ANNEXE A
ÉNONCÉ DE TRAVAIL

Réseau étendu à définition logicielle (REDL)

Solution client

Finale Version 2.0
7 décembre 2021

Table des matières

Liste des figures

1 INTRODUCTION

1.1 Objet

(1) Services partagés Canada (SPC) a besoin dans les plus brefs délais d'une solution de réseau étendu à définition logicielle (REDL), pour répondre à ses besoins opérationnels immédiats.

(2) Les réseaux du gouvernement du Canada relient plus de 3 500 emplacements dans plus de 1 300 villes et villages. SPC assure les services de réseau de 42 ministères et organismes fédéraux. Les bureaux des clients peuvent être tant des emplacements critiques où la disponibilité doit être très élevée, comme les administrations régionales des ministères et les bureaux bien en vue, que des bureaux éloignés difficiles d'accès.

(3) Services partagés Canada (SPC) a actualisé sa stratégie sur les réseaux et la sécurité afin de l'harmoniser avec les pratiques exemplaires actuelles et pour l'adapter aux besoins futurs de son réseau et de ses services de sécurité. Les réseaux logiciels, et particulièrement les réseaux logiciels étendus, sont un pilier essentiel de la mise en place de cette stratégie.

(4) L'impératif de réviser cette stratégie est renforcé par la nature des données transmises sur les réseaux gouvernementaux : données ministérielles, transmissions vidéo en temps réel, renseignements personnels des Canadiens qui interagissent avec les agences et les ministères fédéraux, et bien d'autres choses.

(5) En conformité avec sa stratégie, SPC prévoit de se procurer une solution de REDL pour les sites internationaux et de répondre aux besoins opérationnels immediats. Comme SPC veut centraliser au nom de ses clients la gestion de tous les réseaux superposés, ce réseau logiciel devra être fourni par un seul fabricant d'équipement d'origine (FEO) et fournisseur de la solution.

1.2 Résultats opérationnels

(6) Par la mise en œuvre du REDL, SPC s'attend aux principaux avantages suivants :

a) expérience de l'utilisateur améliorée, par la visibilité de bout-en-bout et la capacité de surveiller et rehausser automatiquement la qualité du service (QdS) selon l'application et l'emplacement;

b) fiabilité accrue et meilleur contrôle du trafic, par l'exploitation de plusieurs voies de transport en fonction des politiques et des ententes sur les niveaux de service (ENS);

c) sécurité renforcée, par une visibilité et un contrôle centralisés des services et dispositifs réseau, notamment la détection immédiate des incidents et la capacité d'y répondre tout aussi vite en appliquant des politiques de sécurité à tous les dispositifs du REDL;

d) robustesse du réseau améliorée, par l'automatisation, la correction automatique et la reprise automatique;

e) administration simplifiée du réseau étendu, par la configuration centralisée de tous les réseaux;

f) déploiement sans intervention, ce qui réduira le travail des techniciens sur place;

g) gestion du trafic de tous les réseaux logiques;

h) réduction du coût moyen de la bande passante, et possibilité de réduire ces frais ou d'augmenter considérablement la bande passante par l'utilisation accrue de réseaux à large bande; et

i) éliminer les obstacles technologiques à l'accessibilité des technologies de l'information et des communications (TIC).

1.3 Stratégie

(7) Le contrat qui pourra découler du présent appel d'offres devra permettre à SPC de se procurer un réseau logiciel qui répondra aux besoins opérationnels à court terme d'au moins un de ses clients.

(8) La solution de réseau logiciel devra comprendre les périphériques, le logiciel de commande et d'orchestration et tout matériel nécessaire, selon la solution choisie, et un portail Web d'abonnés qui permettre à SPC de gérer de façon centralisée tous les aspects des réseaux superposés qui forment le REDL. Les réseaux superposés eux-mêmes (MLPS, Internet large bande ou Ethernet câblé, par exemple) dépassent la portée de la solution recherchée.

(9) SPC entend ainsi se procurer :

a) quatre cent quatorze périphériques de capacités diverses, en fonction des caractéristiques de chaque emplacement;

b) un ensemble redondant de tout logiciel et matériel de commande et d'orchestration nécessaire pour administrer le REDL;

c) toute licence nécessaire pour activer les fonctions de tous les éléments du REDL;

d) des services de maintenance et de soutien technique pour cinq ans tout d'abord sur tout l'équipement du REDL, conformément aux niveaux de service de maintenance établis.

(10) SPC se chargera de l'installation et du déploiement de tous les éléments du REDL.

(11) SPC administrera le REDL à l'aide des composants de commande et d'orchestration faisant partie du contrat.

2 VUE D'ENSEMBLE DE LA SOLUTION

2.1 Modèle du REDL

(12) Le modèle de service du REDL est illustré à la figure 1.

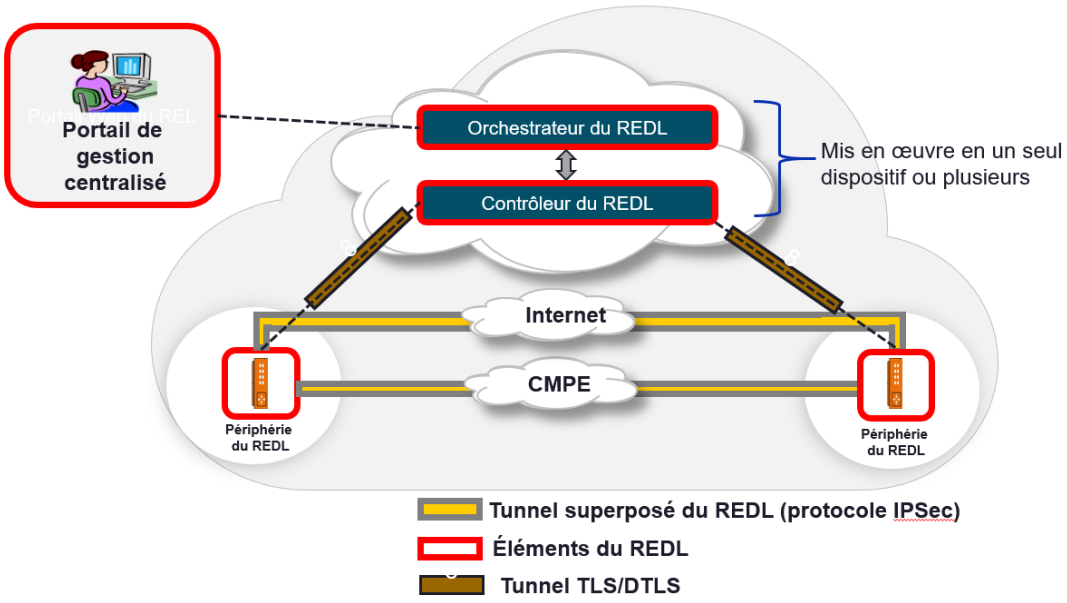

Figure 1 : modèle de service du REDL

2.2 Portée

(13) L'entrepreneur doit fournir une solution de REDL qui comprend au moins :

a) des périphériques matériels et logiciels;

b) le matériel et les logiciels de contrôle et d'orchestration mettant en œuvre une gestion centralisée;

c) les licences nécessaires;

d) la maintenance et le soutien technique.

(14) Les réseaux superposés eux-mêmes (MLPS, Internet large bande ou Ethernet câblé, par exemple) dépassent la portée de la solution recherchée.

2.2.1 Périphérique du REDL

(15) Un périphérique du REDL gère le routage de la couche données. Il prend des décisions de routage en fonction des politiques transmises par le contrôleur du REDL pertinent. Ces dispositifs sont le plus souvent installés sur place, dans les locaux du client.

2.2.2 Commande et orchestration du REDL

(16) Le service de commande et d'orchestration du REDL permet de le gérer, c'est-à-dire prestation du service, réglage des performances, utilisation, statistiques, sécurité et application des politiques. Il sert à configurer le service REDL de bout en bout entre les périphériques. Il fournit une capacité de gestion centralisée avec une grande variété de fonctionnalités pour la solutions REDL.incluant la création autorisée de politiques et l'attribution automatique de ressources et de bande passante pour des applications ou un type de données précis.

2.2.3 Licences

(17) En général, les solutions de REDL activent par licences les divers fonctions ou niveaux de fonctions et capacités des éléments qui le composent.

2.2.4 Maintenance et soutien

(18) On entend par services de maintenance et de soutien tout appui (matériel, logiciels, micrologiciels, abonnements et ressources) nécessaire pour la restauration après une panne, le bon fonctionnement continu et la maintenance préventive de tous les éléments du REDL.

3 APPROVISIONNEMENT DE LA SOLUTION

(19) L'entrepreneur devra fournir tout le matériel, tous les logiciels, toutes les licences et tout le soutien nécessaires pour répondre aux besoins décrits dans les présentes.

3.1 Configuration matérielle

(20) L'entrepreneur devra fournir les dispositifs matériels du REDL avec la configuration matérielle demandé pour que le Canada puisse déployer et utiliser les dispositifs du REDL livrés avec toutes les fonctionnalités requises identifiées dans le présent EDT.

(21) Les dispositifs de REDL fournis par l'entrepreneur doivent tous pouvoir être montés dans un bâti de 19 po.

(22) La solution de commande et d'orchestration du REDL fournie doit disposer des ressources matérielles voulues (modèle, processeur, mémoire vive et de masse) pour être en mesure de gérer au moins cinq cents périphériques, où chacun est connecté à au moins deux

contrôleurs du REDL. S'il faut plus d'un appareil pour mettre en place les fonctions de commande et d'orchestration du déploiement du REDL, l'entrepreneur doit fournir les appareils nécessaires en une unité intégrée et indiquer à l'annexe B le prix de celle-ci. L'entrepreneur doit décrire clairement à l'annexe C la configuration matérielle de tous les éléments de cette unité intégrée (modèle, processeur, mémoire vive et de masse, etc.).

(23) L'entrepreneur doit fournir des périphériques du REDL selon la figure 2 (configuraitons matérielles). Le dispositif d'accès REDL doit:

a) être fourni avec le matériel approprié (CPU, mémoire et stockage) pour prendre en charge les exigences SD-WAN identifiées dans le tableau 2 et la section 5.1 (échelonnabilité);

b) doit fournir un minimum de débit de plan de données, crypté avec le trafic IMIX et le pare-feu de niveau 4 activé;

c) prendre en charge un nombre minimal de dispositifs d'accès REDL dans la topologie de superposition spécifiée; et

d) soutenir un minimum de deux réseaux de transport indépendants.

(24) L'entrepreneur doit fournir des périphériques du REDL et les licences en conformité aux catégories suivantes (elles sont résumées à la figure 2, ci-dessous):

a) Catégorie 1 : périphériques de configuration matérielle suffisante (processeur, mémoire vive et stockage, etc.) pour fournir jusqu'à 200 Mbit/s de débit de plan de données crypté avec le trafic IMIX et le pare-feu de niveau 4 (basé sur des zones) activé. Chaque périphérique doit disposer d'au moins deux ports Ethernet gigabit pour sa connexion à un réseau local et deux ports Ethernet gigabit pour sa connexion à un réseau étendu. Un port de gestion hors bande doit être fourni. Chaque périphérique doit être livré avec un bloc d'alimentation redondant. Le dispositif d'accès doit prendre en charge un minimum de 50 dispositifs d'accès REDL avec deux connexions au réseau (e.g. MPLS et Internet) dans une topologie de superposition entièrement maillée.

b) Catégorie 2 : périphériques de configuration matérielle suffisante (processeur, mémoire vive et stockage, etc.) pour fournir jusqu'à 500 Mbit/s de débit de plan de données crypté avec le trafic IMIX et le pare-feu de niveau 4 (basé sur des zones) activé. Chaque périphérique doit disposer d'au moins deux ports Ethernet gigabit pour sa connexion à un réseau local et deux ports Ethernet gigabit pour sa connexion à un réseau étendu. Un des ports doit supporter 100 Mbit/s. Un port de gestion hors bande doit être fourni. Chaque périphérique doit être livré avec un bloc d'alimentation redondant. Le dispositif d'accès doit prendre en charge un minimum de 200 dispositifs d'accès REDL avec deux connexions au réseau (e.g. MPLS et Internet) dans une topologie de superposition entièrement maillée.

c) Catégorie 3 : périphériques de configuration matérielle suffisante (processeur, mémoire vive et stockage etc.) pour fournir jusqu'à 2 Gbit/s de débit de plan de données crypté avec le trafic IMIX et le pare-feu de niveau 4 (basé sur des zones) activé. Chaque périphérique doit disposer d'au moins quatre ports Ethernet gigabit pour sa connexion à un réseau local et quatre ports Ethernet gigabit pour sa connexion à un réseau étendu. Un port de gestion hors bande doit être fourni. Chaque périphérique doit être livré avec un bloc d'alimentation redondant. Le dispositif d'accès doit prendre en charge un minimum de 200 dispositifs d'accès REDL avec deux connexions au réseau (e.g. MPLS et Internet) dans une topologie de superposition entièrement maillée.

d) Catégorie 4 : périphériques de configuration matérielle suffisante (processeur, mémoire vive et stockage, etc.) pour fournir jusqu'à 10 Gbit/s de débit de plan de données crypté avec le trafic IMIX et le pare-feu de niveau 4 (basé sur des zones) activé. Chaque

périphérique doit disposer d'au moins huit ports Ethernet 10 gigabits : quatre pour réseau étendu et quatre pour réseau local ou étendu. Chaque périphérique doit être livré avec un bloc d'alimentation redondant. Un port de gestion hors bande doit être fourni. Le dispositif d'accès doit prendre en charge un minimum de 200 dispositifs d'accès REDL avec deux connexions au réseau (e.g. MPLS et Internet) dans une topologie de superposition entièrement maillée.

e) Périphériques virtuels REDL avec le logiciel nécessaire pour un débit allant jusqu'à 2 Gbit/s de trafic IMIX crypté et pare-feu de niveau 4 (basé sur des zones) activé

	Périphérique de catégorie 1	**Périphérique de catégorie 2**	**Périphérique de catégorie 3**	**Périphérique de catégorie 4**
Débit de chiffrement dans le plan de données avec pare-feu de niveau 4 (basé sur des zones) activé	200 Mbit/s	500 Mbit/s	2 Gbit/s	10 Gbit/s
Capacité et nombre de ports minimaux	2 ports Ethernet gigabit pour réseau local 2 ports Ethernet gigabit pour réseau étendu	2 ports Ethernet gigabit pour réseau local 2 ports Ethernet gigabit pour réseau étendu (1 port doit supporter 100 Mbit/s)	4 ports Ethernet gigabit pour réseau local 4 ports Ethernet gigabit pour réseau étendu	4 ports Ethernet 10 gigabit pour réseau local 4 ports Ethernet 10 gigabit pour réseau étendu
Nombre minimum de dispositifs d'accès REDL supportés	50	200	500	1000
Bloc d'alimentation redondant	Non	Oui	Oui	Oui
Port de gestion hors bande	Oui	Oui	Oui	Oui
Facteur de forme	1 unité de rack (maximum)	1 unité de rack	1 ou 2 unités de rack	1 ou 2 unités de rack

Figure 2: configurations matérielles

3.2 Périphériques

(25) Il incombe à l'entrepreneur de veiller à ce que les produits du REDL qu'il fournit respectent au minimum les fonctions et caractéristiques techniques décrites dans les présentes.

(26) Il lui incombe aussi de veiller à ne fournir que du matériel et des composants à l'état neuf, c'est-à-dire ni utilisés auparavant ni reconditionnés.

3.3 Commande et orchestration

(27) L'entrepreneur doit fournir un ensemble redondant de tout logiciel et / ou matériel de commande et d'orchestration nécessaire pour administrer le REDL proposé. En d'autres termes, si les fonctions de commande et d'orchestration du REDL exigent deux appareils distincts, un pour la commande, l'autre pour l'orchestration, l'entrepreneur doit fournir deux appareils pour chacune, assortis de tout logiciel et toute licence nécessaires pour que tout fonctionne comme prévu. La solution de commande et d'orchestration doit être configurable pour assurer au besoin sa haute disponibilité en modes actif-actif et actif-veille.

(28) L'entrepreneur doit prévoir une fonction de gestion centralisée du REDL; le Canada l'utilisera pour créer, surveiller et gérer tous les réseaux superposés du REDL et gérer toutes les licences pertinentes.

3.4 Licences

(29) L'entrepreneur doit fournir toutes les licences voulues pour activer les fonctions et la capacité nécessaires au respect de toutes les exigences du présent EDT, c'est-à-dire les licences du niveau le plus élevé voulu pour cela. Ces abonnements ou ces licences doivent être valides pendant au moins cinq ans à partir de la date de réception du matériel visé.

3.5 Fonctions de gestion et de sécurité

(30) Le REDL fourni par l'entrepreneur doit prendre en charge les fonctions suivantes de gestion et de sécurité :

a) réseaux étendus virtuels;
b) abstraction des réseaux;
c) gestion du trafic élastique;
d) optimisation du routage;
e) choix dynamique des voies;
f) routage en fonction des applications;
g) configuration des dispositifs à l'aide de modèles;
h) gestion de certificats;
i) gestion des éléments;
j) gestion des logiciels et application automatique des mises à jour;
k) statistiques sur le trafic et le rendement; et
l) gestion centralisée fondée sur les politiques.

(31) L'entrepreneur doit décrire en détail les fonctions de gestion et de sécurité que permettent les licences du REDL qu'il propose.

3.6 Maintenance et soutien

3.6.1 Soutien

(32) L'entrepreneur doit prévoir pour tous les éléments du REDL fournis des services de maintenance et de soutien valables pour cinq ans à partir au plus tôt de la date de livraison de chaque élément.

(33) L'entrepreneur devra être l'intermédiaire entre l'État et le FEO, et facilitera l'accès direct de l'État au soutien technique de celui-ci et à ses outils de soutien technique en ligne si l'État le demande afin d'assister le travail de ses propres ressources.

(34) Les services de maintenance et de soutien doivent comprendre au moins :

a) le soutien technique par téléphone, par courriel et sur la plateforme de soutien en ligne FEO;

b) l'accès aux correctifs de sécurité et aux mises à jour des micrologiciels visant les éléments du REDL diffusés sur la plateforme en ligne du FEO;

c) l'accès aux ressources didactiques et à la base de connaissances en ligne du FEO.

3.6.2 Entretien du matériel

(35) Durant toute la période de maintenance et de soutien, l'entrepreneur doit fournir un service de préautorisation de retour de marchandise (ARM) afin de remplacer tout matériel ne fonctionnant plus si le Canada l'en informe.

(36) L'entrepreneur doit par ce service remplacer tout matériel défectueux signalé par le Canada par un matériel identique au plus tard un jour ouvrable après en avoir été informé. Toute demande de remplacement d'un matériel ou d'une fonction identique provenant de l'entrepreneur doit être approuvée par le Canada.

4 SÉCURITÉ

4.1 ITSG-33

(37) Le Centre canadien pour la cybersécurité (CCC) a préparé à l'intention du Canada des lignes directrices sur la gestion des risques liés à la sécurité informatique (https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie). Elles orientent la mise en place des normes, politiques et lignes directrices en sécurité durant le cycle de vie du développement d'un système.

(38) L'entrepreneur doit fournir une solution REDL qui utilise des modules cryptographiques validés FIPS 140-2 niveau 1 et/ou FIPS 140-3 conformément à l'article ITSP.40.111 du CCCS. Les modules en cours d'examen par le NIST peuvent être acceptés, mais doivent figurer sur la liste publiée des modules en cours d'examen à l'adresse suivante https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list .

4.2 Généralités

(39) Le REDL fourni par l'entrepreneur doit intégrer une fonction centralisée de consultation de toutes les données sur la sécurité.

(40) La solution REDL fourni par l'entrepreneur doit intégrer un pare-feu de niveau 4 (basé sur des zones).

(41) La solution REDL fourni par l'entrepreneur doit permettre de séparer les réseaux en fonction de la zone, du type d'environnement, comme production, préproduction et essai, et par organisation (ministères et agences).

(42) La solution REDL fourni par l'entrepreneur doit permettre aux administrateurs de créer et de gérer des RAV ou des RPV pour séparer le trafic.

(43) La solution REDL fourni par l'entrepreneur doit permettre aux administrateurs de séparer et d'isoler virtuellement le trafic réseau selon les profils des locataires et les politiques de sécurité.

(44) La solution REDL fourni par l'entrepreneur doit intégrer la surveillance de la sécurité et la production de rapports pertinents en temps réel.

(45) La solution REDL fourni par l'entrepreneur doit acheminer l'enregistrement des événements de tous les dispositifs le constituant à un serveur de journalisation central hébergé dans les locaux du Canada.

(46) La solution REDL fourni par l'entrepreneur doit prendre en charge les listes de contrôle d'accès.

(47) La solution REDL fourni par l'entrepreneur doit prendre en charge la gestion centralisée des correctifs à appliquer aux périphériques du REDL et un portail de gestion afin de rester au fait des vulnérabilités rectifiées par le FEO (cela comprend les signatures antivirus et les mises à jour des micrologiciels).

4.3 Authentification

(48) La solution REDL fourni par l'entrepreneur doit prendre en charge la gestion des clés publiques pour les services de sécurité, notamment la sécurité de la couche de transport (TLS) et la sécurité du protocole Internet (IPSec).

(49) La solution REDL fourni par l'entrepreneur doit prendre en charge l'authentification des utilisateurs par le système de contrôle d'accès du contrôleur d'accès au terminal (TACACS+) pour contrôler l'accès des administrateurs aux dispositifs du REDL.

(50) La solution REDL fourni par l'entrepreneur doit permettre l'inscription et le renouvellement du certificat du dispositif manuellement.

(51) La solution REDL fourni par l'entrepreneur doit permettre l'inscription et le renouvellement du certificat du dispositif via des protocoles d'intégration PKI tels que Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) ou (Automatic Certificate Management Environment (ACME).

(52) La solution REDL fourni par l'entrepreneur doit permettre le renouvellement de l'autorité de certification PKI.

(53) La solution REDL fourni par l'entrepreneur doit permettre de dissocier un dispositif d'accès REDL (contenant un certificat invalide/révoqué) du réseau REDL.

(54) La solution REDL fourni par l'entrepreneur doit aussi utiliser les certificats sur tous les contrôleurs.

4.4 Gestion des comptes des utilisateurs

(55) La solution REDL fourni par l'entrepreneur doit intégrer les fonctions de gestion qui permettent à un administrateur de configurer l'accès, c'est-à-dire au moins les fonctions suivantes :

a) ajout, suppression, modification et configuration des comptes d'utilisateurs, aux fins d'administration d'un dispositif;

b) gestion des mots de passe de chaque utilisateur, y compris l'option d'authentification à deux facteurs;

c) ajout, suppression, modification et configuration de groupes d'utilisateurs, aux fins d'administration d'un dispositif;

d) ajout et suppression des comptes d'un groupe d'utilisateurs;

e) journalisation des changements apportés et création de rapports sur ceux-ci.

(56) La solution REDL fourni par l'entrepreneur doit prendre en charge le Contrôle de l'accès en fonction des rôles (CAFR) et l'authentification, l'autorisation et la traçabilité à l'aide de TACACS+, afin de restreindre les droits d'accès (consultation et configuration) par réseau

logique.

4.5 Couche de contrôle

(57) La solution REDL de l'entrepreneur doit protéger la confidentialité, l'intégrité et la disponibilité des communications de la couche de contrôle entre les contrôleurs REDLet les dispositifs d'accès à l'aide de la sécurité de la couche de transport (TLS/DTLS) ou de la sécurité IP (IPSec), comme le recommande le document ITSP.40.062 Conseils sur la configuration sécurisée des protocoles réseau (Version 2).

4.6 Couche de données

(58) La solution REDL de l'entrepreneur doit protéger la confidentialité, l'intégrité et la disponibilité du transport des données entre les dispositifs d'accès REDL à l'aide de la sécurité IP (IPSec), conformément aux recommandations du document ITSP.40.062 Conseils sur la configuration sécurisée des protocoles réseau (Version 2) incluant :

a) une association de sécurité IPSec (SA) doit être établie par IKEv2;

b) le protocole de sécurité d'encapsulation (ESP) doit être utilisé en mode tunnel;

c) la durée de vie de la clé de l'association de sécurité (SA) du protocole de sécurité d'encapsulation (ESP) ne doit pas dépasser 8 heures; et

d) la durée de vie de l'authentification SA IKEv2 ne doit pas dépasser 24 heures.

5 EXIGENCES TECHNIQUES

5.1 Échelonnabilité

(59) La solution REDL fourni par l'entrepreneur doit pouvoir prendre en charge jusqu'à 2 000 périphériques REDL du même FEO dans l'éventualité où le Canada ferait l'acquisition de dispositifs d'accès REDL supplémentaires dans le cadre d'achats ultérieurs.

(60) La solution REDL fourni par l'entrepreneur doit prendre en charge jusqu'à 16 RPV.

(61) La solution REDL fourni par l'entrepreneur doit prendre en charge jusqu'à 1000 dispositifs par RPV.

(62) La solution REDL fourni par l'entrepreneur doit prendre en charge au moins 200 dispositifs d'accès REDL avec deux connexions au réseau (e.g. MPLS and Internet) dans une topologie superposée entièrement maillée.

(63) La solution REDL fourni par l'entrepreneur doit prendre en charge au moins 50 000 connexions NAT par périphérique.

(64) La solution REDL fourni par l'entrepreneur doit intégrer des interfaces de capacité maximale de 10 Gbit/s.

(65) La solution REDL fourni par l'entrepreneur doit prendre en charge au moins 500 comptes d'utilisateurs avec une capacité de contrôle basée sur les rôles..

5.2 Déploiement

(66) La solution REDL fourni par l'entrepreneur doit prendre en charge le déploiement et la configuration des dispositifs par approvisionnement sans intervention.

(67) La solution REDL fourni par l'entrepreneur doivent prendre en charge les topologies suivantes sur ses réseaux superposés : en étoile, partiellement maillé, entièrement maillé et point à point.

(68) La solution REDL fourni par l'entrepreneur doit prendre en charge les configurations en pile double (IPv4 et IPv6).

(69) La solution REDL fourni par l'entrepreneur doit permettre aux administrateurs d'appliquer des modèles de configuration aux périphériques du REDL.

(70) La solution REDL fourni par l'entrepreneur doit permettre pour gérer les dispositifs à distance la gestion hors bande s'il est impossible de gérer un dispositif du REDL par gestion intrabande sur la couche de commande.

(71) Pour augmenter la disponibilité, la solution REDL fourni par l'entrepreneur doit prendre en charge le déploiement de périphériques multiples sans perdre d'autres fonctions, comme la visibilité des applications, la gestion du trafic et les fonctions de sécurité lorsqu'activées.

(72) La solution REDL fourni par l'entrepreneur doit permettre de distribuer des routes superposées de sorte qu'un chemin entre deux (2) dispositifs de bordure REDL puisse être réalisé via un ou plusieurs dispositifs d'accès REDL (par exemple, un VPN connecté à la dispositif d'accès A et au dispositif d'accès C peut traverser par le dispositif d'accès B).

5.3 Disponibilité

(73) La solution REDL fourni par l'entrepreneur doit permettre, pour assurer une haute disponibilité, de regrouper des contrôleurs géographiquement éloignés par le nuage et/ou la configuration sur place.

(74) La solution REDL fourni par l'entrepreneur doit fournir des périphériques du REDL prenant en charge le basculement quasi instantané à une voie de communication d'appoint connectée au même périphérique.

5.4 Capacité

(75) La solution REDL fourni par l'entrepreneur doit avoir la capacité d'identifier et de classer les flux de trafic des applications. Les critères de flux d'applications peuvent être définis à l'aide des éléments suivants:

a) Signatures d'applications prédéfinies pour les applications cloud/SaaS les plus populaires. Les signatures prédéfinies doivent pouvoir être mises à jour dynamiquement de façon régulière ; et

b) Critères de signature de l'application personnalisée comprenant un ou plusieurs des éléments suivants :

i) Adresse IP source et/ou destination (hôte ou préfixe IPv4/IPv6) ;

ii) Protocole IPv4 ou en-tête suivant IPv6 (registre des numéros de protocole de l'IANA);

iii) Source de transport et/ou port de destination (registre des noms de service et des numéros de port de l'IANA) ; et/ou

iv) Capacité heuristique/algorithmique sur le Uniform Resource Locator/Localisateur de Ressources Uniformes (URL) avec prise en charge des caractères génériques (par exemple, *.application.gc.ca).

(76) La solution SD-WAN de l'entrepreneur doit détecter et surveiller la latence, la gigue et la perte de paquets (par lien réseau).

(77) La solution REDL fourni par l'entrepreneur doit permettre la correction d'erreurs sans voie de retour (FEC) entre les dispositifs d'accès REDL.

(78) La solution REDL fourni par l'entrepreneur doit prendre en charge ainsi la surveillance des voies de communication et de la QdS :

a) routage dynamique du trafic sur une voie privilégiée, en fonction d'une politique ou du type d'application;

b) à l'aide de codes d'accès aux services différenciés (DSCP), mise en correspondance des classes de QdS des réseaux superposés avec les classes de QdS des réseaux sous-jacents;

c) prise en charge de jusqu'à cinq queues QdS, dont une queue

(79) La solution REDL fourni par l'entrepreneur doit acheminer le trafic vers la voie au rendement le plus élevé d'un site, en fonction des facteurs suivants : latence, gigue et la perte de paquets

(80) La solution REDL fourni par l'entrepreneur doit tenir compte de la nature asymétrique du service Internet DSL et par câble, et acheminer les données en conséquence pour respecter les politiques établies sur le profil de trafic.

(81) La solution REDL fourni par l'entrepreneur doit permettre à un administrateur d'appliquer par une seule commande et de façon centralisée des politiques à des dispositifs précis ou à tous les dispositifs du REDL.

(82) En fonction des politiques, la solution REDL fourni par l'entrepreneur doit réacheminer automatiquement le trafic d'applications moins prioritaires à d'autres voies pour maintenir le rendement des applications prioritaires, comme le trafic VoIP.

5.5 Gestion centralisée — interface graphique

(83) La solution REDL fourni par l'entrepreneur doit présenter un affichage centralisé de l'état du réseau et des incidents, et permettre de dépanner tous les réseaux logiques à partir d'une seule interface graphique mise en œuvre sur un portail accessible par un navigateur Web; ce portail doit présenter tant un tableau de bord général que des affichages détaillés qui permettent de surveiller et de configurer les paramètres suivants :

a) RPV : affichage et configuration de tous les tunnels RPV, y compris des statistiques sur les données entrantes et sortantes : état, gigue, latence et pourcentage de paquets perdus;

b) Ports : affichage et configuration de tous les ports des contrôleurs et des périphériques du REDL;

c) Applications : affichage de toutes les applications et de tous les groupes d'applications utilisées sur le réseau et du tunnel RPV qu'elles empruntent;

d) Politiques : affichage et configuration de toutes les politiques du REDL;

e) Liens : configuration sur demande de la topologie des réseaux, et affichage de l'état de tous les liens;

f) Profils de sécurité : affichage et configuration de tous les profils de sécurité.

(84) Le portail de la solution REDL fourni par l'entrepreneur doit prendre en charge de nombreux navigateurs accessibles librement, dont Microsoft Edge et Google Chrome.

(85) La solution REDL fourni par l'entrepreneur doit représenter visuellement les topologies physiques et logiques, y compris celles des sous-ensembles de dispositifs.

(86) La solution REDL fourni par l'entrepreneur doit prendre en charge la surveillance de toutes les connexions de commande entre les contrôleurs et les périphériques du REDL.

(87) La solution REDL fourni par l'entrepreneur doit prendre en charge la surveillance du fonctionnement de tout dispositif : état, trafic, température, pourcentage d'utilisation du

processeur, mémoire et bloc d'alimentation.

(88) La solution REDL fourni par l'entrepreneur doit permettre aux administrateurs de :

a) créer des groupes d'applications (des sous-ensembles de celles-ci) qu'un dispositif du REDL pourra détecter et surveiller;

b) fixer des mesures de rendement et les appliquer à une application ou à un groupe d'applications; et

c) créer des définitions adaptées de catégories d'applications.

(89) La solution REDL fourni par l'entrepreneur doit prendre en charge le contrôle d'accès fondé sur les rôles.

5.6 Gestion des politiques

(90) La solution REDL fourni par l'entrepreneur doit permettre aux administrateurs d'effectuer les tâches suivantes de façon centralisée :

a) création de politiques d'entreprise et application de celles-ci à tous les dispositifs du REDL;

b) création de politiques fondées sur les applications afin d'aiguiller dynamiquement le trafic en fonction des applications ou du type d'application (comme en temps réel, par transactions ou par lots);

c) création de profils fondés sur les voies, qui permettent de fixer les voies préférentielles en cas de dépassement de certains critères de QdS ou de dégradation ou panne d'un lien;

d) création de modèles servant à configurer de multiples dispositifs.

5.7 Protocoles

(91) La solution REDL fourni par l'entrepreneur doit prendre en charge les protocoles suivants :

a) Internet Protocol version 4 (IPv4) (RFC 791, RFC 2474);

b) Internet Protocol version 6 (IPv6) (RFC 2460);

c) Canalisation des ports à l'aide du protocole LACP (Link Aggregation Control Protocol) (802.1AX-2008, anciennement 802.3ad) ou d'une configuration);

d) Simple Network Management Protocol (SNMP, protocole de gestion de réseau simple), versions 2 et 3;

e) Network Address Translation (NAT, traduction d'adresses de réseau);

f) Border Gateway Protocol (BGP, protocole de passerelle frontière), ASN de 2,4 octets et BGP-Multiprotocol (BGP-MP));

g) Open Shortest Path First (OPSF, premier itinéraire ouvert le plus court) version 2, pour IPv4 et IPv6;

h) Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) et services de relais DHCP, notamment DHCP version 6 (avec et sans état), NAT64 et protocole SLAAC pour IPv6;

i) Protocol Independent Multicast (PIM, multidiffusion indépendante du protocole);

j) IETF IP flow information Export (IPFIX, exportation des données de trafic IP IETF) et/ou protocole Netflow version 9;

k) Network Time Protocol (NTP, protocole d'horloge réseau);

l) Virtual Router Redundancy Protocol (VRRP, protocole de redondance des routeurs virtuels);

m) IPSec (sécurité IP), notamment Encapsulating Security Payload (ESP, encapsulation sécurisée des données);

n) Link Layer Discovery Protocol (LLDP, protocole de découverte sur la couche Liaison) (802.1AB);

o) Internet Group Management Protocol (IGMP, protocole de gestion de groupe Internet).

5.8 Interfaces

(92) Les dispositifs de la solution REDL fourni par l'entrepreneur doivent au besoin prendre en charge les interfaces suivantes :

a) Ethernet conforme à la norme IEEE 802.3u 100 BASE-TX via l'auto-négociation 10/100/1000BASE-T ou Small Form-factor Pluggable (SFP) à 100 Mbps selon SFF INF-8074;

b) Gigabit Ethernet de 1000 Mbit/s, conforme aux normes IEEE 802.3ab;

c) 10 Gigabit Ethernet de 10 000 Mbit/s, conforme aux normes IEEE 802.ae et IEEE 802.3-2008an;

d) Small form-factor pluggable (SFP, modules enfichables à faible encombrement) de 1000 Mbit/s, conformes à la norme SFF INF-8074;

e) SFP de 10 000 Mbit/s, conforme à la norme SFF 8431 4.1.

(93) La solution REDL fourni par l'entrepreneur doit prendre en charge de nombreux types de réseaux sous-jacents, notamment MPLS, Internet à large bande et Internet par câble.

5.9 Ressources infonuagiques

(94) La solution REDL fourni par l'entrepreneur doit pouvoir communiquer avec de nombreux logiciels-service, plateformes-service et infrastructures-service dans un environnement multinuagique. Il doit au moins pouvoir accéder à de multiples services infonuagiques, notamment AWS (Amazon Web Services), Microsoft Azure et Microsoft 365.

(95) La solution REDL fourni par l'entrepreneur doit prendre en charge l'optimisation des voies de communication pour les applications infonuagiques, détecter les types de trafic infonuagiques comme Office 365 et aiguiller ce trafic vers les voies optimales établies par les politiques.

(96) La solution REDL fourni par l'entrepreneur doit distinguer les applications et le trafic des logiciels-service et ceux des infrastructures-service faisant partie des applications infonuagiques, comme les flux multimédias de MS Teams.

5.10 Interfaces applicatives (API) prises en charge

(97) La solution REDL fourni par l'entrepreneur doit prendre en charge les interfaces applicatives de transfert d'état représentationnel (en anglais, RESTful APIs) et les interfaces applicatives ouvertes.

(98) La solution REDL fourni par l'entrepreneur doit permettre l'intégration et l'automatisation à l'aide d'interfaces applicatives, au minimum dans les catégories suivantes :

a) Gestion : intégration à des systèmes externes de surveillance, d'approvisionnement, de gestion de l'inventaire et de gestion du changement;

b) Infonuagique : développement d'interfaces vers les plateformes infonuagiques à l'aide de langages de programmation.

5.11 Rapports et statistiques

(99) La solution REDL fourni par l'entrepreneur doit surveiller le trafic, et mesurer et présenter des rapports statistiques sur les liens comprenant au moins les mesures suivantes : latence, perte de paquets, gigue, capacité et utilisation du lien, temps de parcours total et taux d'erreurs.

(100) La solution REDL fourni par l'entrepreneur doit mesurer les caractéristiques de rendement des applications des utilisateurs, comme le temps de réponse, le taux d'erreurs et le délai des transactions.

(101) La solution REDL fourni par l'entrepreneur doit pouvoir présenter des rapports sur la QdS : fonctions de classification, de marquage, de mesure, d'abandon, de mise en queue et d'ordonnancement.

(102) La solution REDL fourni par l'entrepreneur doit présenter un aperçu de l'utilisation générale de la capacité par chaque lien de réseau étendu, y compris le cumul des octets envoyés et reçus.

(103) La solution REDL fourni par l'entrepreneur doit présenter un affichage géographique montrant en temps réel l'état de tous les dispositifs et liens le composant.

(104) La solution REDL fourni par l'entrepreneur doit prendre en charge l'affichage graphique des données sur le trafic des applications.

(105) La solution REDL fourni par l'entrepreneur doit pouvoir afficher l'état de chacun des ports d'un dispositif du REDL.

(106) La solution REDL fourni par l'entrepreneur doit pouvoir produire un rapport sur toutes les politiques, dont celles de sécurité, appliquées à un dispositif du REDL ou à un groupe de dispositifs.

(107) La solution REDL fourni par l'entrepreneur doit pouvoir produire des rapports de sécurité comme rapports de journalisation, alertes de sécurité, événements des pare-feu, etc.

(108) La solution REDL fourni par l'entrepreneur doit pouvoir produire des rapports sur le rendement par locataire et site, qui comprennent des fonctions d'analyse par locataire et site comme applications les plus gourmandes en capacité, applications où la latence ou la gigue est la plus élevée, liens les plus utilisés, site ou dispositifs ne respectant pas les ENS, etc.

(109) La solution REDL fourni par l'entrepreneur doit permettre de créer des rapports adaptés aux besoins.

(110) La solution REDL fourni par l'entrepreneur doit pouvoir présenter au besoin des rapports antérieurs, notamment quotidiens, hebdomadaires ou mensuels.

DOCUMENTS CONNEXES

ANNEXE B — LISTE DES PRODUITS LIVRABLES ET DE LEUR PRIX

ANNEXE C — CRITÈRES D'ÉVALUATION TECHNIQUES