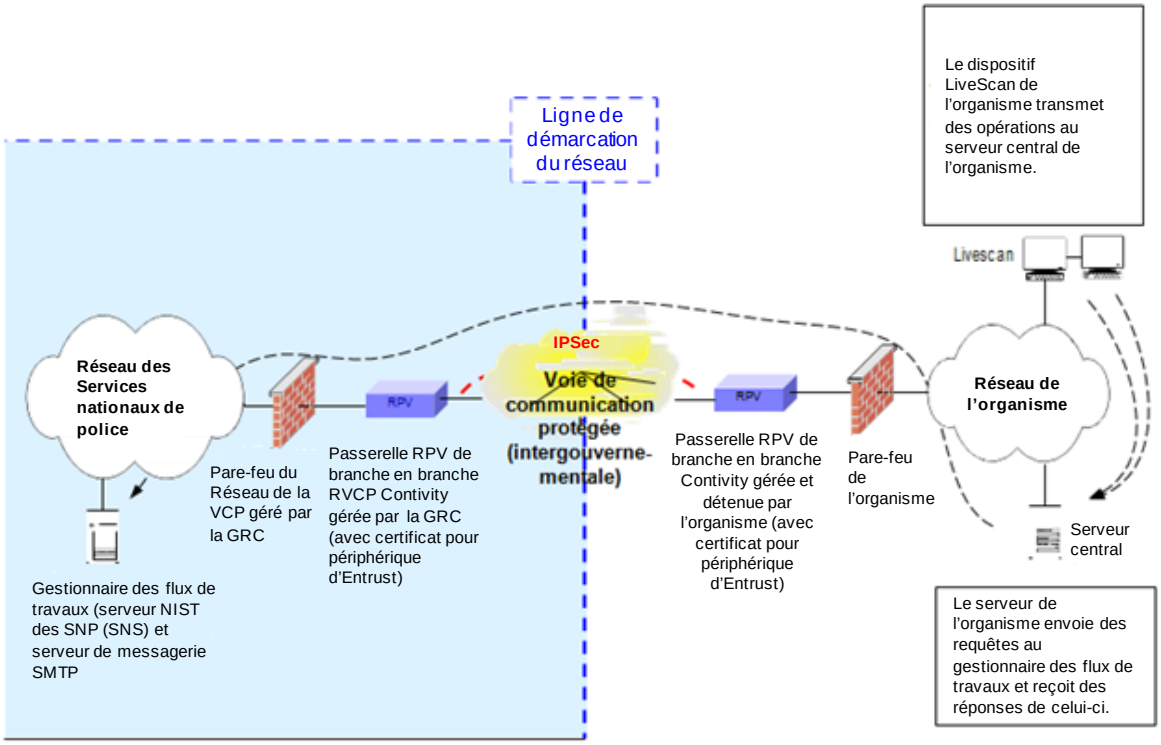
### 3.4.1 Recommandation

- On recommande fortement à l'organisme de se procurer et d'installer un pare-feu conforme EAL-4.

# 4 VOIE DE COMMUNICATION PROTÉGÉE (COMMUNICATIONS INTERGOUVERNEMENTALES)

## 4.1 ORGANISMES FÉDÉRAUX – CONNEXION RÉSEAU DE SYSTÈME À SYSTÈME

Figure 3 - Organismes fédéraux – Connexion réseau de système à système




### 4.1.1 Aperçu

- Une connexion réseau de système à système facilite la mise en œuvre et l'utilisation du modèle de connexion par PAU.
- La connexion est établie par le Réseau de la VCP entre le serveur de l'organisme (p. ex. PAU) et le gestionnaire des flux de travaux.

### 4.1.2 Exigences

- Un RPV fiable utilisant le Réseau de la VCP comme transporteur sera établi entre le RPV de l'organisme et la passerelle RPV de branche en branche RVCP de la GRC.
- Le chiffrement de lien sera fourni par le RPV fiable entre la passerelle RPV de l'organisme et la passerelle RPV de branche en branche RVCP de la GRC.
- Un certificat pour périphérique d'Entrust[3] cocertifié par la GRC est obligatoire.
- Le système de la GRC déterminera que le serveur de l'organisme tente d'accéder au réseau à partir de sa propre adresse IP enregistrée auprès de l'IANA.

[3] Pour obtenir de plus amples renseignements à propos des services de certificat ICP, les organismes fédéraux doivent communiquer avec la Gestion des justificatifs internes de Travaux publics et Services gouvernementaux Canada (TPSGC).

## 4.2 ORGANISMES FÉDÉRAUX – RESPONSABILITÉS

- L'organisme doit se doter de sa propre passerelle RPV, laquelle doit avoir fait l'objet d'un certificat pour périphérique d'Entrust cocertifié par la GRC et être compatible avec le mode de déploiement du RPV de la GRC.
- L'organisme doit s'assurer que le dispositif de la passerelle RPV est branché à une alimentation secteur adéquatement régulée et ventilée, qui est généralement reliée au système d'alimentation sans coupure directe ou à tout autre système similaire de la salle des serveurs, et installé dans une salle sécuritaire et bien aérée.
- Il incombe à l'organisme de réparer ou de remplacer sa passerelle RPV au besoin.
- L'organisme doit collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC au maintien, à la modification ou à la mise à niveau de son équipement (p. ex. RPV) à la suite de toute menace à la sécurité de l'information, évolution des normes technologiques ou transition à un nouvel équipement.
- L'organisme doit fournir les noms et les coordonnées d'une personne-ressource principale et d'une personne-ressource secondaire qui seront chargées de résoudre les problèmes techniques et fonctionnels.

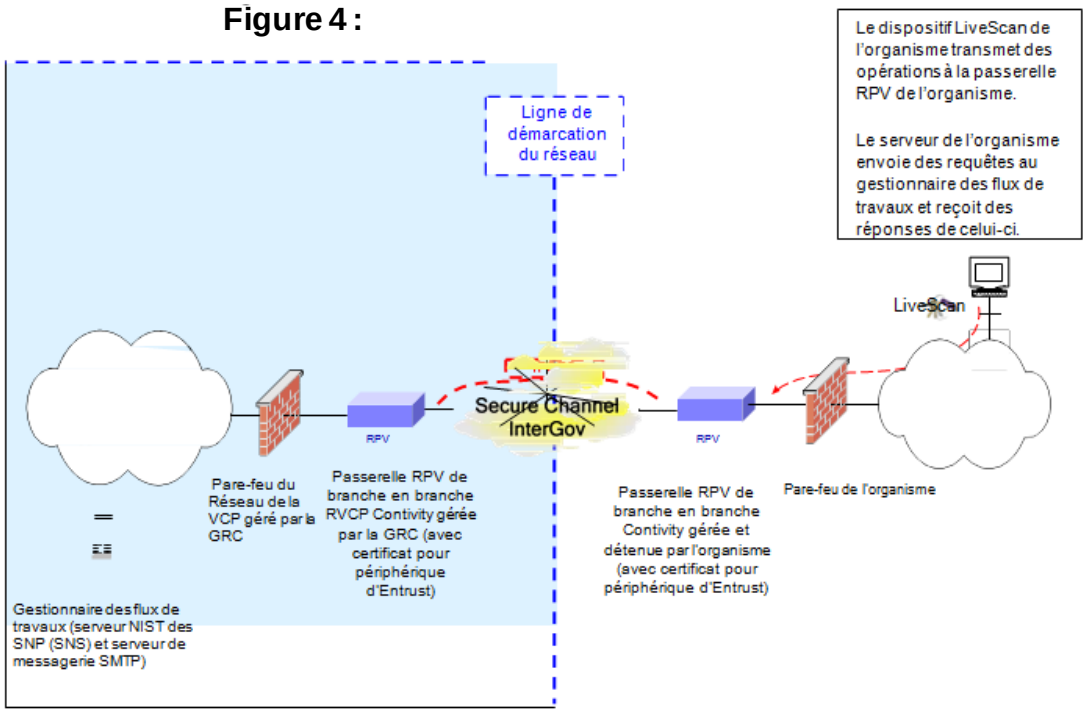
### 4.2.1 Recommandation

- On recommande fortement à l'organisme de se procurer et d'installer un pare-feu conforme EAL-4.

## 4.3 ORGANISMES FÉDÉRAUX – CONNEXION RÉSEAU DE CLIENT À SYSTÈME

Figure 4 : Organismes fédéraux – Connexion réseau de client à système – L'organisme fournit la connexion à un RPV de client à passerelle RPV.

**Figure 4 :**




### 4.3.1 Aperçu

- Une connexion réseau de client à système facilite la mise en œuvre et l'utilisation du modèle de connexion par PAU.
- La connexion est établie par le truchement du Réseau de la VCP entre le DLEE (p. ex. LiveScan ou CardScan) de l'organisme fédéral et le gestionnaire des flux de travaux.

### 4.3.2 Exigences

- Un RPV fiable utilisant le Réseau de la VCP comme transporteur sera établi entre le RPV de l'organisme et la passerelle RPV d'une direction générale à l'autre de la GRC qui est reliée au Réseau de la VCP.
- Le chiffrement de lien sera fourni par le RPV fiable entre la passerelle RPV de l'organisme et la passerelle RPV d'une direction générale à l'autre de la GRC qui est reliée au Réseau de la VCP.
- Un certificat pour périphérique d'Entrust[4] cocertifié par la GRC est obligatoire.
- Le système de la GRC déterminera que le DLEE de l'organisme tente d'accéder au réseau à partir de sa propre adresse IP enregistrée auprès de l'IANA.

[4] Pour obtenir de plus amples renseignements à propos des services de certificat ICP, les organismes fédéraux doivent communiquer avec la Gestion des justificatifs internes de Travaux publics et Services gouvernementaux Canada (TPSGC).

- L'organisme doit établir une session de travail cryptée lorsqu'il se branche à son RPV de client à passerelle.

## 4.4 ORGANISMES FÉDÉRAUX – RESPONSABILITÉS

- L'organisme doit se doter de sa propre passerelle RPV, laquelle doit avoir fait l'objet d'un certificat pour périphérique d'Entrust cocertifié par la GRC et être compatible avec le mode de déploiement du RPV de la GRC.
- L'organisme doit s'assurer que le dispositif de la passerelle RPV est branché à une alimentation secteur adéquatement régulée et ventilée, qui est généralement reliée au système d'alimentation sans coupure directe ou à tout autre système similaire de la salle des serveurs, et installé dans une salle sécuritaire et bien aérée.
- Il incombe à l'organisme de réparer ou de remplacer sa passerelle RPV au besoin.
- L'organisme doit collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC au maintien, à la modification ou à la mise à niveau de son équipement (p. ex. RPV) à la suite de toute menace à la sécurité de l'information, évolution des normes technologiques ou transition à un nouvel équipement.
- L'organisme doit fournir les noms et les coordonnées d'une personne-ressource principale et d'une personne-ressource secondaire qui seront chargées de résoudre les problèmes techniques et fonctionnels.
- L'organisme doit établir une session de travail cryptée lorsqu'il se branche à son RPV de client à passerelle.

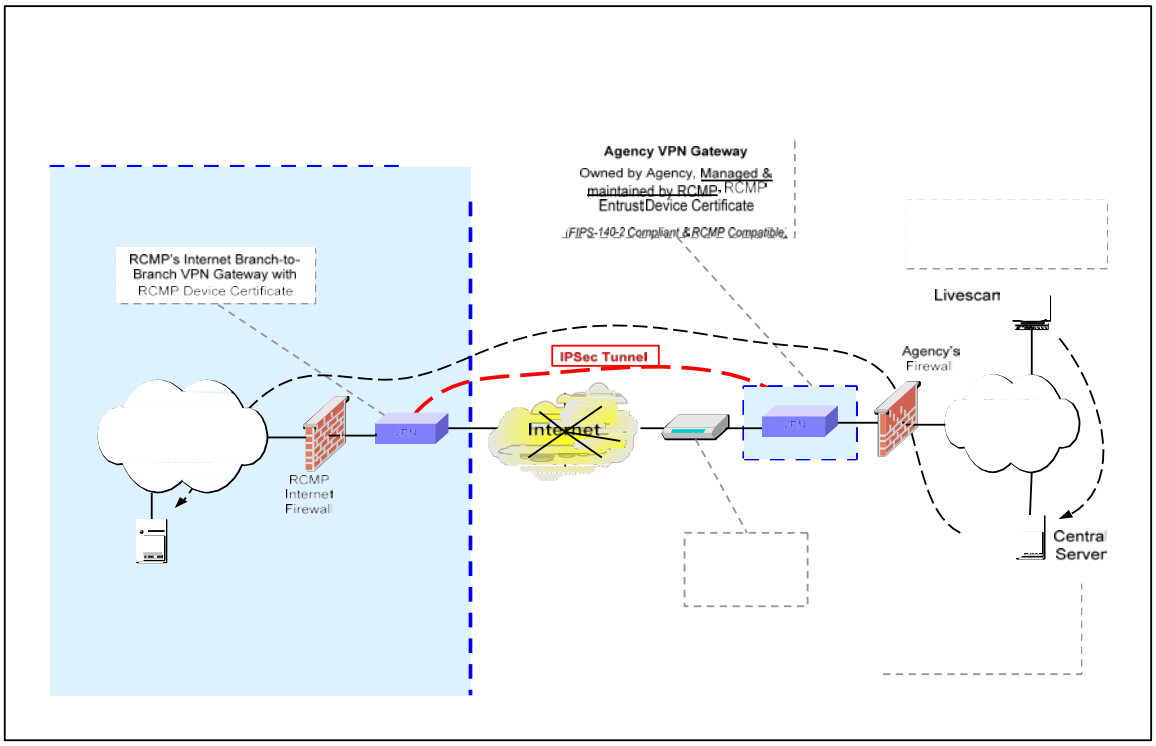
### 4.4.1 Recommandation

- On recommande fortement à l'organisme de se procurer et d'installer un pare-feu conforme EAL-4.

# 5 CONEXION INTERNET SÉCURISÉE

## 5.1 ENTREPRISES PRIVÉES – CONNEXION RÉSEAU DE SYSTÈME À SYSTÈME

Figure 5 : Entreprises privées – Connexion réseau de système à système




### 5.1.1 Aperçu

- Une connexion réseau de système à système facilite la mise en œuvre et l'utilisation du modèle de connexion par PAU.
- La connexion est établie par le truchement d'un lien Internet sécurisé entre le serveur de l'entreprise privée (p. ex. PAU) et le gestionnaire des flux de travaux.

### 5.1.2 Exigences

- L'adresse IP du serveur de l'entreprise qui sera reconnue par le RSNP doit être une adresse IP statique[5] enregistrée[6].
- Si le dispositif d'accès à Internet (p. ex. routeur, commutateur Ethernet, etc.) est utilisé par d'autres éléments du réseau de l'entreprise privée que le RPV, il doit pouvoir prendre en charge un tunnel IPSec, sinon, le RPV ne pourra pas communiquer avec la GRC.

[5] Les adresses IP statiques sont attribuées à des dispositifs permanents reliés à un réseau dont les adresses IP sont constantes et ne changent jamais.

[6] Le protocole DHCP (*Dynamic Host Configuration Protocol*) n'est pas pris en charge par ce type de connexion, parce qu'il complique les opérations d'entretien et de réparation. Nota : Vu cette exigence, il est impossible d'utiliser un accès par ligne commuté relié au RTCP, ce type de service ne prenant pas en charge les adresses IP statiques.

- Le RPV de l'entreprise obtiendra un certificat pour périphérique d'Entrust de la GRC, qui installera et configurera le RPV de l'entreprise en fonction des paramètres de ce certificat.

## 5.2 ENTREPRISES PRIVÉES – RESPONSABILITÉS

- L'entreprise ne doit se connecter au réseau de la GRC que par le truchement d'une adresse IP statique enregistrée à son propre nom ou détenue par un tiers au nom de l'entreprise, comme dans le cas d'un fournisseur d'accès Internet (FAI[7]).
- L'entreprise privée doit collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC au maintien, à la modification ou à la mise à niveau de son réseau à la suite de toute menace à la sécurité de l'information, évolution des normes technologiques ou transition à un nouvel équipement.
- L'entreprise privée doit fournir le nom et les coordonnées d'une personne-ressource principale et d'une personne-ressource secondaire qui seront chargées de résoudre les problèmes techniques et fonctionnels.
- Il incombe à l'entreprise de réparer ou de remplacer son équipement (à l'exception des dispositifs de RPV).
- L'entreprise privée doit se doter d'un RPV compatible avec le mode de déploiement du RPV de la GRC.
- L'entreprise doit s'assurer que le RPV est branché à une alimentation secteur adéquatement régulée et ventilée, qui est généralement reliée au système d'alimentation sans coupure directe ou à tout autre système similaire de la salle des serveurs, et installé dans une salle sécuritaire et bien aérée.
- L'entreprise privée doit fournir un accès libre raisonnable aux techniciens autorisés de la GRC qui seront chargés de réparer, d'entretenir ou d'inspecter le dispositif de RPV à la suite d'un problème ou aux fins d'entretien ou d'examen périodique de l'équipement.
- En cas de défaillance du dispositif de RPV d'une entreprise privée, un technicien de la GRC peut lui prêter un autre dispositif afin qu'elle continue de fonctionner pendant les travaux de réparation de son RPV. Il incombe toutefois à l'entreprise privée de faire réparer son dispositif de RPV ou de le remplacer.
  - L'entreprise est tenue de faire réparer son dispositif ou de le remplacer dans un délai raisonnable. Une fois que son dispositif est réparé, elle doit communiquer avec le Bureau d'assistance centrale (**BAC**) de la GRC afin qu'il envoie un technicien remplacer le dispositif prêté par son propre dispositif de RPV réparé.
  - L'entreprise est tenue de collaborer de façon continue avec les responsables techniques de la sécurité et du réseau de la GRC. Il pourrait être nécessaire de mettre à jour le matériel, les logiciels ou les micrologiciels du dispositif de RPV afin d'en maintenir le rendement soutenu[8] (p. ex. capacité à garantir la sécurité des

[7] Les adresses IP sont enregistrées au nom des entreprises par les fournisseurs d'accès Internet ou de services de télécommunications de celles-ci ou inscrites directement dans un registre Internet régional (RIR).

[8] Il incombe à l'entreprise privée de décider si elle souhaite se prévaloir des programmes d'entretien du matériel, des logiciels, des micrologiciels ou autres du fabricant du RPV ou d'un tiers.

communications, compatibilité avec l'équipement de la GRC, capacité à obtenir du soutien du fabricant, etc.).

- Si le dispositif de RPV requiert des mises à jour, l'entreprise doit s'en occuper dans un délai raisonnable (c.-à-d. dans les 30 à 60 jours ou moins). S'il s'agit de mises à jour nécessaires pour atténuer une menace à la sécurité, l'entreprise privée est tenue de prendre les mesures qui s'imposent le plus rapidement possible (p. ex. les délais dépendent de la gravité de la menace).

### 5.2.1 Recommandation

- On recommande à l'entreprise privée de se prévaloir d'un service d'accès Internet commercial, qui présente habituellement une meilleure disponibilité sous-jacente et un temps moyen de dépannage plus court que les services résidentiels ou non commerciaux.
- On recommande fortement à l'entreprise privée de se procurer et d'installer un pare-feu conforme EAL-4.
- Si l'entreprise choisit d'installer un pare-feu, elle doit s'assurer qu'il est conforme aux exigences (p. ex. exigences de configuration) du SSN de la GRC[9].

[9] L'entreprise privée partagera de façon confidentielle suffisamment d'information sur la configuration de son pare-feu pour permettre l'établissement d'une connexion sécurisée. Plus particulièrement, le pare-feu doit être configuré de manière à accepter seulement les communications transitant par le tunnel RPV qui proviennent de la GRC. Le partage de cette information ne nécessite pas que la GRC certifie ou valide la configuration du pare-feu.

# 6 CONNEXION DES ORGANISMES FÉDÉRAUX AU RSNP

## 6.1 CONNEXION AU RÉSEAU D'ITR

Les organismes fédéraux doivent se connecter au RSNP par le truchement d'un tunnel partagé qui emprunte le Réseau de la VCP, tel que mentionné à la section 4 du présent document.

## 6.2 TRANSITION À LA CONNEXION INTERENTREPRISES

La GRC s'efforce de faire en sorte que tous les organismes soient reliés aux services du RSNP par le truchement d'un point d'accès unique. On considère que l'accès au RSNP par tunnel RPV empruntant le Réseau de la VCP constitue une connexion interentreprises entre les organismes fédéraux et le RSNP. La GRC entend faire en sorte que cette connexion permanente soit le seul mécanisme grâce auquel les organismes fédéraux accèdent aux services d'ITR et aux autres applications du RSNP, telles que l'application du Centre d'information de la police canadienne (**CIPC**) (p. ex. site Web du CIPC).

À l'heure actuelle, plusieurs organismes fédéraux accèdent aux services du RSNP (p. ex. site Web du CIPC) par un ou plusieurs circuits de connexion directe fournis par la GRC. Dans le cadre du modèle de connexion par PAU, les organismes fédéraux doivent intégrer à leur propre réseau tous les services du RSNP auxquels ils ont accès (p. ex. site Web du CIPC). En résumé, tous les services du RSNP dont un organisme fédéral peut avoir besoin seront accessibles à partir du réseau de l'organisme par le truchement d'une connexion interentreprises à un RPV unique empruntant le Réseau de la VCP.

## 6.3 AVANTAGES DE LA CONNEXION INTERENTREPRISES

Au moyen d'une seule connexion réseau, les organismes fédéraux peuvent avoir accès à de nombreux services du RSNP de la GRC. Pour ce faire, ils devront peut-être intégrer les icônes des applications du RSNP (p. ex. site Web du CIPC) à leurs bureaux informatiques actuels, ce qui éliminera la nécessité de consacrer des postes de travail au seul accès à ces applications.

- Les figures présentées aux pages suivantes illustrent la transition de la GRC vers un modèle de connexion interentreprises au Réseau de la VCP pour les organismes fédéraux.

Figure 6 : Organismes fédéraux – Connexion gérée de bout en bout de la GRC – *Aperçu de l'actuel modèle de connexion que les organismes fédéraux peuvent utiliser pour accéder aux applications du RSNP.*

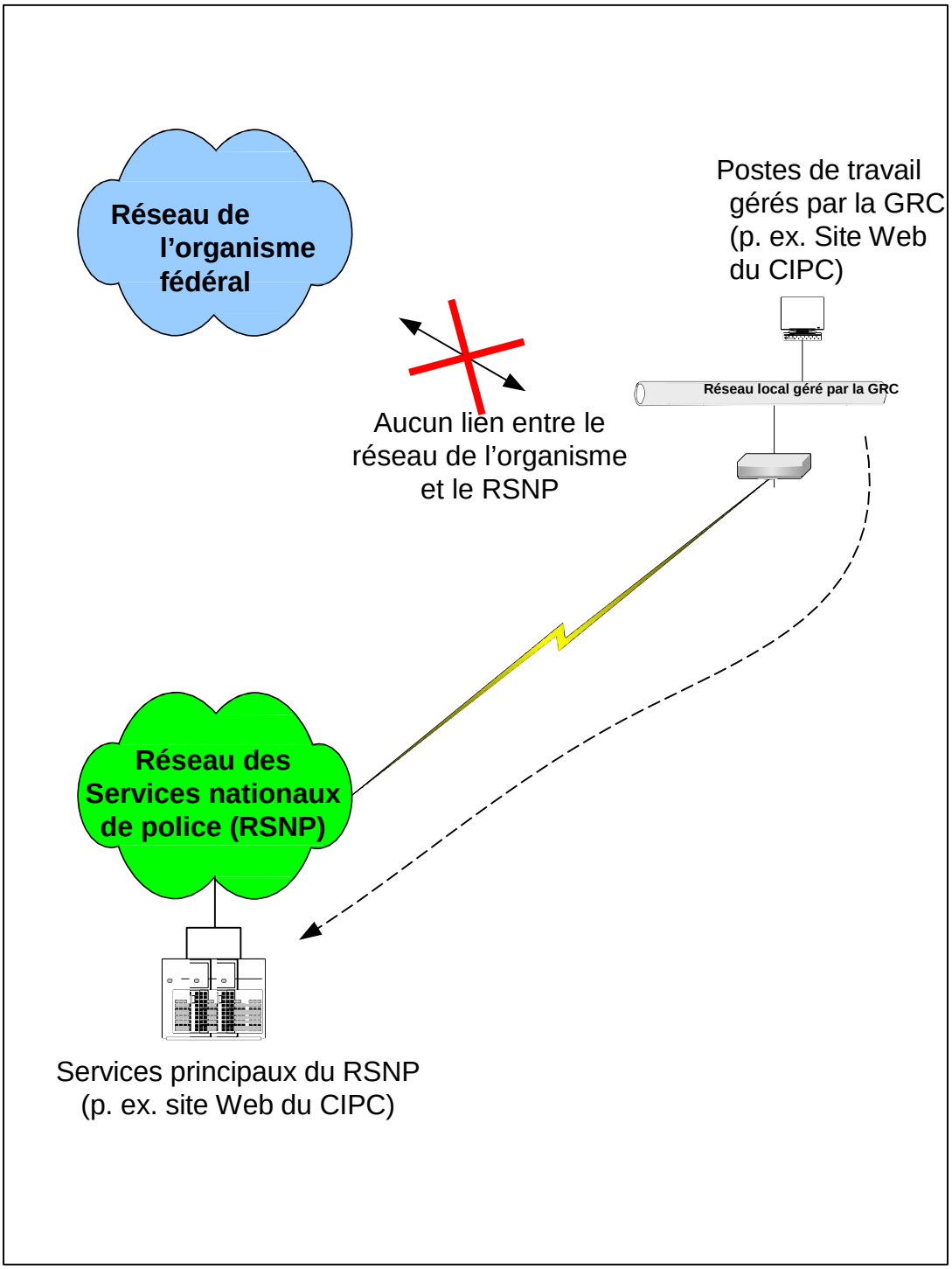
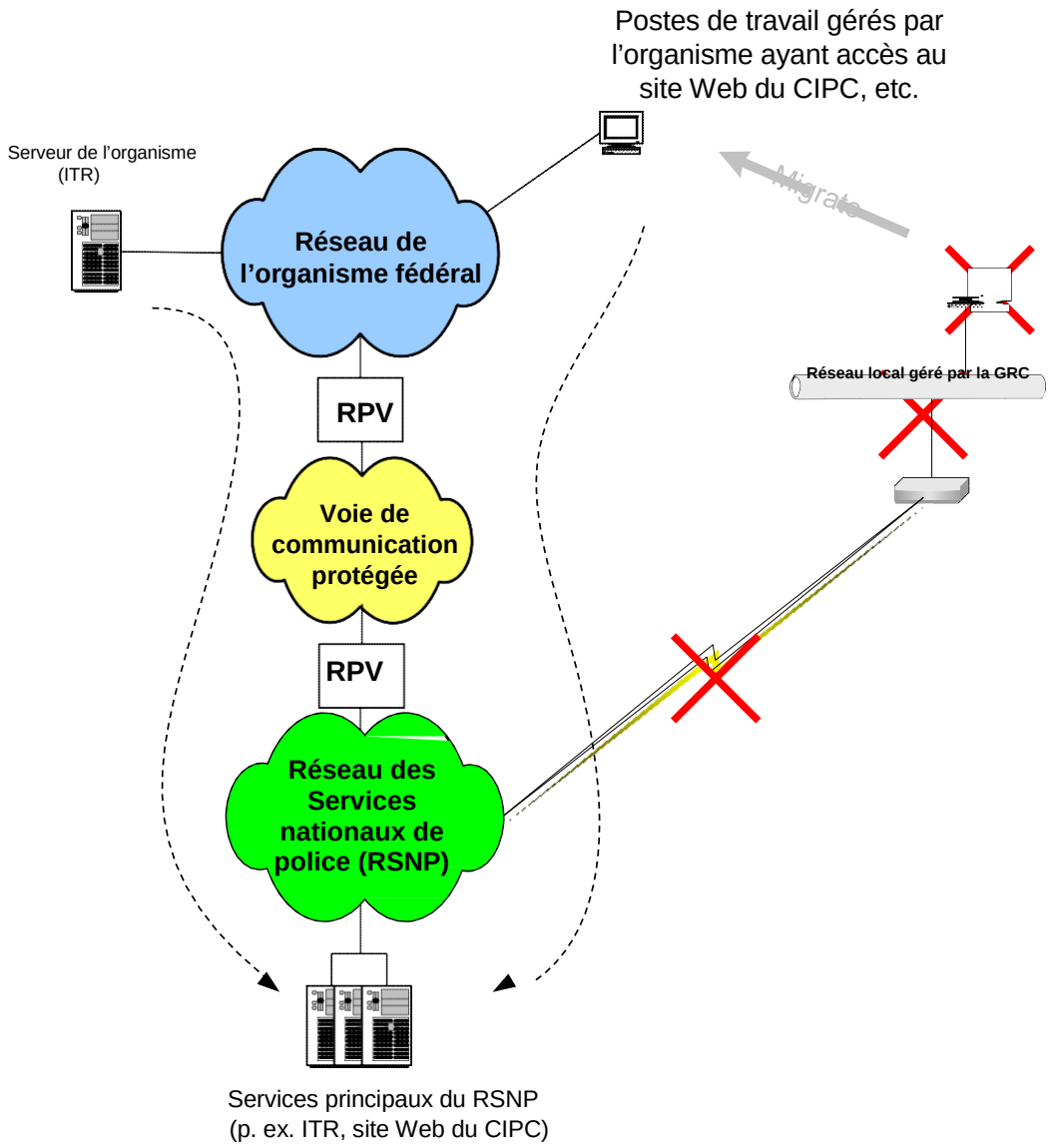


Figure 7 : Organismes fédéraux – Connexion interentreprises consécutive à la mise en fonction du projet d'ITR – *Aperçu de la migration des organismes fédéraux vers une connexion interentreprises empruntant le Réseau de la VCP pour accéder au RSNP*.

**Figure 7 :** Organismes fédéraux – Connexion interentreprises consécutive à la mise en fonction du projet d'ITR



### 6.4 ITR et applications du CIPC

Pour qu’un organisme du gouvernement fédéral puisse intégrer une application du CIPC à son propre réseau, celui-ci doit avoir été approuvé par le CIPC.

Tous les organismes fédéraux qui accèdent actuellement aux services du RSNP à partir d’un réseau géré par la GRC devront se prêter au processus de modification ou de demande d’autorisation de connexion au RSNP en vue de la migration de tous les services du RSNP au tunnel partagé qui emprunte le Réseau de la VCP. Une fois que la migration est entamée et que la date d’annulation des circuits de connexion directe au RSNP a été fixée provisoirement, l’organisme fédéral peut commencer à établir l’interface avec le RSNP aux fins d’ITR.

# 7 COORDONNÉES

**Soutien opérationnel et Services à la clientèle des SCICTR**

- Courriel : CCRTIS-SCICTR@rcmp-grc.gc.ca
- Renseignements généraux et information sur la certification

**Bureau d'assistance centrale (BAC)**

- 1-800-461-7797
- Soutien technique et fonctionnel à l'ITR pour le personnel autorisé
- **Nota :** Un organisme doit avoir été certifié par la GRC avant de pouvoir communiquer avec le BAC