NON CLASSIFIÉ

Stratégie en matière de réseau et de sécurité

Architecture de réseau et de sécurité
Habilitation numérique
Direction générale du dirigeant principal de la technologie

Version : 1.9

Shared Services Canada | Services partagés Canada

Canada

Approbations du document

Don Messier Directeur général Habilitation numérique, Direction générale du dirigeant principal de la technologie Services partagés Canada	Date
Raj Thuppal Dirigeant principal de la technologie Direction générale du dirigeant principal de la technologie Services partagés Canada	Date
Patrice Nadeau Sous-ministre adjoint Direction générale des réseaux, de la sécurité et des services numériques Services partagés Canada	Date

Registre des modifications du document

Version	Date de publication	Auteurs	Description du changement
0.1	13 mai 2020	C. Johnson, K. Galbraith, Q. Walajahi, B. McKittrick, C. Parsons, Deloitte	Création du document initial
1.0	19 mai 2020	Chris Johnson	Mises à jour, après l'examen par l'équipe interne
1.1	28 mai 2020	Chris Johnson	Mises à jour, examen par le directeur
1.2	26 juin 2020	Chris Johnson	Mises à jour/modifications apportées en fonction des commentaires reçus après l'examen
1.3	3 juillet 2020	Chris Johnson	Mises à jour en fonction des commentaires du Secrétariat du Conseil du Trésor du Canada (SCT), du Centre de la sécurité des télécommunications Canada (CST), de Services partagés Canada (SPC) et de l'équipe interne. Rétroaction donnée par : - Chris Wharram, RSSN, SPC - Po Tea-Duncan, SCT - Mario Lefebvre, CCC, CST
1.4	14 juillet 2020	Chris Johnson	Révisions internes de l'équipe de l'habilitation numérique
1.5	1er septembre 2020	Chris Johnson et Brian McKittrick	Mises à jour en fonction des commentaires du DPT et du DG.
1.7	23 octobre 2020	Chris Johnson	Mises à jour après l'examen des rédacteurs techniques et des autres intervenants, dont : - Michel Fortin, RSSN, SPC - John Bain, AE, DGDPT, SPC - Marty Gratton, RSSN, SPC
1.8	20 novembre 2020	Chris Johnson	Mises à jour en fonction des commentaires internes de l'équipe de l'habilitation numérique
1.9	5 février 2021	Chris Johnson	Modifications et révision à la suite de la révision de Gartner

Table des matières

Résumé

Le gouvernement du Canada (GC) est sur le point d'entreprendre l'une de ses plus grandes transformations technologiques depuis des décennies alors qu'il entame le processus de consommation de services en nuage du point de vue informatique et logiciel. Ces exigences de transformation sont similaires à celles observées dans l'ensemble de l'industrie. Des secteurs comme les chaînes de vente au détail, les banques et les chaînes d'hôtels entreprennent tous de transformer de manières comparables le réseau et la sécurité afin de tirer parti des avantages de l'utilisation de solutions en nuage pour soutenir leurs principales activités. La tâche est d'autant plus difficile pour SPC qui doit soutenir une grande variété d'organisations (plus de 40). En raison de cette diversité, Services partagés Canada (SPC) doit axer sa stratégie en matière de réseau et de sécurité sur les exigences qui sont communes à toutes les organisations dans ces domaines.

Aujourd'hui, on s'attend généralement à pouvoir être en ligne en tout temps, quelles que soient la demande ou les circonstances, car presque tous les employés du gouvernement doivent compter sur la technologie de l'information (TI) pour offrir leurs services. La diversité des services reposant sur la connectivité d'un réseau sécurisée est également en pleine expansion. Au cours des dernières années, l'utilisation des services infonuagiques, d'Internet, des services de collaboration, de vidéoconférence, de cyberconférence et d'accès à distance protégé a explosé dans l'ensemble du GC. Il sera vraiment important d'offrir une infrastructure de réseau dont la rapidité, la sécurité et la fiabilité seront accrues, car les services actuels et nouveaux devraient poursuivre leur croissance à l'avenir.

Des événements récents ont sensibilisé les gens au besoin d'encourager la souplesse des exigences de travail pour aider un pourcentage élevé d'employés en télétravail qui utilisent d'autres options d'accès à distance.

L'utilisation croissante de ces nouveaux services en nuage augmentera la surface d'attaque de l'infrastructure et des applications gouvernementales. C'est pour cette raison que SPC doit revoir la façon d'aborder la prestation des services de réseau et de sécurité pour aider les ministères et organismes du GC à offrir leurs services à la population canadienne.

Les principaux facteurs opérationnels de la version à jour de la stratégie en matière de réseau et de sécurité de SPC sont les suivants :

- augmenter l'efficacité opérationnelle de la prestation et de la gestion des services de réseau et de sécurité à compter de maintenant;
- définir une plateforme de réseau qui procure une mobilité transparente à l'utilisateur final, en tout temps et n'importe où à partir d'appareils approuvés par le GC, en accordant une attention particulière à l'accès à distance protégé (ADP) et au télétravail;
- améliorer la posture de sécurité globale des services de réseau;
- augmenter les performances du réseau pour mettre en place la prochaine génération de services de réseau;

- améliorer la résilience de la plateforme de l'ensemble du réseau, réduisant ainsi le nombre d'incidents et de pannes;
- définir une approche axée sur des normes ouvertes en ce qui a trait à l'état du réseau à l'avenir, réduisant ainsi la dépendance aux fournisseurs;
- prolonger le cycle de vie des biens actuels en optimisant les cycles d'actualisation des biens de TI;
- améliorer la gérance de la sécurité en offrant une visibilité et un contrôle des biens et des services du réseau;
- mettre en œuvre les principes fondamentaux permettant l'adoption progressive du concept de réseau en tant que service (NaaS).

Le besoin d'établir une stratégie révisée devient d'autant plus évident lorsqu'on examine les données qui traversent les réseaux gouvernementaux : des renseignements personnels que possède l'Agence du revenu du Canada (ARC) sur chaque Canadien et Canadienne, des renseignements sur les services de police de la Gendarmerie royale du Canada et bien plus encore. La venue d'acteurs parrainés par des États étrangers qui mènent des attaques sophistiquées contre les biens gouvernementaux oblige le gouvernement canadien à entreprendre une refonte fondamentale de la manière de protéger ses réseaux et d'acheminer les données aux employés et à la population canadienne.

Les activités futures de conception et de prestation des services de réseau exigeront également que SPC adopte une approche différente en matière de sécurité. Les organisations du monde entier évoluent vers un nouveau modèle de sécurisation du réseau basé sur le principe qui consiste à « *ne pas faire confiance, mais vérifier* », qu'on appelle architecture zéro confiance (ZTA). La ZTA modifie le paradigme de sécurité qui consistait auparavant à « protéger le périmètre » (appelé aussi l'approche « château et douves ») pour le remplacer par l'idée plus récente qui vise à protéger le flux de données de bout en bout, soit de l'utilisateur à l'application.

SPC actualise présentement sa stratégie en matière de réseau et de 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 technologies, comme l'infonuagique, Internet des objets (IdO) et les services de réseau cellulaire numérique de 5e génération (5G), sont des exemples de technologies émergentes auxquelles l'infrastructure gouvernementale doit s'intégrer. Ces tendances technologiques obligeront SPC à repenser la manière dont il conçoit, fournit, gère et sécurise ses services de réseau et à être suffisamment agile pour intégrer toute technologie jugée nécessaire aux opérations gouvernementales.

Pour élaborer cette stratégie en matière de réseau et de sécurité, de nouvelles approches, axées sur l'automatisation, une infrastructure définie par logiciel (IDL) et un concept de zéro confiance, sont nécessaires. Les piliers fondamentaux énoncés dans le présent document représentent la base de ces nouvelles approches et constituent le point central de cette stratégie.

Les piliers fondamentaux sont les suivants :

1. **Connectivité** : il s'agit des composants technologiques (commutateurs, routeurs, pare-feu, équilibreurs de charge, etc.) qui composent la structure des réseaux de SPC et couvrent l'accès interne et externe à ces réseaux;
2. **Contrôle d'identité et d'accès** : il s'agit de l'authentification et l'autorisation nécessaires pour que les utilisateurs puissent interagir, à l'aide de leurs appareils, avec les ressources du GC et s'y connecter;
3. **Surveillance** : il s'agit des besoins en surveillance continue liés à la fois aux performances et à la sécurité afin d'activer les différentes capacités de surveillance qui générera une réponse automatisée.

Il est également important d'adopter une nouvelle **approche en matière d'approvisionnement** afin de nous adapter aux progrès technologiques et de répondre aux attentes des utilisateurs en matière de prestation de services au moment opportun. Les utilisateurs s'attendent à ce que les services soient offerts dans les quelques heures ou jours qui suivent, et non quelques semaines ou mois plus tard. Un facteur clé de l'approche consiste à miser sur l'IDL pour mettre en place une infrastructure de réseau et de sécurité.

Cette recommandation repose sur la nécessité de compter sur des compétences évoluées dans des domaines comme la gestion infonuagique, la sécurité infonuagique, l'intelligence artificielle, la réseautique, la sécurité et l'automatisation. SPC devra réfléchir à la manière dont il peut créer une proposition de valeur capable d'attirer des compétences précieuses et de les conserver.

La stratégie en matière de réseau et de sécurité définit l'approche que SPC devra adopter pour permettre au gouvernement de répondre aux demandes d'aujourd'hui et de s'adapter aux demandes de demain en misant sur une stratégie globale d'adoption et de migration progressive.

Pour mettre cette stratégie en œuvre, les principes stratégiques suivants sont recommandés :

1. Veiller à ce que des orientations soient fournies pour les projets existants et à venir et à ce qu'ils ne soient pas réalisés en vase clos, mais réalisés en gardant à l'esprit tous les services axés sur la vision et la stratégie en matière de réseau et de sécurité.
2. Acquérir les capacités fondamentales essentielles afin d'assurer une mise en œuvre rapide pour ensuite en définir la priorité et l'ordre. Quelles initiatives permettront à SPC d'atteindre l'état final souhaité?
3. Ne pas essayer de mettre en place une solution tout-en-un. Il s'agira d'une évolution à partir des projets actuels et des cycles de renouvellement, en commençant à petite échelle et en utilisant la technologie dont SPC dispose déjà.
4. Envisager d'investir dans l'automatisation et l'orchestration de la technologie que SPC prend déjà en charge.

5. Répondre au besoin d'intégration entre les fonctions de sécurité et de réseau dès le début en tant qu'activité primordiale de gestion des changements.
6. Combler le manque de compétences au sein de la main-d'œuvre afin de suivre l'évolution constante des technologies et des besoins en matière de compétences (comme la programmation).

1.1. Connectivité

Les bases de ce pilier comprennent les composants technologiques (commutateurs, routeurs, pare-feu, équilibreurs de charge, etc.) qui composent la structure des réseaux du GC et couvrent l'accès interne et externe à ces réseaux. SPC verra plusieurs technologies émergentes devenir un élément majeur de sa stratégie de connectivité à l'avenir :

- Le réseau cellulaire de 5e génération (5G) est sur le point de transformer profondément la manière dont les services de réseau sont fournis aux consommateurs et aux entreprises. La 5G présente une bande passante (capacité) nettement plus élevée et une latence plus faible que les anciennes technologies sans fil, telles que la 4G ou la LTE.
- Les services d'accès à distance repensés visent à mieux prendre en charge les concepts d'accès au réseau partout et à tout moment et évoluent dans le lieu de travail moderne.
- Un accès sécurisé à haute vitesse et à faible latence aux services infonuagiques est rendu possible grâce au programme Activation et défense du nuage sécurisé (ADNS) de SPC.
- De nouvelles façons d'offrir un accès aux services de réseau étendu (RE) du GC et Internet mises en œuvre sur un RE défini par logiciel (REDL, ou REL).
- Les technologies de réseau local (RL) défini par logiciel (RLDL, ou RLL) permettront l'instanciation efficace et opportune de nouveaux lieux de travail et la segmentation efficace des différents réseaux d'utilisateurs du GC.

L'intégration progressive de ces technologies, en particulier des technologies émergentes, jettera les bases du réseau « prospectif » que SPC cherche à créer.

1.2. Contrôle d'identité et d'accès

Le contrôle d'identité et d'accès fait référence à l'authentification et à l'autorisation nécessaires afin que les utilisateurs puissent interagir, à l'aide de leurs appareils, avec les ressources technologiques du GC et s'y connecter. Le contrôle d'identité et d'accès s'intégrera à la ZTA pour transformer fondamentalement la façon dont les plateformes et les données sont sécurisées. Dans le modèle de ZTA, tout le monde est vu comme une menace, jusqu'à preuve du contraire. Le principal avantage de ce cadre est qu'il permet aux organisations de sécuriser les utilisateurs internes et externes sur l'ensemble du réseau. La complexité tient au fait que ce modèle oblige SPC à repenser fondamentalement le réseau central et les composants technologiques et à consolider les services d'identité au sein des réseaux du GC dans le but d'adopter une identité unique pour les employés et une autre pour les utilisateurs externes.

1.3. Surveillance

La surveillance continue et sa façon de répondre aux besoins en performance et en sécurité signifient les services de réseau de l'avenir devront également présenter différentes capacités en surveillance. SPC devra adopter un ensemble d'outils pour surveiller son réseau, sa plateforme et ses actifs de données de manière efficace. Cela comprendra la manière dont SPC exploite les produits des fournisseurs de technologies en nuage et des tiers pour créer un bassin de données en vue de l'analyse prédictive des menaces, des performances et des défis sur le plan de la disponibilité. En tirant parti de plateformes comme les plateformes d'intelligence artificielle pour les opérations informatiques (AIOps), SPC sera en mesure d'obtenir des renseignements précieux et de générer une réponse automatisée aux incidents. L'infrastructure définie par logiciel et le réseau défini par logiciel (IDL/RDL) serviront de catalyseur essentiel pour l'adoption des AIOps.

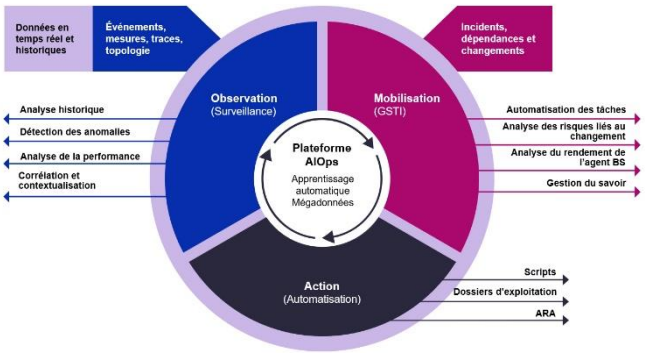


Figure 1 : Plateforme d'AIOps donnant des aperçus continus des opérations et de la surveillance de la TI

1.4. Approche en matière d'approvisionnement

Le gouvernement du Canada doit adapter la façon dont il répond présentement à ses besoins en infrastructure afin de s'adapter aux progrès technologiques et aux attentes des utilisateurs en matière de prestation de services en temps opportun. Les ministères partenaires s'attendront de plus en plus, compte tenu des offres publiques comparables, à ce que les services soient fournis en quelques heures et non en plusieurs semaines ou plusieurs mois. SPC devra tirer parti de l'IDL et du RDL pour permettre la fourniture de ressources de réseau afin de répondre aux demandes attendues.

La stratégie en matière de réseau et de sécurité définit l'approche que SPC devra adopter pour permettre au gouvernement de répondre aux demandes d'aujourd'hui et de s'adapter aux demandes de demain en misant sur une stratégie globale d'adoption et de migration progressive. Pour mettre cette stratégie en œuvre, SPC devra définir un ensemble cohérent d'exigences et d'architectures de référence pour les technologies et les cadres habilitants qui sont définis dans le présent document. Il devra également accélérer l'acquisition de produits et de services pour réaliser la stratégie.

2. Introduction

2.1. But

Le présent document a pour but de présenter plus en détail la *Vision d'avenir en matière de réseau et de sécurité de SPC*, qui établit la vision de SPC pour l'avenir, décrivant essentiellement l'intégration de l'IDL et de la ZTA. Dans le présent document, on tentera d'expliquer ce principe et d'examiner la stratégie et la feuille de route que SPC devrait adopter pour améliorer les services de réseau et de sécurité, faire face aux tendances émergentes en matière de technologie et de sécurité, et rendre opérationnels les principes énoncés dans l'approche d'entreprise SPC 3.0.

Ce document a été élaboré en tirant parti d'un certain nombre de contributions clés tant au sein de SPC qu'au sein du GC en général, des tendances en matière de sécurité et des pratiques émergentes, ainsi qu'en menant des entrevues avec des intervenants de SPC et du Secrétariat du Conseil du Trésor du Canada (SCT).

2.2. Public cible

Le public cible de ce document comprend le Comité tripartite sur la sécurité de la TI, les dirigeants principaux de l'information (DPI) des ministères et organismes gouvernementaux, les membres de la haute direction du Centre canadien pour la cybersécurité (CCC) et les secteurs de service de SPC.

3. Justification de la stratégie

Compte tenu de l'évolution rapide dans le domaine des infrastructures technologiques, SPC doit pouvoir compter sur une nouvelle approche afin de gérer et d'exploiter le réseau et l'environnement de sécurité de SPC. L'approche actuelle ne pourra pas être adaptée pour répondre à ces demandes. Il est difficile pour la main-d'œuvre de suivre le rythme de ces changements, car les progrès technologiques dépassent les compétences disponibles requises.

Non seulement la technologie évolue-t-elle trop rapidement pour suivre les progrès, mais de nouveaux vecteurs de menaces et des atteintes à la sécurité surviennent si souvent que le personnel informatique ne peut réagir assez rapidement pour y remédier. La mobilité et la connectivité accrues des utilisateurs en dehors du centre de données physique se prêtent à un confinement encore plus difficile du point de vue de la sécurité, sans parler de la migration des charges de travail vers le nuage public, ce qui complique encore plus les choses. Le personnel de TI est incapable de répondre assez rapidement, car il ne dispose pas des bons renseignements pour prendre des décisions éclairées. Une meilleure surveillance englobant une collecte de données plus vaste (concernant les événements de sécurité, les événements du réseau, la gestion de l'identité et de l'accès, les paramètres de performances du réseau) est nécessaire pour assurer une visibilité suffisante dans toute l'entreprise.

Dans l'ensemble, la TI est devenue beaucoup plus complexe. Cette complexité accrue a eu des répercussions négatives sur les délais de prestation des services pour les clients de SPC en plus d'avoir réduit les niveaux de service de façon générale. Le personnel des opérations de TI doit constamment apprendre à utiliser de nouveaux logiciels et outils pour suivre le rythme des progrès technologiques. Le taux élevé de changement a entraîné, et continue d'entraîner, des risques accrus liés à l'effort manuel demandé, érodant ainsi davantage la fiabilité des services de SPC pour ses clients.

Pour relever ces défis, de nouvelles approches axées sur l'automatisation, l'IDL et un concept de zéro confiance sont nécessaires. Les piliers décrits dans la section 1 serviront de base à ces approches et seront le point central du présent document de stratégie.

Le présent document consacré à la stratégie en matière de réseau et de sécurité pour l'avenir fait suite au document sur la vision d'avenir du GC en matière de réseau et de sécurité de Services partagés Canada (SPC) et s'inscrit dans l'approche d'entreprise SPC 3.0 et le plan stratégique des opérations numériques du gouvernement du Canada (GC) de 2018-2022[1]. Il s'agit d'une description dynamique et stratégique de l'orientation pour l'avenir du réseau et de la sécurité au sein du GC. La stratégie décrite est une étape essentielle vers la réalisation par le GC de ses objectifs à long terme en matière de gouvernement numérique grâce à l'élaboration d'une « infrastructure technologique moderne, durable, fiable et solide [qui] favorise la prestation de services numériques, la collaboration et la communication d'information de façon horizontale

[1] https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plan-strategique-operations-numerique-2018-2022.html

au sein du gouvernement et avec les citoyens, les entreprises externes, les intervenants et les partenaires. »

La stratégie présente un état futur et une feuille de route qui permettront à SPC d'évoluer pour devenir une organisation de prestation de services moderne et dotée des meilleures technologies et pratiques pour répondre aux besoins futurs des ministères partenaires du GC.

4. Facteurs opérationnels et autres défis

SPC offre une gamme de services aux ministères et organismes du GC. L'organisation joue un rôle clé dans la capacité du GC d'offrir un réseau numérique sécurisé qui permet une expérience utilisateur positive. Dans le tableau ci-dessous, on présente la liste des principaux facteurs d'une stratégie en matière de réseau et de sécurité moderne qui prend en charge les demandes émergentes du gouvernement numérique. Tous sont essentiels, alors il n'y a pas d'ordre particulier (hiérarchisation, dépendances ou mise en œuvre). Certains facteurs sont plus pertinents pour SPC, alors que d'autres le sont davantage pour le GC; cela est indiqué entre parenthèses dans la colonne Facteurs opérationnels.

N°	Facteurs opérationnels	Description
1	Mobilité transparente de l'utilisateur final (GC)	Permet aux utilisateurs de se connecter de façon sécuritaire, transparente et simple au réseau de leur ministère et à Internet ou au nuage. Accès en tout temps et n'importe où à partir n'importe quel appareil approuvé par le GC.
2	Sécurité accrue (GC)	Assure que les biens du GC sont dûment protégés et que les connexions réseau du GC à l'Internet ou au nuage sont surveillées de manière convenable.
3	Performances améliorées du réseau (GC)	Prend en charge les demandes existantes et émergentes de bande passante et permet d'y répondre rapidement. Augmente la fiabilité en réduisant le temps de panne et la dégradation de la performance.
4	Résilience du réseau (GC)	Permet la réparation spontanée, la récupération automatique et l'automatisation afin de créer un réseau plus résilient.
5	Encourager davantage le travail à distance (GC)	Compte tenu de la situation actuelle, permet au plus grand nombre d'employés à ce jour de travailler à distance.
6	Efficience opérationnelle (SPC)	Réduit les efforts manuels et les frais généraux, élabore des solutions évolutives pour réduire le délai de livraison, intègre les équipes et élimine le cloisonnement.
7	Gérer la dépendance envers des fournisseurs (SPC)	Favorise une transition vers une indépendance de tout fournisseur grâce à l'adoption de normes ouvertes.

8	Prolonger le cycle de vie des biens existants (SPC)	Optimise les cycles de renouvellement des biens de TI.
9	Gérance de la sécurité (SPC, SCT, CCC et autres ministères et organismes)	Procure une visibilité et un contrôle sur les biens et les services du réseau.

Tableau 1 – Facteurs opérationnels

Les facteurs opérationnels énumérés ci-dessus comprennent certaines des principales forces motrices de la transformation numérique du GC et de la TI en général. Pour que SPC puisse planifier sa stratégie de réseau, il est important de comprendre les tendances qui mènent au changement dans le domaine de la TI. Le plan stratégique des opérations numériques mentionné ci-dessus doit reposer sur ces premières étapes et tracer la voie à suivre. Le présent document consacré à la stratégie en matière de réseau et de sécurité doit correspondre aux facteurs de changement et aux défis qui ont été considérés comme faisant partie de la base de la vision stratégique, des normes numériques et des mesures de suivi déterminées dans le plan stratégique des opérations numériques.

N°	Autres défis	Description
1	Vieillissement de l'effectif	Diminution du nombre de ressources humaines disponibles.
2	Concurrence au niveau des ressources	Ressources qualifiées recherchées par le secteur privé, ce qui limite encore davantage leur disponibilité.
3	Problèmes de conformité	Obstacles à l'adoption rapide des technologies en évolution (comme les services en nuage).
4	Processus désuets	Incapacité pour les cycles d'approvisionnement du gouvernement de suivre le rythme des perturbations et des innovations technologiques.

Tableau 2 – Autres défis

À l'instar des facteurs opérationnels, les autres défis représentent des obstacles véritables et importants au succès de cette initiative. Contrairement aux facteurs opérationnels, les autres défis sont moins tangibles que les problèmes techniques; la dotation, la conformité et les processus contribueront d'autant plus à la réussite de ce projet, mais puisque ces questions relèvent de la catégorie des personnes et des processus, elles peuvent avoir une incidence davantage politique et donnant ainsi lieu à des exigences particulières.

5. État actuel de la réseautique et de la sécurité au GC

Le réseau du GC comprend une cinquantaine de réseaux logiques, couvrant environ 4 000 sites et 5 000 édifices. Il rejoint plus de 400 000 utilisateurs au Canada et à l'étranger. Comme on pouvait s'y attendre, ce réseau comprend de nombreux appareils physiques, fournisseurs et niveaux d'intégration différents. Les configurations ont été principalement effectuées manuellement par des ingénieurs système et des opérateurs au sein de SPC et d'autres ministères, ce qui peut entraîner certaines incohérences dans les configurations. Ce manque de cohérence a entraîné des problèmes de gestion, une baisse de la fiabilité et une surcharge opérationnelle élevée. Les modifications apportées à l'infrastructure et aux logiciels du réseau et de la sécurité sont lentes et coûteuses, nécessitant souvent le remplacement de matériel de la mauvaise taille ainsi que des remaniements du fait de son inadéquation avec la vision à long terme. La situation est également impossible à gérer puisqu'on doit ajuster la technologie et la topologie actuelles du réseau pour que les services infonuagiques modernes soient en mesure de répondre à la demande sur les plans de l'agilité et de la souplesse. Il y a aussi des coûts associés à ces inefficacités :

« Une étude récente de Gartner[2] a permis d'établir que le modèle de réseau et de sécurité de SPC est coûteux à exploiter, car son coût est supérieur de 19 % ou 427 millions de dollars par rapport à celui de ses pairs. »

Le concept de réseau repose sur des modèles de sécurité traditionnels, comme la notion de périmètre sécurisé. Dans ce concept, la plupart des efforts de sécurité visent à défendre le périmètre. Cette façon de faire a bien fonctionné par le passé lorsqu'il n'y avait qu'une seule « porte à défendre » : essentiellement la « porte » du centre de données. Aujourd'hui, cependant, il existe de nombreuses « portes à défendre », incluant, entre autres :

- les appareils sans fil et mobiles;
- l'infrastructure infonuagique publique;
- les sites éloignés;
- les centres en région.

Il est également important de surveiller les cybermenaces au sein même de l'organisation, car les organisations sont de plus en plus souvent victimes de menaces internes, par exemple, lorsqu'un utilisateur télécharge un fichier infecté (par inadvertance) ou si un employé mécontent exfiltre des données (intentionnellement). Un exemple bien connu est l'atteinte à la protection des données à Desjardins[3], qui a entraîné la fuite de renseignements personnels de plus de 4,2 millions de membres.

---

[2] *Rapport d'examen parrainé par SPC – Gartner 2018*

[3] *4.2 million Desjardins members affected by data breach, credit union now says | CBC News (en anglais seulement)*

Le manque d'uniformité dans la surveillance des dispositifs et le fait que les équipes techniques travaillent de manière cloisonnée s'ajoutent aux couches de complexité qui nuisent à la résolution rapide et rentable des problèmes. Compte tenu de la croissance continue de l'intégration interdomaine au sein des technologies, l'ancien modèle d'équipes cloisonnées s'avérera incompatible avec ce nouveau paradigme. Les équipes d'ingénierie, de sécurité et de soutien doivent collaborer afin de répondre à ces nouvelles demandes de services de réseau et de sécurité de l'avenir. L'intégration interdomaine a également des répercussions sur la formation, ce dont on doit tenir compte au moment d'élaborer les plans de formation. Le rôle d'« ingénieur hybride » fait son apparition. Cette personne aura une compréhension approfondie des nouveaux modèles de consommation pour le réseau, la sécurité et les opérations. Elle possédera donc de nouvelles compétences essentielles pour mettre en œuvre avec succès la prochaine génération d'infrastructures de réseau et de sécurité.

Une autre exigence clé concerne la visibilité en temps réel de l'état du réseau et de la sécurité de l'infrastructure au grand complet. La surveillance continue est fondamentale pour comprendre non seulement les données historiques en matière d'examen judiciaire et d'analyse des tendances, mais aussi l'état ponctuel de l'environnement; nonobstant la capacité de détecter et de répondre aux menaces en temps opportun. Pour gérer efficacement les changements, qu'ils soient manuels ou programmatiques, il est essentiel de comprendre l'état actuel. Ce n'est qu'alors qu'il devient possible de planifier et de mettre en œuvre des changements éclairés.

La dernière considération est la nature géodistante du réseau du GC. Au-delà des frontières nationales, les utilisateurs du GC peuvent être situés n'importe où sur la planète et les solutions actuelles sont inadéquates. Bien que la nature complexe du besoin en services distribués ne change pas, il sera le plus avantageux à l'avenir de se concentrer sur les possibilités d'optimisation et de modélisation du trafic.

En bref, le risque croissant de cybermenaces, la complexité de l'infrastructure de réseau et de sécurité actuelle, ainsi que le manque de surveillance et de compétences transversales entraîneront une baisse de l'efficience opérationnelle, une incapacité à répondre aux demandes croissantes et des problèmes au niveau de la disponibilité des services.

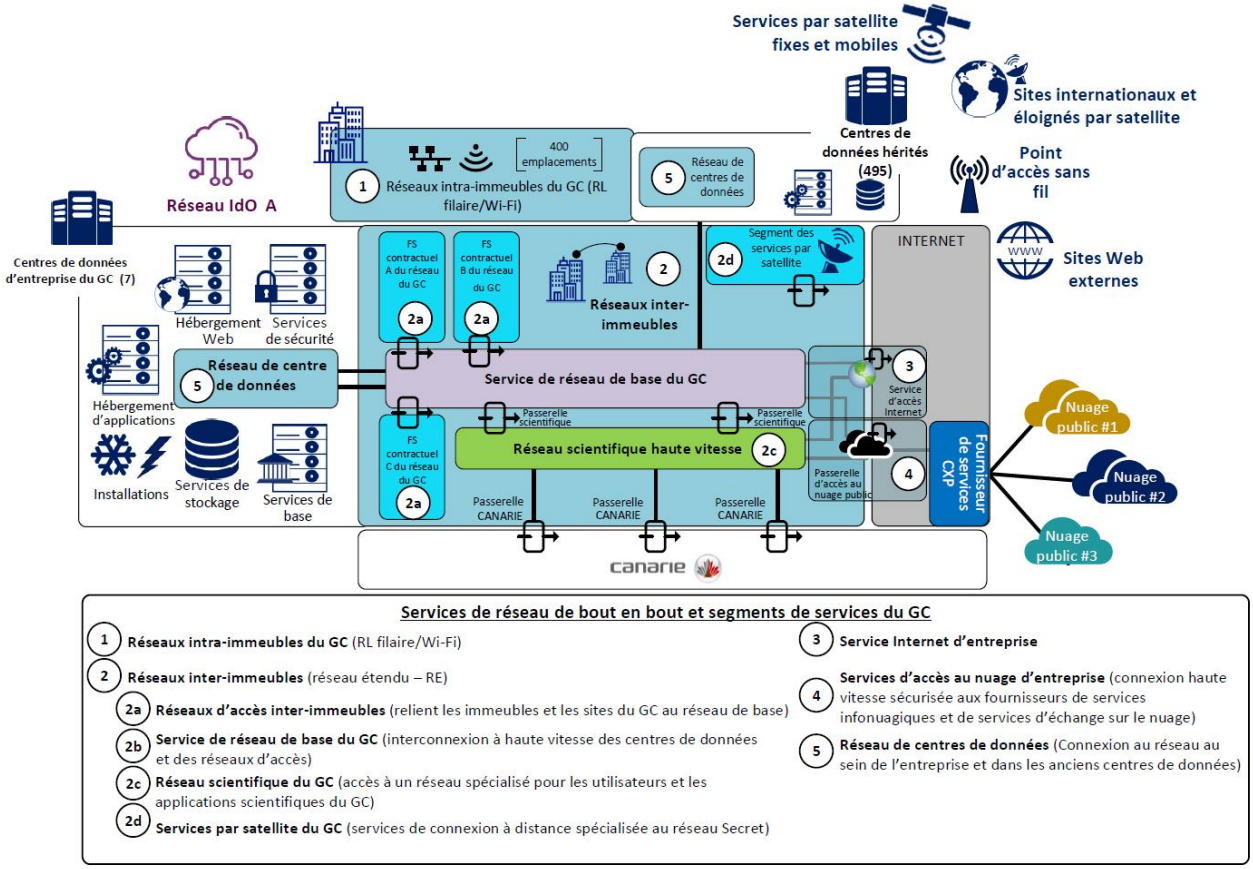


Figure 2 – Réseau actuel de SPC

6. Tendances émergentes dans l'industrie

Au cours de la dernière décennie, la transition vers l'infonuagique a pris son essor et les taux d'adoption continuent d'augmenter. Le nuage offre à l'entreprise la plateforme qui lui permet de prendre en charge l'agilité et le rythme accéléré exigés par leurs utilisateurs. En plus de l'infonuagique et de l'attrait sans précédent du changement, il existe aussi une attente quant à la façon dont les utilisateurs souhaitent travailler. Le « travail » n'est plus considéré comme un lieu, mais comme une activité, et cette notion devient la norme dans de nombreuses entreprises et une caractéristique attendue du lieu de travail. Enfin, l'IdO introduit des appareils dans le réseau, ce qui aurait été, jusqu'à récemment, inconcevable. En raison de l'adoption des services en nuage – infrastructure-service, plateforme-service et logiciel-service (IaaS/PaaS/SaaS), il est de plus en plus difficile de définir, et encore plus de gérer, le périmètre que doivent contenir les défenses de sécurité.

Ces tendances obligent SPC à examiner de nouvelles approches pour offrir des services de réseau au GC et assurer sécurité de l'information du GC. Collectivement, ces changements dans l'industrie influencent les modifications ultérieures de l'infrastructure de l'entreprise, car les organisations ne contrôlent plus l'emplacement ou les limites de l'ensemble des services utilisés pour les opérations. Le modèle traditionnel de sécurité du périmètre (l'approche « château et douves ») n'est plus suffisant; le périmètre ne relève plus du contrôle d'une seule organisation.

6.1. Architecture zéro confiance (ZTA)

Les tendances émergentes dans l'industrie et les risques qu'elles imposent de manière intrinsèque nécessitent l'adoption d'un nouveau paradigme dans l'approche de la sécurité; ce paradigme est la ZTA. Cette nouvelle approche renonce à toute confiance implicite (des utilisateurs ou de l'emplacement), suppose une hostilité au sein du réseau, remplace les idées obsolètes de sécurité basées sur l'emplacement physique et passe à un modèle dynamique axé sur les politiques concernant l'utilisateur, l'appareil et l'application. Historiquement, les réseaux de protocole Internet (IP) ont été conçus dans le but de détecter facilement les périphériques sur le réseau. Cette approche ne suffit plus pour assurer la sécurité, alors que le concept de ZTA sans droit d'accès implicite (c'est-à-dire un réseau sombre) permet à un utilisateur de voir uniquement les périphériques et les applications qu'il souhaite voir ou auxquels il prévoit accéder. Cela réduit de manière importante plusieurs des risques associés à une faille de sécurité typique. Plus important encore, cette approche prend en charge les nuages publics, hybrides et privés, ainsi que

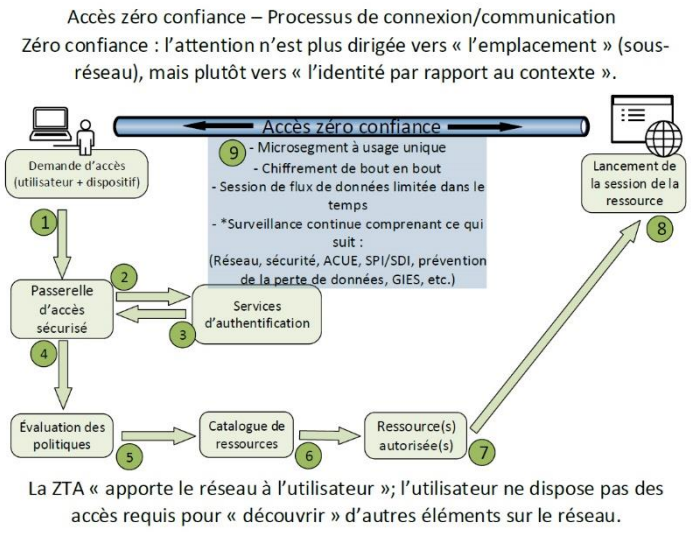


Figure 3 – Processus d'accès zéro confiance

l'accès aux systèmes physiques hérités. La figure 2 montre la complexité de l'environnement d'entreprise moderne, qui héberge de nombreux systèmes informatiques, y compris des solutions de fournisseurs mixtes ou des systèmes en nuage privé.

6.2. Télétravail et accès à distance protégé

Les événements récents ont poussé les services technologiques dans presque tous les secteurs à s'adapter rapidement à un changement de lieu de travail. En réaction à la pandémie de COVID-19, la plupart des organisations ont été contraintes d'adopter le télétravail et un modèle de travail nécessitant un accès à distance. Ce changement de lieu a poussé ces services jusqu'au point de rupture, mais il a également permis de mettre au point des solutions innovantes pour répondre à ces besoins. Bien que fonctionnelles, les applications de réseau privé virtuel (RPV) traditionnelles ou de bureau à distance n'étaient généralement pas adaptées pour permettre à la majorité des travailleurs de les exploiter simultanément. Le service d'accès sécurisé en périphérie (SASE) est devenu chose commune avec une visibilité croissante des principaux groupes de recherche (p. ex., Gartner, Deloitte et KPMG) et a connu une croissance exponentielle dans l'adoption de leurs services. Ce qu'on voyait comme étant marginal il n'y a pas si longtemps est désormais courant et occupe une place centrale dans de nombreuses stratégies de « feuille de route ».

6.3. Infrastructure définie par logiciel (IDL)

Les réseaux hérités ont bien servi à leur époque, mais les demandes nouvelles et changeantes imposées à ces installations révèlent leurs lacunes. La mise en œuvre est longue, les changements sont lents et les coûts sont élevés, pour ne citer que quelques-uns des défauts les plus courants mentionnés par les intervenants. Un concept fixe, bien que très performant et prévisible, est également à l'origine de la nature statique de l'infrastructure. En outre, il a été observé que le modèle de trafic au sein du réseau d'entreprise a évolué. Historiquement, le trafic se déplaçait en majeure partie de l'entreprise vers le consommateur ou vers une autre entreprise (trafic nord-sud); plus récemment, la majorité du flux de données reste au sein de l'organisation (trafic est-ouest). Cette évolution du flux de trafic modifie les risques de sécurité et l'exposition à ces risques qui nécessitent une diligence supplémentaire au sein de l'entreprise. Par le passé, on considérait que le flux de données interne était fiable uniquement en fonction de son emplacement au sein de l'entreprise. Les statistiques récentes sur les atteintes à la protection des données démontrent que plus de 80 %[4] d'entre elles proviennent d'une exposition interne ou d'une compromission. De plus, à mesure que la demande d'accès à partir de l'extérieur de l'organisation augmente, il est essentiel de pouvoir passer à un modèle qui traite chaque demande d'accès aux données de manière égale, quel que soit son emplacement. Tout comme la virtualisation a révolutionné les paradigmes de calcul et de stockage, le réseau et les périphériques de sécurité subissent désormais un changement similaire. L'abstraction du réseau et des

[4] *Indice des menaces d'après ClearSwift Insider – https://www.clearswift.com/about-us/pr/press-releases/cybersecurity-incidents-insider-threat-falls-uk-and-germany-post-gdpr (en anglais seulement)*

dispositifs de sécurité permet une flexibilité de conception qui convient mieux au nouveau modèle de technologies distribuées.

L'IDL aura une influence considérable sur l'infrastructure technologique et les modèles opérationnels. L'IDL représente un ensemble de services définis par logiciel : RLDL (réseau local qu'on retrouve couramment dans les immeubles en périphérie), REDL (options de routage intelligent sur la liaison RE), CDDL (y compris le calcul, le stockage) dans un contexte virtuel, RDL (englobe à la fois le réseau et la sécurité), qui exploitent le nouveau paradigme de la séparation des logiciels. L'IDL modifie les modèles fonctionnels traditionnels avec un matériel réseau qui utilise un logiciel spécialisé dédié.

L'**infrastructure définie par logiciel (IDL)** représente un ensemble de services définis par logiciel, notamment :

- **Réseau local défini par logiciel (RLDL)** – aspect RL ou RM du réseau d'entreprise.
- **Périmètre défini par logiciel (PDL)** – extension de la définition « par logiciel » à l'accès à distance pour assurer la flexibilité du télétravail et l'accès à distance selon le concept de « connexion en tout lieu ».
- **Réseau étendu défini par logiciel (REDL)** – transport des utilisateurs des directions générales, des régions et des utilisateurs à distance vers les centres de données d'entreprise, l'AC de la RCN ou les services infonuagiques.
- **Centre de données défini par logiciel (CDDL)** – (calcul, stockage, réseau et sécurité virtualisés), généralement dans le contexte d'un hyperviseur.
- **Réseau défini par logiciel (RDL)** – terme générique le plus souvent associé au centre de données.

L'IDL changera la façon dont les technologies seront déployées à l'avenir, alors qu'elles ne nécessiteront plus de matériel spécifique pour des fonctionnalités nouvelles ou améliorées. En outre, les avantages de l'IDL l'emporteront largement sur l'incidence potentielle liée au débit qu'on remarque parfois lorsque des périphériques matériels hautement optimisés (fonctionnant à une vitesse proche de la ligne) sont remplacés par des périphériques logiciels.

L'IDL favorise la souplesse des ressources grâce à l'application de fonctions qui lui sont propres. Les modifications à la demande des caractéristiques de l'infrastructure, telles que la capacité, la vitesse, la qualité de service et la sécurité, sont mises en œuvre à l'aide des technologies d'IDL. Ce type de fonctionnalité permet un approvisionnement rapide et efficient en ressources, ce qui se traduit par une efficience opérationnelle, une utilisation rentable des ressources et, finalement, la satisfaction du client grâce à l'amélioration des offres de services.

L'IDL découple le matériel et le logiciel. Cela procure des fonctionnalités et une flexibilité supplémentaires à une infrastructure qui était auparavant relativement statique tout au long de son cycle de vie de trois à cinq ans. L'IDL permet à plusieurs composants logiciels de coexister sur un composant matériel donné, produisant ainsi des dispositifs multifonctions (par exemple, un routeur coexistant avec un pare-feu fournissant des fonctionnalités avancées de réseautique et de sécurité intégrées).

6.3.1. RLDL – Réseau périphérique – Services RL de bureau ou d'immeuble

Priorité correspondante du point de vue technologique : Accès défini par logiciel (RLDL)

Le RLDL détermine la façon dont les bureaux (par rapport aux individus) se connecteront au réseau local de l'avenir. Des technologies telles que le Wi-Fi 6 et la 5G offriront l'occasion de moderniser et d'améliorer l'expérience utilisateur, car elles sont exploitées comme un moyen de connectivité plus flexible. *Réseau périphérique – Services de bureau ou d'immeuble* comprend ce qu'il faut pour brancher les appareils des utilisateurs finaux au réseau par l'entremise du Wi-Fi ou Wi-Fi 6 et de la 5G. Même si la stratégie ou l'approche *sans-fil d'abord* simplifiera la connectivité des utilisateurs, réduira les coûts d'aménagement et améliorera l'expérience utilisateur, certains appareils (comme les imprimantes et les postes de vidéoconférence) ne sont pas pratiques relativement à la connectivité sans fil. Cette approche permettra également une plus grande prévisibilité dans l'acheminement du trafic vers ces appareils et à partir de ceux-ci, offrant une optimisation du trafic.

Les performances du réseau sont d'une importance cruciale pour les immeubles en périphérie – services de bureau ou d'immeuble et pour la connectivité Internet directe (REDL) qui permet l'accès utilisateur (par rapport au retour vers des pare-feu centralisés) et doivent être envisagées comme un moyen d'améliorer l'efficience et l'efficacité du réseau. Considérant que jusqu'à plus de 60 % du trafic réseau concerne les documents de « bureau » (qui seront destinés à O365), les liaisons d'accès direct à Internet (DIA) et le REDL peuvent réduire concrètement le trafic du réseau au sein du réseau de base du GC tout en améliorant simultanément l'expérience de l'utilisateur type. Dans le cadre de la stratégie d'IDL, avec une conception améliorée et des changements aux politiques à la fois dans le réseau et dans les domaines de sécurité, cela servira à améliorer la performance des applications et, par conséquent, l'expérience utilisateur. Compte tenu de l'adoption des services infonuagiques, des attentes relatives à l'intégration des appareils de l'IdO et de l'appel croissant au mode PAP (« Prenez vos propres appareils), il est raisonnable de supposer que l'ancienne approche de protection du périmètre ne suffira pas. Le modèle à zéro confiance offre la flexibilité et la capacité de gestion qui seront nécessaires pour l'état futur, et devrait donc être envisagé pour une intégration précoce dans le cadre de la mise en œuvre de la stratégie en matière de réseau et de sécurité.

6.3.2. Accès à distance [PDL]

L'accès à distance (périmètre défini par logiciel) repose sur la façon dont les utilisateurs se connectent à distance aux services du GC.

Priorité correspondante du point de vue technologique : Périmètre défini par logiciel (PDL)

Dans ce contexte, l'accès à distance est défini comme toute connexion où un utilisateur n'est pas directement branché à un réseau du GC en utilisant une infrastructure filaire traditionnelle ou un service Wi-Fi avec accès direct au réseau de l'entreprise.

Les nouvelles technologies telles que la 5G et le Wi-Fi 6 modifieront les services du « dernier kilomètre » des utilisateurs à moyen terme. Des changements sont déjà en cours dans la façon dont les appareils des utilisateurs finaux à distance sont sécurisés dans des domaines, comme l'authentification des utilisateurs et la protection des points terminaux pour les ordinateurs portatifs, les téléphones mobiles et les tablettes. Ces changements et leur incidence sur les exigences en matière de sécurité de ces appareils imposent de nouvelles contraintes sur la façon dont les services d'accès à distance seront mis en œuvre à l'avenir. Une authentification robuste des utilisateurs est essentielle dans un environnement de ZTA, alors que l'authentification multifacteur (AMF) à l'échelle du GC représente un aspect essentiel. Avec l'adoption du mode PAP, de l'IdO et des applications et services hébergés dans le nuage, il devient clair que le contrôle du périmètre n'est plus facilement définissable; compte tenu de cette « perte de contrôle », de nouvelles mesures d'atténuation doivent être mises en place pour sécuriser l'entreprise. La ZTA nous offre cette fonction. En priorisant la sécurité entre l'utilisateur final et la session et l'application, quel que soit l'endroit où il réside, le flux de données peut être sécurisé et rendu conforme à la politique. Cela concerne deux aspects clés de la sécurité : premièrement, l'utilisateur n'a accès qu'aux applications qu'il est autorisé à utiliser, et deuxièmement, le modèle à zéro confiance sous-entend une visibilité limitée. Une visibilité limitée signifie qu'un utilisateur ou un système ne peut voir ou découvrir d'autres périphériques sur le réseau à l'extérieur s'il s'agit d'une isolation basée sur des politiques (voir microsegmentation).

6.3.3. Réseau étendu défini par logiciel (REDL)

Le REDL est une application spécifique de la technologie RDL (réseautique définie par logiciel) appliquée aux connexions de réseau étendu (RE), comme l'ancien point à point, l'Internet à haut débit, la 4G, la LTE ou la MPLS. Le REDL connecte intelligemment les réseaux d'entreprise sur plusieurs liaisons par le biais d'un routage de trafic optimal. Pour ce faire, il tient compte de facteurs tels que la disponibilité de la liaison, la charge, le temps de réponse, le type de trafic et la priorité. Par exemple, cette approche gère et dirige le trafic réseau des bureaux d'une direction générale destiné aux services externes, qu'ils soient dans le nuage ou dans un centre de données d'entreprise. L'objectif du REDL est d'optimiser le flux du réseau et d'améliorer l'expérience utilisateur sur de plus grandes distances géographiques.

Le REDL a servi à plusieurs applications depuis sa création, mais sa principale contribution a été le remplacement des coûteuses connexions point à point ou du RE MPLS avec une connexion DIA.

6.3.4. Réseau de base et accès au nuage et à Internet du GC – RE [REDL]

Priorité correspondante du point de vue technologique : Réseau étendu défini par logiciel (REDL)

Le REDL englobe toutes les connexions en direction de l'entreprise et au sein de celle-ci. Les connexions entre le réseau périphérique et les centres de données d'entreprise, les services en nuage et les services Internet bénéficieraient tous de la mise en œuvre du REDL. La connectivité au réseau externe décrit la façon dont le centre de données

d'entreprise se branchera aux partenaires et services connectés au nuage, à Internet et au RE du GC. Des efforts sont en cours pour réaligner la connectivité externe avec les applications SaaS en nuage existantes et à venir, dont Office 365. Les activités de migration des services traditionnels des fournisseurs de service Internet (FSI) vers les services de point d'interconnexion Internet (IXP) et de point d'interconnexion du nuage (CXP) offriront des possibilités d'intégration du REDL avec un accès contrôlé aux ressources externes.

Alors que SPC se tourne vers le REDL, il peut tirer des avantages significatifs de son déploiement :

- Optimiser le flux de trafic pour améliorer l'expérience utilisateur.
- Fournir des options à moindre coût pour la connectivité au RE du GC à partir d'emplacements gouvernementaux plus petits ou éloignés.
- Améliorer la sécurité du réseau grâce à des capacités de sécurité intégrées améliorées dans les solutions de type REDL.
- Tirer parti des capacités logicielles du REDL pour rapidement apporter des modifications à la configuration ou fournir de nouveaux services.
- Offrir la possibilité de fournir (dans certains cas) une connectivité Internet locale sécurisée sans avoir à rediriger le trafic Internet vers les centres de données du GC, ce qui améliorera les performances à venir des solutions Internet, dont Office 365.
- Permettre un meilleur débit réseau que les solutions basées seulement sur la MPLS, car les plateformes REDL tireront parti du choix du « chemin intelligent » pour optimiser les performances du réseau.
- Optimiser l'utilisation et les performances du réseau grâce aux protocoles de routage prenant en charge les applications.
- Il existe plusieurs cas d'utilisation possible du REDL dans l'environnement de réseau du gouvernement à la fois dans l'état actuel et à venir (par exemple, des sites gouvernementaux de petite à moyenne taille utilisant des circuits de MPLS coûteux).
- Les emplacements éloignés (en particulier à l'extérieur du pays) doivent renvoyer le trafic Internet vers un centre de données du GC, puis « rediriger » le trafic vers Internet pour les services Internet, ce qui crée des délais aller-retour importants, en plus d'aggraver l'expérience de l'utilisateur à distance.
- Résilience – compte tenu de la nature du REDL, qui consiste à définir le trafic sur plusieurs lignes ou routes, l'interruption ou le retard sur une route est automatiquement détecté et le trafic est acheminé vers un autre chemin.
- Fournir rapidement des capacités d'approvisionnement en tant que mécanisme de basculement tel que la 4G, la LTE ou éventuellement, la 5G en cas de défaillance du circuit primaire.

Alors que SPC commence à envisager une stratégie de type REDL, la situation actuelle des fournisseurs de REDL doit être examinée. De nombreux fournisseurs en sont encore

aux premières étapes de la définition de leurs solutions de REDL et peuvent ne pas avoir les capacités que SPC exige. Cependant, certaines organisations proposent désormais également des solutions de REDL entièrement gérées qui devraient être considérées comme faisant partie d'une stratégie d'exploitation du réseau plus large.

6.3.5. Centre de données d'entreprise (CDE) et services de réseau central [CDDL et RDL]

Priorité correspondante du point de vue technologique : Centre de données défini par logiciel (CDDL) et réseautique définie par logiciel (RDL)

Les technologies CDDL et RDL offrent les moyens de fournir des services de connectivité entre les centres de données d'entreprise, ainsi qu'à l'intérieur même de ces centres, de même que les interconnexions entre les périphériques de stockage virtuels et physiques, les dispositifs de sécurité et toute autre plateforme de centre de données. Dans le centre de données, CDDL signifie l'ensemble des services d'IDL (calcul, réseau, stockage, etc.) qui sont utilisés dans le cadre de la topologie du centre de données.

6.3.5.1. Centre de données défini par logiciel (CDDL)

Le centre de données (CD) défini par logiciel (qui utilise une architecture de réseau sous-jacent et de réseau superposé) est la prochaine évolution logique par rapport à l'architecture traditionnelle à trois niveaux pour les CD hautement virtualisés où la mobilité de la machine virtuelle (MV), les périmètres zéro confiance, les services de réseau à la demande et l'informatique en nuage représentent des priorités élevées. Cette architecture de la nouvelle génération fournit un nombre de sauts, une latence et une bande passante cohérents entre tous les périphériques qui font partie du réseau. Certaines des exigences clés d'un centre de données moderne défini par logiciel sont les suivantes :

- l'automatisation simplifiée grâce à un modèle de politique axé sur les applications;
- la gestion, l'automatisation et l'orchestration centralisées;
- l'optimisation mixte de la charge de travail et de la migration/l'équilibrage de la charge;
- l'environnement d'architecture mutualisée sécurisé et évolutif;
- les périmètres à zéro confiance;
- l'extensibilité et l'ouverture – source ouverte, API ouvertes et flexibilité logicielle ouverte pour les équipes responsables des opérations de développement et intégration des partenaires de l'écosystème.

La structure de CDDL offre une virtualisation de réseau intégrée pour toutes les charges de travail connectées, alors que le contrôleur peut gérer non seulement les périphériques physiques, mais également les commutateurs virtuels.

Le nouveau modèle d'infrastructure de conception logicielle passera d'un modèle d'entreprise unique à un modèle de fournisseur de services prenant en charge une architecture mutualisée. Parce que l'architecture évolue vers un modèle de fournisseur

de services, le nouveau centre de données évoluera également vers ce même modèle et se procurera une grande partie de son architecture auprès des fournisseurs infonuagiques. Les emplacements physiques du CD influenceront la conception du centre de données de deux façons principales : la proximité de l'IXP ou du CXP et la distance par rapport au CDE. Dans le premier cas, la présence d'un fournisseur de services IXP/CXP plus rapproché permettra une évacuation plus précoce du trafic SaaS (M365, env. 60 % du trafic réseau). Dans l'autre cas, une plus grande distance imposera une plus grande latence, c'est une simple question de physique – nous sommes limités à la « vitesse de la lumière ».

6.3.5.2. Réseau défini par le logiciel (RDL)

En termes courants, le RDL permet de séparer le « plan de contrôle » du « plan de données », alors que certaines solutions ajoutent le « plan de gestion » comme séparation supplémentaire. Ces couches de séparations permettent de modifier le plan de contrôle (couche d'instructions) sans avoir de répercussion sur le plan de données (c'est-à-dire que les paquets continuent à se déplacer). Cette approche permet de traiter le réseau sous-jacent physique indépendamment des couches « superposées ». Ces superpositions au niveau du réseau central dans le centre de données d'entreprise (CDE) acceptent une ou plusieurs superpositions qui peuvent servir d'interface avec différents concepts. Par exemple, un CD type possède une collection de matériel physique constituant le réseau sous-jacent; sur ce réseau, on trouve une première couche de recouvrement qui concerne la gestion de la couche physique. Ensuite, en option, le CDDL pourrait fournir une autre superposition distincte pour le contrôle des dispositifs relatifs au réseau et à la sécurité qu'on y trouve.

Comme indiqué précédemment, le RDL virtualise et sépare les services fonctionnels des appareils du réseau dans le plan de contrôle et le plan de données. Dans le réseau central, cela peut offrir des avantages considérables lorsqu'on désire modifier, ajouter ou supprimer des ressources. L'interaction avec le CDDL peut reposer davantage sur l'automatisation, réduisant le besoin d'intervenir manuellement pour étendre l'empreinte des ressources physiques du CDDL, éliminant ainsi les complexités de la planification et de la programmation multiéquipes pour les activités de routine. Des interactions similaires avec le REDL peuvent accroître l'efficacité et optimiser les itinéraires du trafic qui entre dans le CDE et qui en sort.

7. Feuille de route pour l'adoption

Ce document utilise des piliers stratégiques pour décomposer la stratégie en parties consommables : connectivité, contrôle d'identité et d'accès, et surveillance. La connectivité englobe les dispositifs de réseautique traditionnels comme infrastructure sous-jacente : commutateurs, routeurs, pare-feu, équilibreurs de charge, etc. Dans ce contexte, la connectivité introduit également la définition par logiciel pour améliorer les services traditionnels de sorte que l'adaptabilité et l'optimisation de l'infrastructure permettent une optimisation en cascade des services d'application. Le contrôle d'identité et d'accès intègre les services d'identité et de sécurité modernes vers des options évolutives plus avancées, notamment : l'authentification intrinsèque sans mot de passe, la gestion d'accès privilégié (GAP) et la gouvernance des identités centralisées, et l'authentification unique adaptative contextuelle. La surveillance dans ce cas comprend également la collecte, le traitement et la diffusion de l'ensemble des données du réseau (performances et disponibilité), de la sécurité (utilisateurs, contexte de l'appareil, accès, authentification et incidents) et des données d'application (utilisation, distribution) pour faire place aux futures solutions qui tireront parti de l'intelligence artificielle (IA) et de l'apprentissage automatique (AA) pour optimiser l'expérience utilisateur en accédant aux renseignements requis grâce à l'automatisation et à l'orchestration. De plus, une nouvelle approche en matière d'approvisionnement doit être adoptée afin de répondre aux progrès technologiques et aux attentes des utilisateurs en ce qui a trait à la prestation de services en temps opportun. On s'attend à ce que les services soient fournis au bout de quelques heures ou de quelques jours, et non de quelques semaines ou de quelques mois. Un facteur clé consiste à tirer parti de l'IDL pour permettre la mise en place d'une infrastructure de réseau et de sécurité.

La figure 4 montre les piliers stratégiques et la manière dont leur évolution, associée à une nouvelle approche en matière d'approvisionnement, est nécessaire pour l'infrastructure définie par logiciel, l'architecture à zéro confiance et qu'elle évolue finalement vers une innovation améliorée des applications et services, de l'intelligence artificielle pour les opérations informatiques (AIOps) et de OASI (orchestration et automatisation de la sécurité et intervention).

7.1. Piliers stratégiques

Cette section du document décrit les trois piliers stratégiques essentiels qui constituent la base de la stratégie de réseau et de sécurité. Ces trois capacités confirment la vision d'avenir en matière de réseau et de sécurité de SPC et sont harmonisées avec la stratégie SPC 3.0 et le plan stratégique des opérations numériques de 2018-2022. Cette

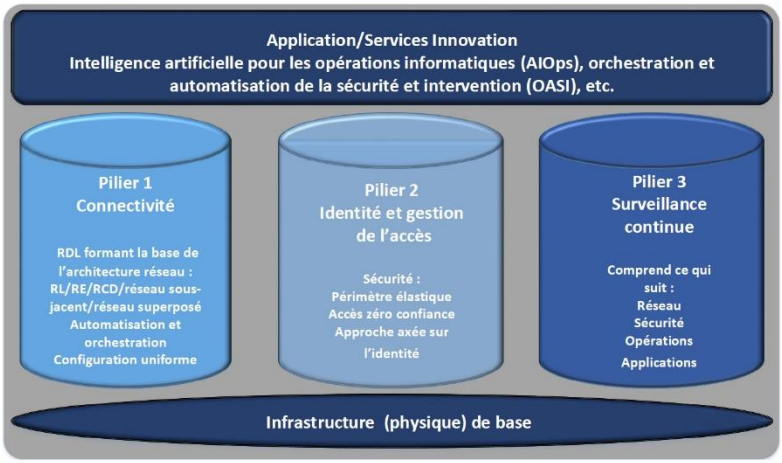


Figure 4 – Piliers stratégiques

section a pour but de décrire l'état final souhaité pour SPC dans chacun de ces domaines. Bien que ces capacités ne soient pas toutes réalisables à court terme, la feuille de route ultérieure et les activités connexes décrivent la voie à suivre à moyen terme pour réaliser l'état futur décrit dans cette section.

7.2. Pilier 1 : Connectivité

7.2.1. Aperçu

La connectivité en tant que pilier repose sur l'infrastructure physique fondamentale sous-jacente pour offrir les services définis par logiciel sur les aspects du réseau qui concernent le RL, le RE et le RCD (réseau de centres de données). Ceci permet au réseau sous-jacent et au réseau superposé définis par logiciel de séparer le plan de contrôle du plan de données, ce qui permet d'isoler la gestion du réseau de la couche de transmission de paquets. Cette approche centralisée permet non seulement une plus grande cohérence de la configuration des appareils en automatisant l'orchestration, mais également moins de services gênants qui ont des répercussions sur les performances.

La connectivité au sein du réseau du GC et la stratégie en matière de réseau et de sécurité peuvent être classées en quatre grands domaines :

1) Réseau périphérique – Services de bureau ou d'immeuble – RL
2) Service de base et accès au nuage et à Internet du GC – RE
3) RCD – Centre de données d'entreprise et services de réseau central
4) Accès à distance

Chaque domaine présente sa propre complexité et des possibilités d'amélioration des communications au sein du GC en intégrant la panoplie de services de réseau et de sécurité requis, comme la gestion des identités et des accès, la confiance zéro, le nuage d'abord, le sans-fil d'abord et d'autres compétences. L'IDL rendra également ces réseaux plus flexibles et plus efficaces.

7.2.2. État actuel

Le GC gère actuellement un réseau hérité complexe, procurant des services de TI de base à environ 4 000 sites et 5 000 immeubles, en plus de brancher des centaines de milliers d'appareils pour les employés du GC, les entrepreneurs et les citoyens.

Réseaux intra-immeubles

Il n'existe présentement aucune norme en matière d'infrastructure; chaque ministère présente des configurations physiques et logiques, des procédures d'exploitation, des niveaux de service et des cas d'utilisation différents. Pour cette raison, un effort de « développement de services standard » est nécessaire.

La majorité de l'infrastructure intra-immeubles existant dans les bâtiments à un ou plusieurs locataires utilise un câblage fixe traditionnel vers les terminaux. L'utilisation de l'infrastructure câblée pour les appareils des utilisateurs finaux diminue régulièrement avec l'acceptation et le déploiement continus de la connectivité basée sur l'accès sans fil (Wi-Fi).

L'infrastructure, l'équipement et le câblage de réseau intra-immeubles ont plusieurs gardiens, ce qui entraîne une complexité des modèles opérationnels avec des stratégies disparates pour les technologies, les fournisseurs, le déploiement, la maintenance et les opérations. Des centaines de projets individuels sont prévus ou en cours pour préserver, actualiser ou remplacer ces environnements sans stratégie globale ou intégrée.

Réseaux interimmeubles

Les réseaux interimmeubles sont constitués d'un ensemble de composants et de services de réseau qui assurent le transport de données entre les bâtiments et les centres de données, à la fois nationaux et internationaux, et s'étendent souvent sur des réseaux externes (Internet, nuage, etc.), incluant :

- Le transport interimmeubles assure le transport du « dernier kilomètre » vers plus de 4 000 sites, dont plus de 400 comptent plusieurs occupants.
- Les services de base interimmeubles fournissent des services de transport par fibre noire à plus de 220 sites (centralisés dans la RCN) et des interfaces de réseau à réseau (IRR) pour la connectivité intranet et extranet.
- Les connexions au réseau satellite sont utilisées au sein de plus de 30 ministères pour des communications secrètes et essentielles aux missions avec plus de 6 000 terminaux mobiles.
- Les réseaux internationaux sont déployés dans le cadre de centaines de missions canadiennes et déployés au sein des forces armées dans le monde entier en tant que réseaux privés du GC. Les technologies comprennent une combinaison de déploiements terrestres et par satellite (VSAT).

La plupart des services énoncés ci-dessus ont fait l'objet d'un catalogage et d'une impartition en tant que contrats à long terme avec différents fournisseurs de services de télécommunications. SPC s'est occupé de la gérance de l'architecture du réseau.

Réseaux des centres de données d'entreprise

En plus des quatre nouveaux centres de données d'entreprise de SPC, les ministères partenaires disposent d'environ 500 centres de données existants qui seront consolidés dans le cadre des efforts continus de SPC visant à consolider les centres de données. Plus de 50 de ces centres de données sont considérés comme des déploiements d'envergure[5].

La plupart de ces centres de données ont été déployés avant l'adoption de normes d'infrastructure communes. Il existe donc peu de points communs dans les structures de réseau et les configurations sous-jacentes. Certains projets antérieurs ciblant la consolidation des centres de données se sont révélés difficiles.

En plus des environnements de production, il faut également tenir compte des environnements intégrés de pré-production ou de laboratoire dans le cadre de cette

[5] *Plan stratégique des opérations numériques de SPC, 2018-2022*

stratégie. À l'heure actuelle, les laboratoires d'essais ne sont pas intégrés à tous les composants et nombre d'entre eux sont limités en raison des limites imposées aux ministères. Cette situation, combinée à la segmentation du réseau, rend difficiles l'essai et la validation des futurs déploiements de l'état, ce qui augmente le risque pour le projet. On a déjà programmé le développement de centaines d'applications. Si on ne dispose pas d'installations d'essai standard avant la production des logiciels, du matériel et de l'infrastructure, la cohérence de l'intégration représentera tout un défi.

Les défis actuels dans ces domaines de connectivité du réseau entraînent plusieurs défis généraux pour le GC :

- Des processus manuels effectués sur un appareil à la fois sont nécessaires afin de gérer le réseau. Par conséquent, les modifications du réseau peuvent exiger beaucoup de temps et d'efforts.
- Une mauvaise télémétrie et un manque d'instrumentation normalisée limitent les capacités en ce qui concerne la production de rapports, puisque l'optimisation du réseau repose sur les « meilleures hypothèses ».
- Le manque de normalisation lié aux silos technologiques et aux politiques d'approvisionnement augmente la complexité du support et de l'intégration.
- L'asservissement ou la dépendance à un fournisseur à différents niveaux du réseau a une incidence sur la capacité du GC d'adopter les technologies futures au fur et à mesure que le secteur des TI évolue et donne lieu à des achats à fournisseur unique.

Connectivité au réseau externe – traditionnelle

Les partenaires de SPC sont connectés aux services en nuage public des manières suivantes :

1. Créer un tunnel sur les réseaux privés virtuels (RPV) existants fournis par SPC, créant essentiellement un tunnel dans un tunnel;
2. Tirer parti des lignes fournies par les opérateurs de télécommunications telles que la ligne d'abonné numérique (DSL) et le câble;
3. Utiliser des solutions de RPV de site à site dans lesquelles un RPV est établi sur le pare-feu géré par le client dans le nuage public;
4. Utiliser des solutions OpenVPN (telles que le serveur d'accès OpenVPN) si elles sont prises en charge par le fournisseur du nuage public.

La seule solution approuvée par SPC que les clients peuvent utiliser est l'utilisation de solutions OpenVPN qui consistent pour SPC à fournir un poste de travail sécurisé et spécialisé afin de permettre au client d'établir la connectivité avec le fournisseur du nuage public. La connectivité décrite ci-dessus est prise en charge uniquement pour les données non classifiées et de niveau Protégé A. Elle ne comprend pas le niveau de sécurité Protégé B ou un niveau de classification supérieur. Les partenaires de SPC exploitent aussi actuellement les solutions MPLS et RPV pour la connectivité aux services du RE du GC.

Au moment de rédiger le présent rapport, des efforts sont en cours pour étendre l'empreinte de sortie et d'entrée du GC aux services en nuage; cela inclura Office365 et d'autres services de SaaS en nuage. Un accès direct sans RPV sera mis en place pour optimiser le trafic et réduire la latence, améliorant ainsi ultimement l'expérience de l'utilisateur.

7.2.3. État futur

Dans l'état cible du GC, les réseaux sont basés sur des normes de système ouvert, hautement automatisé et finalement offert en tant que service par l'entremise d'un portail Web, alors que les changements à la connectivité du réseau prennent quelques secondes ou minutes, plutôt que des jours ou des semaines. La réseautique basée sur l'intention et associé à l'analyse du réseau permettra de procéder à l'optimisation dynamique du réseau pour répondre aux exigences changeantes de connectivité et de performance.

De plus, le GC, en tant qu'entreprise, disposera d'un espace commun pour élaborer des essais, intégrer, mettre en scène et réparer des réseaux sous-jacents, des réseaux superposés et des applications. En utilisant la virtualisation et des réseaux sous-jacents communs, la construction d'une installation de pré-production de composants communs représentera un service à la demande. Les développeurs ne seront plus isolés en raison des limites ministérielles et des segments du réseau, ce qui permettra d'accroître les capacités de tester et de valider (réduire les risques) les déploiements de l'état futur.

Réseaux intra-immeubles

En ce qui concerne la connectivité intra-immeubles, le GC a adopté une stratégie sans fil d'abord pour les utilisateurs finaux et les appareils de l'IdO. De plus, l'architecture du RL et du RE sera en constante expansion pour intégrer les appareils de l'IdO. Au fil du temps, l'adoption des technologies 5G modifiera les modèles de connectivité pour les terminaux accédant aux ressources du GC. Un tel processus pourrait avoir une incidence considérable sur l'utilisation de la connectivité entre un bâtiment et les services de réseau du GC, réduisant ainsi la dépendance à l'égard de la connectivité traditionnelle des bâtiments, tout en augmentant la dépendance à l'égard des ressources externes et des passerelles. À moyen terme, les appareils continueront de reposer à la fois sur la connectivité Wi-Fi et cellulaire (3G/LTE/4G) à mesure que la technologie 5G atteint sa maturité et que les prix sont analysés pour déterminer le potentiel de valeur ajoutée.

La sécurité du réseau doit évoluer au rythme du nouveau modèle de connectivité, avec la capacité d'identifier en toute confiance les appareils et les utilisateurs accédant aux ressources du réseau du GC, en fournissant une connectivité et des services fiables sur n'importe quelle plateforme et n'importe quel appareil (voir la section « Contrôle d'identité et d'accès » pour plus de détails).

Réseaux interimmeubles

Alors que les réseaux interimmeubles commenceront à tirer parti des technologies de l'IDL dont on fait mention ci-dessus, la couche de transport interimmeubles sous-jacente

continuera à court et moyen terme d'être principalement un modèle externalisé tirant parti des investissements dans les infrastructures déjà en place. Au fil du temps, cependant, à mesure que les nouveaux modèles de connectivité (5G hébergée) deviendront plus viables, la dépendance à l'égard des infrastructures des immeubles traditionnels diminuera.

Les services de base interimmeubles resteront probablement les mêmes pour la connectivité dans la région de la capitale nationale, car il s'agit d'une solution rentable avec la majorité des bâtiments du GC situés dans la région.

La gérance de l'architecture technologique doit rester au sein de SPC. Les contrats actuels devront être revus pour s'assurer que les services sont conformes à l'état futur de SPC 3.0.

Centres de données d'entreprise

Sur le plan du réseau, le changement transformationnel majeur dans les centres de données sera le passage au RDL. Le RDL permettra de fournir rapidement de nouveaux services de réseau et des changements. Les AIOps offriront également la possibilité d'effectuer des modifications automatisées en fonction d'éléments tels que la correction des menaces, la gestion des performances, etc.

Le REDL jouera également un rôle dans les centres de données de petite et moyenne taille en tant que nouvelle couche de transport pour l'accès aux services Internet et au RE du GC, éliminant ou remplaçant ainsi les solutions MPLS existantes (et coûteuses).

Connectivité au réseau externe

On s'attend à ce que de nombreux clients continuent d'exploiter l'option précédemment décrite dans la section État actuel pour accéder aux données non classifiées ou de niveau Protégé A. Les données de niveau Protégé B seront accessibles en utilisant la solution de connectivité ADNS (activation et défense du nuage sécurisé). SPC a déclaré que les clients peuvent désormais tirer parti de l'ADNS pour une connectivité de niveau Protégé B. Pour tirer parti de l'ADNS, il a été conseillé aux clients de s'assurer qu'ils répondent à toutes les exigences de sécurité avant d'obtenir la connectivité.

À mesure que les solutions de REDL évoluent, nous verrons de plus en plus de clients tirer parti des solutions de REDL pour permettre l'accès à Internet et aux services SaaS en nuage au lieu des solutions MPLS héritées.

7.2.4. Répercussions et dépendances

Pour réussir à activer l'état cible en matière de connectivité, une seule organisation (c'est-à-dire SPC) doit avoir le pouvoir de garantir la conformité et la disponibilité d'un financement approprié. Il faudra peut-être revoir le projet de Sécurité du périmètre de l'entreprise (SPE) pour tenir compte d'un périmètre « virtualisé » qui s'étend au-delà des limites du périmètre traditionnel. Une ZTA complète devra être mise en place progressivement pour tenir compte de la manière dont le projet de SPE sera harmonisé avec l'approche de ZTA.

7.3. Pilier 2 : Contrôle d'identité et d'accès

7.3.1. Aperçu

Un des principes clés d'une posture de sécurité à zéro confiance est la mise en œuvre d'un principe de privilège minimal et de contrôles de sécurité précis pour renforcer la sécurité de l'information à l'intérieur du périmètre du réseau du GC. L'accès aux ressources est accordé en vertu d'une approche basée sur des politiques pour sécuriser l'accès plutôt que de dépendre de la configuration manuelle des règles de pare-feu, qui est lourde, statique et sujette à des erreurs. Le mouvement latéral à l'intérieur du périmètre est sécurisé par un processus de microsegmentation. La microsegmentation réduit au minimum l'intrusion lorsqu'elle se produit inévitablement. Au lieu d'utiliser des adresses IP et des zones de sécurité pour établir des politiques de segmentation, les politiques sont basées sur des attributs logiques (et non physiques) et procurent un contrôle d'accès granulaire aux applications aux utilisateurs autorisés.

L'intention des contrôles d'accès est de garantir qu'un utilisateur autorisé a accès aux bonnes ressources, comme des bases de données, des applications ou des réseaux et que ces ressources sont inaccessibles aux utilisateurs non autorisés. Les contrôles d'accès comprennent des mesures physiques et logiques. Les contrôles d'accès physique limitent l'accès aux placards, aux salles et aux immeubles du réseau où se trouvent des biens physiques ou des équipements. Les contrôles d'accès logiques accordent ou empêchent l'accès aux ressources (données, applications, systèmes, réseaux, etc.) une fois que l'identité d'un utilisateur, d'une entité ou d'un appareil a été vérifiée. Les droits d'accès logiques ou physiques sont généralement liés aux identités uniques de l'utilisateur, de l'entité ou de l'appareil. À mesure que le paysage technologique du réseau subit une transformation importante, cela augmente davantage l'importance des contrôles d'accès logiques afin de protéger les réseaux et les flux d'information du GC.

7.3.2. État actuel

Le GC a traditionnellement appliqué l'approche « château et douves » au contrôle d'accès, ce qui vise à sécuriser le périmètre en authentifiant les utilisateurs autorisés à des points d'entrée sécurisés et en leur accordant l'accès. Les réseaux se sont étendus pour inclure un grand nombre de points finaux et les adversaires continuent de trouver de nouvelles façons de contourner la sécurité du périmètre. La situation devient encore plus complexe en raison de l'adoption croissante des technologies mobiles qui permettent le télétravail et l'utilisation de services externalisés. Le GC a traditionnellement atténué ces menaces en établissant des zones de réseau et en déployant un nombre accru de pare-feu pour filtrer l'accès au réseau. Cependant, cette approche est devenue lourde et coûteuse, car les règles de pare-feu doivent être continuellement ajustées pour tenir compte à la fois des nouvelles menaces et du nouveau trafic autorisé.

Aujourd'hui, les Canadiens accèdent en toute sécurité aux services en ligne du GC en se connectant avec un identifiant bancaire en ligne (comme un nom d'utilisateur et un mot de passe) provenant d'institutions financières canadiennes par l'entremise du

Service de courtier de justificatifs d'identité ou ils peuvent recourir au service d'identification de marque GC, appelé CléGC.

Les utilisateurs du gouvernement du Canada s'authentifient auprès de différents magasins des utilisateurs, y compris des magasins intégrés, l'Active Directory ministériel et l'Active Directory fédéré, ainsi qu'auprès d'une multitude de services d'AMF différents, y compris la GJI et d'autres solutions ministérielles. Un système d'identité numérique fiable est fondamental pour contrôler l'accès et représente un élément clé d'une sécurité transparente et sans friction dans les systèmes numériques.

7.3.3. Tendances

L'ancienne approche du contrôle d'accès était celle d'une posture de défense en profondeur qui utilise une série de mécanismes défensifs stratifiés afin de protéger les données et les données précieuses. Si un mécanisme échoue, un autre intervient immédiatement pour contrecarrer une attaque. Cette approche n'est plus considérée comme un moyen viable de prévenir et d'atténuer les menaces de sécurité actuelles.

Les tendances en matière de contrôle d'accès sont principalement façonnées par la prolifération d'appareils connectés, les options de connexion, la mobilité accrue des utilisateurs finaux et l'attente accrue d'une expérience cohérente et personnalisée, quels que soient le canal de connexion, l'emplacement ou le type d'appareil utilisé pour établir la connexion. Ces attentes vont au-delà de la définition traditionnelle d'un utilisateur final (généralement considéré comme un consommateur du service) et incluent les utilisateurs avec un droit d'accès (comme les administrateurs de service) et les utilisateurs non humains (comme les robots, les appareils connectés intelligents).

En conséquence, les contrôles d'accès au réseau de la nouvelle génération devraient pouvoir prendre en charge et permettre :

- Les **identités inter-entités** – Les utilisateurs finaux s'attendent à une connectivité transparente aux données et aux services sur site et hors site avec l'appareil et dans l'emplacement de leur choix. Les contrôles d'accès doivent permettre des processus d'authentification des utilisateurs qui sont transparents, résilients et efficaces.
- Les **identités fournies ou approuvées par l'utilisateur final** – Les contrôles d'accès de la prochaine génération doivent tenir compte de la mise en œuvre prévue de la méthode PAP (« Prenez vos appareils personnels »), de l'émergence de la méthode PJI (« Prenez vos justificatifs d'identité ») et de différents modèles d'identité de confiance. Cela comprend l'évolution d'une identité numérique de confiance pour les services destinés au public afin de faciliter les connexions avec les différents ordres de gouvernement à travers le Canada.
- L'**authentification multifacteur** – une simple combinaison de nom d'utilisateur et de mot de passe n'est plus considérée comme étant acceptable pour bien qualifier un utilisateur. En vertu du nouveau paradigme, l'ajout de facteurs supplémentaires est essentiel : l'ajout de données biométriques, d'un jeton matériel ou d'un identificant installé sur l'appareil apporte un niveau d'assurance supplémentaire – quelque chose que vous êtes (biométrique), que vous possédez (jeton ou appareil) et que vous connaissez (mot de passe ou NIP).

- L'**expérience personnalisée, mais cohérente** – un niveau élevé de personnalisation et de cohérence se traduira par une augmentation du partage du profil utilisateur et des métadonnées, ce qui nécessitera des contrôles accrus de protection des données.

7.3.4. État futur

Alors que les menaces à la sécurité se sont multipliées ces dernières années, un changement de paradigme s'est opéré dans la réflexion architecturale sur la façon d'assurer un équilibre entre la protection et la disponibilité tout en soutenant l'évolution d'un nouveau modèle de sécurité centré sur l'information pour les réseaux du GC. Le modèle de réseau de l'état à venir tiendra compte des besoins des utilisateurs finaux tout en garantissant la sécurité de leurs données.

Du point de vue du contrôle d'accès, le changement le plus influent sera lié à la transition d'une approche traditionnelle de sécurité périmétrique vers un « périmètre virtuel »; une approche reposant sur la notion de « zéro confiance » et de microsegmentation appliquée aux réseaux et aux ressources du GC. La notion de zéro confiance repose sur le principe selon lequel il ne faut « jamais faire confiance et toujours vérifier ». L'architecture d'accès au réseau à zéro confiance (« ZTNA ») stipule qu'il faut vérifier tous les accès aux ressources, même s'il s'agit de sources traditionnellement fiables. La sécurité périmétrique traditionnelle peut encore servir de première ligne de défense, mais l'appareil et l'utilisateur seront vérifiés, authentifiés et autorisés en permanence afin d'accéder aux biens et aux ressources, d'où le besoin de microsegmentation, une vue plus granulaire des ressources du réseau. Cela aura des répercussions profondes sur la conception et le fonctionnement des mécanismes de contrôle d'accès.

7.3.5. Répercussions et dépendances

Les répercussions et dépendances suivantes devront être prises en compte pour que le réseau de la prochaine génération réponde aux attentes de l'utilisateur final et du gouvernement numérique en matière d'utilisation et de sécurité :

- **Besoin accru de gestion d'accès privilégié** (GAP) – À mesure que les services de réseau et la fourniture des ressources relèveront de plus en plus du contrôle des logiciels, un certain nombre de nouvelles cibles de sécurité de haut niveau émergeront (comme des tableaux de commande pour les composants du réseau, des moteurs de politique). Il faut en tenir compte et les gérer correctement au moyen de solutions de GAP. La GAP aide les organisations à restreindre l'accès privilégié dans l'environnement d'un répertoire actif existant. La GAP permet d'atteindre deux objectifs :
    - Reprendre le contrôle d'un environnement de répertoire actif compromis en conservant un environnement bastion distinct qui est à l'abri des attaques malveillantes.
    - Isoler l'utilisation de comptes privilégiés pour réduire le risque de vol de ces justificatifs d'identité.
- **Besoin accru de gestion des secrets (mots de passe et clés secrètes)** – Des processus appropriés de pipeline, de développement et de déploiement de type

IC/DC doivent être en place pour prendre en charge la livraison juste à temps des ressources et le passage au « réseau en tant qu'utilitaire ». Un service de gestion des secrets doit être prévu pour permettre l'automatisation et l'orchestration en plus d'être étroitement associé à des mécanismes de contrôle d'accès.

- **Accent accru sur la capacité des mécanismes de contrôle d'accès** – le passage à la ZTA entraînera des exigences accrues en matière de capacité pour tous les éléments des mécanismes de contrôle d'accès, car le processus d'authentification et d'autorisation de l'utilisateur final, de l'entité ou de l'appareil devient continu et multimodal. Une transition accrue vers des moteurs de risque « intelligents » entraînera des exigences additionnelles sur le plan de la capacité pour permettre la collecte et le traitement des métadonnées des utilisateurs finaux et des appareils de manière transparente et efficace.
- **Priorisation accrue de la gouvernance des données et des mesures de protection contre la fuite de données** – à mesure que des métadonnées supplémentaires relatives aux utilisateurs finaux et aux appareils sont recueillies et traitées, des attributs d'identité d'utilisateur de confiance externes sont acquis et utilisés pour permettre le déroulement des processus de vérification, d'authentification, d'autorisation et d'élaboration des politiques. Il sera encore plus important de pouvoir compter sur une gouvernance des données, une gestion des données de base et des protections efficaces contre les fuites de données.

7.4. Pilier 3 : Surveillance

7.4.1. Attention particulière relative à la sécurité

Étant donné que le Centre canadien pour la cybersécurité (CCC) est propriétaire du Centre des opérations de la sécurité (COS) et du processus de gestion de l'information et des événements de sécurité (GIES), de nombreux recoupements d'intérêts et de responsabilités seront mis en évidence dans cette section. Bien que ce document n'essaie pas de délimiter les tâches ou les responsabilités spécifiques, il sera essentiel d'évaluer les recoupements et de tenir compte des incidences et des changements opérationnels pour l'optimisation du modèle de processus. La référence à la solution de GIES a pour unique but de souligner que la GIES est effectivement nécessaire. On ne doit pas l'interpréter comme une fonction de SPC.

Selon les recherches menées par Gartner & Forrester et d'autres, l'état à venir des réseaux démontrera une convergence ou un alignement des domaines fonctionnels; cet état imposera un alignement des centres d'opérations, du Centre des opérations de réseau (COR) et du Centre des opérations de sécurisé (COS), de sorte qu'il a été proposé qu'un modèle de centre des opérations de réseau et de sécurité (CORS) devienne la voie de l'avenir. À mesure que SPC et le GC évoluent dans ce nouveau paradigme, des étapes intermédiaires ouvriront la voie à la convergence finale.

Alors que les événements de sécurité liés aux utilisateurs et au système resteront sous la responsabilité du COS (CCC), les intérêts de sécurité liés aux composants de l'infrastructure seront intégrés dans la solution de surveillance continue. Cela favorisera les capacités de réponse automatisée de l'IDL.

7.4.2. Aperçu

La surveillance consiste à gérer de manière proactive le rendement et la sécurité de l'infrastructure de TI du GC. La portée des capacités de surveillance s'étend aux dispositifs de réseautique et au trafic, aux serveurs et aux périphériques des utilisateurs finaux, ainsi qu'aux applications exécutées sur ces périphériques. Une surveillance efficace permet une identification proactive des événements liés aux appareils du réseau et permet de corriger ces événements pour accroître la sécurité, la fiabilité et la performance.

7.4.3. État actuel

Il existe dans l'ensemble du GC une combinaison d'outils et de données de surveillance gérés par les partenaires et gérés par SPC. Il en résulte un manque de clarté, de responsabilité et de couverture des fonctions de surveillance. Des compétences spécifiques et des configurations de solutions ont été adaptées aux besoins de chaque service. Les outils de surveillance sont utilisés pour les alertes et les rapports de base. System Center Operations Manager (SCOM) de Microsoft en est un exemple.

SPC dispose d'une capacité décentralisée et non standard de GIES qui est décentralisée et non standard (niveaux de maturité et configurations variés) et qui procure une couverture partielle. Cela signifie que SPC ne bénéficie pas d'une visibilité totale sur l'environnement du GC pour cerner les risques et réagir rapidement aux incidents.

La configuration de ces solutions permet d'automatiser plusieurs tâches opérationnelles simples, mais une intervention humaine est nécessaire pour tout ce qui est plus complexe. Le manque de capacités d'automatisation et d'orchestration et de corrélation entre les événements mène à des renseignements non pertinents et non exploitables que les équipes opérationnelles de TI doivent examiner. Cela entraîne des temps d'analyse et de résolution plus longs en plus d'éroder la prestation des services. De plus, le modèle opérationnel actuel de SPC rend la maintenance des ressources d'infrastructure coûteuse, en plus de demander un temps énorme et d'être propice aux erreurs humaines.

7.4.4. Tendances

Les organisations procèdent de plus en plus à la mise en œuvre de technologies qui assurent l'ingestion et la corrélation des sources de surveillance et de journalisation, regroupent ces données et appliquent à la fois la logique humaine et la logique machine pour détecter et exécuter des actions dans le but d'enquêter et de résoudre les incidents ou les événements. Ces plateformes comprennent l'orchestration et automatisation de la sécurité et intervention (OASI), l'analyse comportementale et l'IA. Le marché des produits pour ces solutions continue d'évoluer et les solutions n'ont pas encore atteint leur potentiel prévu (voir l'annexe A – Tendances en matière de réseau et de sécurité).

De plus, les organisations adoptent une position de « violation présumée ». Ce faisant, les entreprises intègrent la chasse aux menaces dans les capacités de surveillance de

la sécurité pour rechercher en permanence des anomalies qui pourraient révéler l'existence d'un cyberévénement.

7.4.5. État cible

Dans l'état cible, SPC devra passer des outils et processus de surveillance autonomes à un ensemble intégré de technologies qui sont prises en charge par un dépôt central de données qu'on qualifie ici de « lac de données de SPC » et qui offre une visibilité améliorée. SPC devra mettre en œuvre l'IA, l'automatisation et l'orchestration pour améliorer l'efficacité avec laquelle il sécurise l'infrastructure de TI. Une initiative est en cours au sein de SPC afin d'étudier l'IA pour les opérations (« AIOps »).

Figure 5 : Technologie multicouche AIOps

SPC, en coordination avec les partenaires, s'efforcera de réduire le nombre de solutions de surveillance dans l'état futur, en adoptant une approche » 70/30 », en vertu de laquelle un seul outil répond à 70 % des exigences de surveillance, alors que les 30 % restantes seront de multiples solutions ponctuelles. 70 % des outils doivent être des « solutions complètes » agnostiques du domaine pour les cas d'utilisation les plus courants. Les 30 % de ces « solutions ponctuelles », qui sont axées sur un domaine spécifique (par exemple, le réseau, la sécurité, les systèmes d'extrémité ou la surveillance du rendement des applications), devraient être centrées sur le domaine.

Il sera essentiel de consolider les centres de données pour faciliter la consolidation des outils de surveillance et du lac de données de SPC. Cela comprendra la mise en place, dans les CDE, d'une solution de surveillance centralisée qui représentera la base d'une capacité de surveillance centralisée pour le GC.

La maturation de la capacité de GIES sera essentielle pour acquérir une connaissance de la situation dans les environnements du GC et créer des capacités d'intervention plus rapides et coordonnées lorsque survient un incident. Cela devrait inclure une solution de GIES intégrée de la prochaine génération, l'adoption d'un contenu de cas d'utilisation avancé pour détecter les événements (à l'aide d'une combinaison d'analyses comportementales basées sur des règles et des utilisateurs ou des entités) et des capacités d'OASI pour améliorer la détection des menaces et automatiser la réponse. Il sera essentiel d'adopter une capacité de connaissance de la situation afin de prévoir les niveaux d'exposition des biens de TI aux cybermenaces et prendre des décisions de correction fondées sur le risque.

Pour prendre en charge l'agrégation et la corrélation des données, le lac de données de SPC sera créé et utilisé pour stocker et analyser les données de journalisation. Plus on insérera de données dans le système, plus il sera possible de prendre des décisions

intelligentes grâce aux technologies émergentes, comme l'apprentissage machine, l'OASI et l'IA. Pour réaliser des économies d'échelle plus importantes aux fins de l'analyse, SPC devrait étudier l'utilisation de solutions en nuage public de type IaaS ou PaaS pour son lac de données, dans lequel un modèle en nuage hybride est utilisé pour assurer la connectivité avec les CDE.

Les technologies et les solutions décrites ci-dessus continueront d'améliorer la correction automatique, l'infrastructure de réparation spontanée, la corrélation entre les événements et l'analyse prédictive. Le diagramme ci-dessous nous montre un système de GIES proposé pour la prochaine génération qui est pris en charge par un lac de données centralisé de SPC.

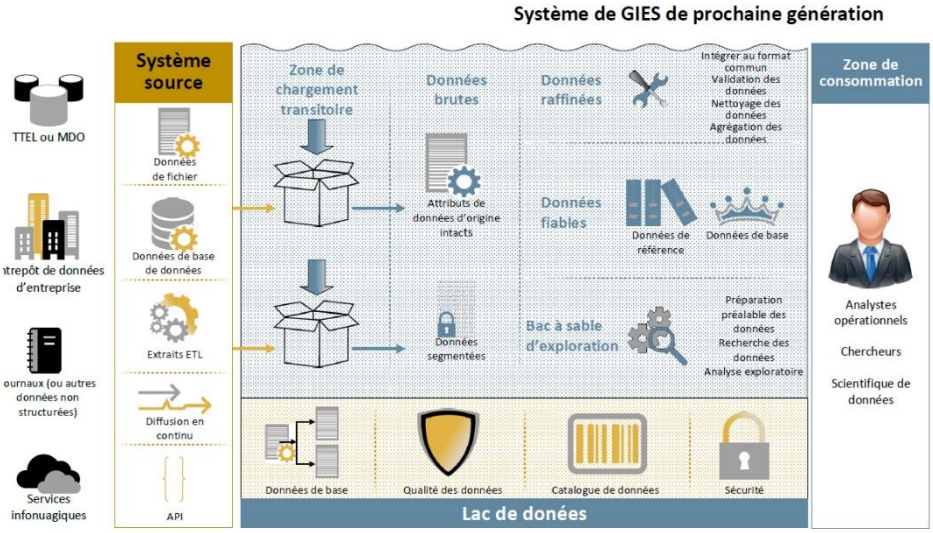


Figure 6 : Système de GIES de la nouvelle génération avec lac de données de SPC

7.4.6. Répercussions et dépendances

Les suites d'infrastructure de surveillance présentent des fonctionnalités étendues et intégrées, tandis que les meilleurs outils de surveillance sont dotés de fonctionnalités spécifiques au domaine. La principale dépendance pour réaliser la future stratégie de surveillance sera que tous les partenaires partagent les données de journalisation dans la pile technologique (y compris les données de performance des applications) avec SPC, et que ces données devront être stockées dans un dépôt central (lac de données de SPC). Cette intégration permettra de constater l'état général de la sécurité du GC, favorisera les cas d'utilisation avancée et accélérera les interventions en cas d'incidents. Il sera également essentiel pour SPC de collaborer avec les partenaires et le CCC pour s'assurer que les rôles et les responsabilités en matière de détection, d'intervention et de correction des incidents sont clairs.

7.5. Approvisionnement

7.5.1. Aperçu

L'approvisionnement fait référence à la capacité de la plateforme technologique et de la solution d'implanter les composants de la solution globale. Dans le contexte de la réseautique et de la sécurité, l'approvisionnement offre la possibilité de mettre en œuvre les composants du réseau et de sécurité, comme l'ajout ou la modification des configurations du réseau ou l'ajout ou la modification des règles de pare-feu. L'approvisionnement doit être vu de manière globale à tous les niveaux de a réseautique, du calcul et de la sécurité, en exploitant les capacités, comme l'IDL en tant que facilitateurs pour accroître les capacités d'approvisionnement.

7.5.2. État actuel

À l'heure actuelle, le GC compte un certain nombre de fournisseurs qui procurent des services de réseautique, de calcul et de sécurité (fournisseurs de matériel, de logiciels et de services). Cette situation a donné lieu à une prolifération des plateformes à travers le GC qui, dans de nombreux cas, nécessitent des solutions technologiques et des compétences uniques sur ces plateformes pour assurer leur gestion et leur surveillance.

Le délai d'approvisionnement est l'une des principales préoccupations des DPI. Les DPI dépendent de SPC en ce qui concerne la prestation de services de calcul, de stockage et de réseau afin de mettre en œuvre de nouvelles applications qui permettent la mise en œuvre des programmes du GC. Par conséquent, le délai d'approvisionnement de SPC est un des facteurs essentiels de l'exécution agile des programmes. L'objectif consiste à réduire le délai de prestation des services d'infrastructure de quelques semaines ou mois à quelques heures ou jours. De plus, bon nombre des plateformes de réseau, de calcul et de sécurité déjà existantes approchent ou ont dépassé la fin de leur durée de vie et doivent être remplacées afin de protéger les biens techniques du GC et pour les gérer de manière efficace.

La venue de nouvelles capacités technologiques mentionnées dans le présent document, comme la ZTA et le RDL, exigera que la plupart des plateformes de réseau et de sécurité existantes soient remplacées ou, à tout le moins, mises à niveau pour permettre ces nouveaux paradigmes de fonctionnement.

7.5.3. Tendances

Les domaines de la réseautique, du calcul et de la sécurité font l'objet d'une refonte en profondeur à mesure que les organisations se tournent vers des technologies habilitantes, comme l'informatique en nuage. Le nuage oblige à fournir immédiatement des services de réseautique, de calcul et de sécurité afin de prendre en charge les demandes dynamiques des services en nuage. L'utilisation des opérations d'IA favorise également la vitesse d'approvisionnement en automatisant de nombreuses tâches opérationnelles pour la prestation des services de TI.

7.5.4. État futur

Des capacités d'approvisionnement améliorées permettront de fournir les services de réseau, de calcul et de sécurité en quelques minutes (plutôt qu'en quelques jours ou semaines). Les tendances à l'origine du besoin d'améliorer l'approvisionnement sont les suivantes :

- L'innovation nécessite de nouvelles capacités.
- Les cybermenaces demandent des changements au réseau automatisé pour atténuer les menaces.
- Les DPI ont besoin rapidement de nouveaux environnements technologiques, ainsi que des services de réseau et de sécurité associés.

L'état futur verra la mise en œuvre de technologies habilitantes, telles que le RDL et l'IDL, intégrés à l'infrastructure locale, comme l'infrastructure hyperconvergée, le RDL et les plateformes de sécurité. Le nuage extérieur permettra de fournir rapidement des services de réseau, de sécurité et de calcul.

Il faut tenir compte de plusieurs approches lorsqu'il s'agit de fournir les capacités définies par logiciel, y compris la sélection d'une solution d'écosystème basée sur le fournisseur (comme l'infrastructure CISCO axée sur les applications, Contrail de Juniper, EOS d'Arista) ou une solution de source ouverte (comme le RDL OpenDayLight).

Dans l'état futur, SPC sera en mesure d'assurer un approvisionnement dynamiquement en solutions de réseau, de calcul et de sécurité par l'entremise d'une plateforme logicielle améliorant les délais d'approvisionnement et la satisfaction des clients à l'égard des DPI des ministères.

7.5.5. Répercussions et dépendances

La stratégie permettant d'accroître les capacités d'approvisionnement devra tenir compte des répercussions et des questions suivantes :

- De quelle façon les différentes solutions de réseau et de sécurité favorisent-elles les capacités (par exemple, l'architecture de réseau zéro confiance)?
- En quoi consiste le processus qui permet de définir et de mettre en œuvre une compétence intégrée en matière d'approvisionnement, en particulier si SPC entreprend une approche faisant appel à des fournisseurs multiples en matière de réseau et de sécurité?
- SPC entreprend-il le processus de normalisation des fournisseurs afin de fournir une capacité d'approvisionnement améliorée et intégrée ou opte-t-il pour la voie des solutions à fournisseurs multiples ou de source ouverte?
- L'auto-approvisionnement sera-t-il proposé dans le cadre de la stratégie, en particulier dans les domaines du calcul?
- Comment SPC aidera-t-il à intégrer les opérations d'automatisation et d'intelligence aux activités d'approvisionnement?

7.6. Considérations

7.6.1. Requalification et réoutillage de l'organisation

Compte tenu du rythme accéléré du changement que suscitent les progrès rapides de la technologie et les méthodes de travail de l'avenir, le personnel actuel de SPC devra adapter son modèle opérationnel, ses compétences et ses opérations pour prendre en charge la future plateforme de réseau et de sécurité.

Modèle d'exploitation

SPC devra entreprendre une transformation profonde de son modèle d'exploitation à mesure de son évolution vers le nuage et vers les nouvelles capacités de réseau et de sécurité. Cela nécessitera des changements en ce qui concerne les éléments suivants :

- Structure organisationnelle de SPC;
- Compétences requises;
- Processus opérationnels;
- Capacités de gestion des fournisseurs.

Le modèle opérationnel devra modifier fondamentalement la façon dont SPC est axé sur les services de réseau et de sécurité depuis le soutien technique quotidien jusqu'à l'équipe de direction.

Compétences

Les changements apportés au niveau du réseau et de la sécurité exigeront un nouvel ensemble de compétences et de capacités au sein de SPC, telles que :

- le réseautique zéro confiance pour concevoir, mettre en œuvre et exploiter l'environnement de l'état futur;
- une réseautique définie par logiciel et une infrastructure définie par logiciel qui représenteront le modèle opérationnel de l'avenir pour la conception et la prestation de services de réseau et de sécurité;
- des capacités relatives aux opérations de développement incluant une expérience au niveau des infrastructures en tant que code;
- l'adoption d'un mode de recherche avancée des menaces et la création d'un contenu avancé pour surveiller les événements de sécurité, y compris en utilisant l'analyse comportementale et en combinant le contenu organisationnel et de sécurité pour détecter les anomalies;
- le renouvellement des compétences de l'organisation pour améliorer et accroître ses compétences en matière de gestion des fournisseurs alors que SPC évolue vers un rôle de gestion des fournisseurs dans certains domaines de responsabilité et que l'organisation étend son utilisation des services gérés;
- l'exploitation des partenaires fournisseurs et des consultants pour combler les lacunes établies sur le plan des compétences grâce à un plan axé sur l'embauche de ces compétences ou sur la définition de contrats d'externalisation à long terme pour ces compétences.

Rôles et responsabilités

Les changements apportés au modèle opérationnel exigeront également que de nouveaux rôles soient définis à l'appui du modèle d'état futur au sein de SPC. De nouveaux rôles seront nécessaires, notamment les suivants :

- Architecte défini par logiciel;
- Architecte de ZTA;
- Gestion des fournisseurs;
- Priorisation accrue de la gestion des relations avec les partenaires dans tous les rôles.

Les questions qui se posent quant à l'avenir de la main-d'œuvre à SPC sont les suivantes :

- De quelles compétences aura-t-on besoin à l'avenir?
- Quelles tâches pourrions-nous automatiser ou confier à des talents différents?
- Comment pouvons-nous assurer la transition de la main-d'œuvre?
- Modification ou mise à niveau en cours des compétences?
- À quoi ressembleront les répercussions?
- Quel en sera le coût?

Pour répondre à ces questions, SPC devra entreprendre un programme de modèle opérationnel cible distinct pour :

- Comprendre les tendances externes, les priorités internes et les pressions que subissent les employés du ministère;
- Déterminer les compétences et les tâches clés qui sont nouvelles, croissantes ou décroissantes, puis établir la correspondance entre les compétences et les tâches et les rôles aux fins de la priorisation;
- Définir une approche pour combler le déficit de compétences prioritaires : numérisation et automatisation, embauche externe, emprunt de talents à court terme ou perfectionnement à l'interne;
- Élaborer le modèle opérationnel de TI (ITOM) de l'état à venir;
- Définir les rôles et les responsabilités nécessaires;
- Élaborer les processus de gestion du changement afin de gérer le changement opérationnel (très important) en suivant les pratiques exemplaires en matière de GSTI.

Les résultats de ce programme devraient orienter les stratégies d'atténuation des lacunes en matière de compétences et de rôles à l'échelle du ministère et de l'entreprise, en plus d'estimer les coûts de renforcement des compétences et les répercussions sur l'ensemble de la main-d'œuvre.

7.7. Prochaines étapes recommandées

Dans les sections précédentes, les piliers de l'état futurs ont été décrits en détail afin de décrire la voie que SPC doit suivre pour intégrer l'IDL et la ZTA. Dans cette section, nous décrirons les prochaines étapes nécessaires recommandées pour y parvenir en termes de principes, de projets et d'initiatives.

7.8. Les « principes »

Pour mettre cette stratégie en œuvre, des principes de base ont été élaborés en raison de la complexité de l'infrastructure de réseau et de sécurité de SPC. Il est impossible de se procurer et de mettre en œuvre d'un seul coup une IDL et une ZTA entièrement fonctionnelle. Pour cette raison, les principes stratégiques suivants sont recommandés :

Figure 7 : Étapes de base

7.9. Plan de communication

Un plan de communication détaillé est essentiel et doit être mis en œuvre pour partager la vision, la stratégie et le plan en matière de réseau et de sécurité pour l'avenir. Ce processus doit se dérouler au sein de SPC, et ce, tant au niveau de la haute direction qu'au niveau opérationnel pour garantir l'adhésion et la compréhension au sein de l'organisation. Cependant, il ne s'agit pas uniquement d'une initiative de SPC; pour que cette initiative réussisse, il faut pouvoir compter sur l'aide et l'adhésion de tous les partenaires de SPC, car cela s'étend jusqu'aux services commerciaux et aux applications que SPC fournit à ces partenaires.

7.10. Architectures de référence

Des documents d'architecture de référence (DAR) doivent être élaborés afin de fournir une architecture, une méthodologie, des lignes directrices et des principes pour les

différentes technologies à un niveau élevé et ces documents doivent être répartis en fonction des différents niveaux de service. Les DAR :

1. Présenteront les relations par rapport à la vision et la stratégie en matière de réseau et de sécurité de SPC;
2. Permettront de comparer et d'harmoniser les exigences de SPC avec les technologies émergentes de l'industrie;
3. Fourniront des lignes directrices et des principes qu'il faudra suivre en lien avec les services, les produits et les projets;
4. Seront axés sur la fonction plutôt que sur les technologies.

Un DAR directeur général sera d'abord élaboré. Il s'agira d'une architecture qui interconnecte tous les DAR secondaires afin de garantir la cohérence des objectifs généraux entre les fonctions et les technologies interdépendantes.

Les DAR secondaires seront élaborés et reliés au DAR directeur général. Les DAR secondaires qui devraient être élaborés dans un premier temps sont les suivants :

1. RLDL (RL défini par logiciel);
2. REDL (RE défini par logiciel);
3. CDDL (centre de données défini par logiciel);
4. Connectivité du nuage, de l'Internet et de l'accès à distance;
5. CDE/RCD (centre de données d'entreprise/réseau de centres de données – réseau central);
6. ZTA (architecture zéro confiance).

7.11. Soutenir les initiatives en cours

Des projets et initiatives existants sont actuellement en cours et planifiés depuis un certain temps. Plusieurs d'entre eux auraient été identifiés avant même que les concepts d'IDL ou de ZTA ne soient bien connus. Cependant, bon nombre de ces projets et initiatives sont des éléments importants de l'infrastructure de base pour amener SPC vers l'IDL et la ZTA.

Il est recommandé que les responsables des projets en cours et des nouveaux projets prennent le temps de réfléchir à la vision et à la stratégie en matière de réseau et de sécurité de SPC, ainsi qu'aux « principes » définis dans ce document, et qu'ils collaborent avec SPC pour déterminer les possibilités visant à harmoniser les activités de manière encore plus optimale que ce qui était initialement prévu dans les projets.

Le tableau suivant présente une liste des projets de SPC et des sous-initiatives importantes qui soutiennent la vision et la stratégie en matière de réseau et de sécurité pour l'avenir et qui devraient continuer à être soutenus par SPC.

Projet	Description	Sous-projets ou initiatives

ADNS	Activation et défense du nuage sécurisé	• ADNS principale • Portiers en sécurité infonuagique (PSI)
ADR (maintenant GCVDC)	Authentification des dispositifs réseau/Gestion du cycle de vie des dispositifs chiffrés	S.O.
CARGC	Contrôle de l'accès au réseau du GC	S.O.
GIES	Gestion de l'information et des événements de sécurité	• Système de journalisation centralisé (SJC) • OASI • GIES (traditionnelle) • Analyse du comportement des utilisateurs et des entités (ACUE) • Visibilité de l'infrastructure, sensibilisation et sécurité (VISS)
GRJC	Gestion des répertoires, des justificatifs et des comptes	S.O.
GVCE	Gestion de la vulnérabilité et de la conformité d'entreprise	S.O.
MADP	Migration de l'accès à distance protégé	S.O.
MRP	Modernisation du réseau périphérique	S.O.
RGC	Réseau de gestion centralisé	S.O.
SACI	Service d'authentification centralisé interne	S.O.

SCAA	Service de contrôles d'accès administratifs	S.O.
SCR	Stratégie des centres régionaux	S.O.
SPE	Sécurité du périmètre de l'entreprise (SPE)	S.O.
VSSPT	Visibilité, sensibilisation et sécurité de point de terminaison	S.O.

Tableau 3 – Soutenir les projets et les initiatives de SPC

La carte des points chauds suivante montre comment chacun des projets ci-dessus s'harmonise avec la vision en matière de réseau et de sécurité.

● Pleine valeur ajoutée ▲ Valeur partielle

Projet	IDL	ZTA	Surveillance continue
GIES-SJC	S.O.	●	●
GIES-OASI	●	●	●
GIES-ACUE	S.O.	●	●
GIES-VISS	S.O.	●	●
GIES-principale	S.O.	●	●
VSSPT	●	●	●
GVCE	▲	▲	●
RCC	●	●	●
GRJC	●	▲	S.O.
SCAA	▲	●	●
ADR	▲	●	▲
SACI	▲	●	S.O.
CARGC	●	▲	▲
MRP	●	▲	▲
GADP	●	●	●
SCR	●	▲	▲
ADNS-PSI	●	▲	▲
ADNS-principale	●	▲	▲

Tableau 4 – Carte des points chauds d'harmonisation du projet

7.12. Initiatives futures requises

Le résumé de la feuille de route en matière de réseau et de sécurité présentée ci-dessous, *Annexe B : Feuille de route en matière de réseau et de sécurité*, décrit les étapes progressives nécessaires pour passer de l'état actuel à l'état final projeté vers l'architecture logicielle et la ZTA. Cette évolution nécessitera la mise en place de certaines étapes et technologies spécifiques pour chacune de ces disciplines ainsi que l'augmentation et l'évolution des services d'identité et de la sécurité. Le schéma suivant nous présente un résumé de l'adoption progressive recommandée des initiatives futures nécessaires qui devront être soutenues pour continuer de faire évoluer SPC vers l'architecture logicielle et la ZTA. Pour plus de détails, veuillez consulter le document complet de la feuille de route en cliquant sur le lien ci-dessus.

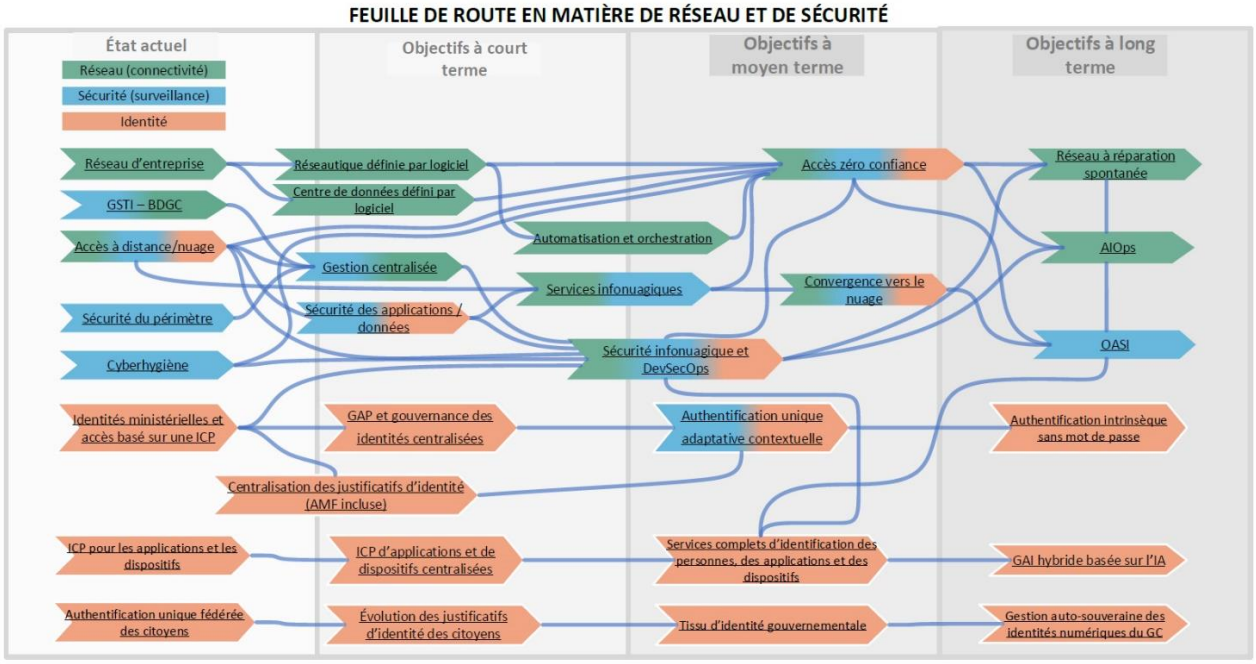


Figure 8 : Initiatives à venir

8. Conclusion

Tout au long du présent document, trois thèmes persistants sont mis en évidence :

1) l'accélération continue du changement;
2) la nécessité de suivre ces changements tout en maintenant la sécurité et le contrôle;
3) le caractère essentiel de la collecte et de l'utilisation des données de surveillance et d'analyse.

« Le changement est inévitable » est depuis longtemps un mantra dans les cercles de TI, mais l'ampleur et le rythme du changement continuent de poser le plus grand défi. L'adoption et l'intégration des services en nuage et l'acceptation de l'expansion de l'empreinte technologique de l'IdO, non seulement dans le centre de données, mais à tous les niveaux dans la vie personnelle et professionnelle modifient les attentes des utilisateurs quant à la manière, au moment et à l'endroit où l'accès aux systèmes GC est nécessaire.

L'établissement et l'adoption de technologies (y compris le réseau, la sécurité, le calcul, le stockage) qui peuvent évoluer en permanence occupent une place primordiale, mais la modernisation des processus et des politiques qui définissent l'utilisation et la fonction de la technologie est tout aussi essentielle. L'acceptation sociale doit précéder l'adoption de ce paradigme technologique essentiellement nouveau.

La surveillance, ou « surveillance continue », telle qu'elle a été décrite tout au long du présent document, propose d'aller au-delà de la surveillance traditionnelle des fonctions, des performances et de la sécurité. Ces modes de surveillance seront et doivent rester intégrées dans toute solution, mais ce qui était au départ une convergence entre les appareils et les fonctions se poursuivra et comprendra de manière prévisible les renseignements sur la sécurité des utilisateurs et des appareils et l'autorisation du moteur de politique. Ce modèle amélioré rassemblera beaucoup plus de « données de surveillance » qu'auparavant, permettra aux différentes équipes de recueillir des données correspondant à leurs besoins et favorisera davantage l'intégration de solutions basées sur l'intelligence artificielle afin d'exploiter les capacités de l'infrastructure définie par logiciel de demain.

9. Sigles et acronymes

Acronyme	Description
AA	Apprentissage automatique
ADNS	Activation et défense du nuage sécurisé
ADP	Accès à distance protégé
AIOps	Intelligence artificielle pour les opérations informatiques
GAP	Gestion d'accès privilégié
GIES	Gestion de l'information et des événements de sécurité
IA	Intelligence artificielle
IC/DC	Intégration continue/développement continu
IdO	Internet des objets
IDL	Infrastructure définie par logiciel
IRR	Interface réseau à réseau
NaaS	Réseau en tant que service
OASI	Orchestration et automatisation de la sécurité et intervention
PAP	Prenez vos appareils personnels
PJI	Prenez vos justificatifs d'identité
PSON	Plan stratégique des opérations numériques
RE	Réseau étendu
RL	Réseau local
RM	Réseau métropolitain
RDL	Réseau défini par le logiciel

TCP/IP	Protocole de contrôle de transmission/protocole Internet
Wi-Fi	Marque déposée faisant référence à la famille de normes sans fil 802.11 pour l'accès au réseau sans fil
ZTA	Architecture zéro confiance ou Accès zéro confiance – un cadre architectural remplaçant la « défense en profondeur » traditionnelle
ZTNA	Accès au réseau zéro confiance

10. Références

1. Conseils en matière de sécurité des technologies de l'information n° 33 (ITSG-33) : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie
2. Stratégie de l'informatique en nuage d'abord, stratégie SPC 3.0
3. Plan stratégique des opérations numériques du gouvernement du Canada (GC) de 2018 à 2022

Annexe A – Tendances en matière de réseau et de sécurité

Les tableaux suivants décrivent les différentes tendances qui sont les plus pertinentes pour la vision stratégique de SPC. Certaines de ces tendances sont courantes, tandis que d'autres ne sont pas aussi matures, mais elles gagnent en popularité sur le marché. Une définition, une analyse et une application pour SPC sont présentées pour chaque tendance.

Tendance nº 1 – Architecture zéro confiance

Qu'est-ce que l'architecture zéro confiance (ZTA)?
La ZTA fait appel à une approche définie par logiciel pour établir un périmètre et crée une frontière d'accès logique basée sur l'identité et le contexte autour d'une application ou d'un ensemble d'applications. Les applications sont cachées pour en empêcher la découverte, alors que l'accès est limité par un courtier de confiance à un ensemble d'entités nommées. Le courtier vérifie l'identité, le contexte et le respect de la politique des participants choisis avant d'autoriser l'accès. Cette façon de faire supprime les ressources de l'application de la visibilité publique et réduit considérablement la zone d'attaque. Bien que les offres de ZTA diffèrent de par leurs approches techniques, elles présentent généralement la même proposition de valeur fondamentale : • Retrait des applications et des services de la visibilité directe sur l'Internet public. • Accès granulaire aux applications validé par un programme ou par un accès basé sur les rôles et en appliquant le principe de privilège minimal. • Validation de l'accès indépendamment de l'emplacement physique de l'utilisateur. Les politiques d'accès sont basées sur les identités des utilisateurs, des appareils et des applications. • Accès accordé uniquement à l'application spécifique, mais non à l'infrastructure sous-jacente du réseau. Cela limite le besoin d'un accès excessif à tous les ports et protocoles ou à toutes les applications, dont certaines peuvent ne pas être autorisées par l'utilisateur. • Chiffrement de bout en bout des communications sur le réseau. • Inspection facultative du flux de trafic pour les risques excessifs sous forme de traitement des données délicates et de logiciels malveillants. Activation de la surveillance facultative de la séance pour les indications d'activité inhabituelle, de durée ou de besoins en matière de bande passante.

Analyse des tendances
Le marché de la ZTA en est encore à ses débuts, mais il se développe rapidement – l'intérêt porte principalement sur les organisations à la recherche d'une solution plus flexible aux RPV et à celles qui recherchent un contrôle d'accès plus granulaire aux applications.

Applicabilité à SPC

- Mise à jour de leur cadre de sécurité réseau daté actuel
- Harmonisation avec la stratégie de l'informatique en nuage d'abord de SPC – de nouveaux périmètres sont établis
- Expérience utilisateur cohérente pour accéder aux applications – sans client ou par l'entremise d'un client de la ZTA quel que soit l'emplacement du réseau
- Intégration des techniques d'automatisation au cadre de sécurité

Tendance nº 2 – Périmètre défini par logiciel

Qu'est-ce que le périmètre défini par logiciel (PDL)?

La ZTA est généralement mise en œuvre par l'entremise de PDL et de la microsegmentation. Le PDL est une nouvelle technologie très polyvalente qui offre un accès confidentiel et sécurisé aux applications d'entreprise. La technologie est mise en œuvre dans le logiciel sur les appareils des utilisateurs finaux, les passerelles, les contrôleurs ou les serveurs. Un PDL peut s'acquérir comme un produit autonome (exploité par l'équipe réseau) ou en tant que service.

Analyse des tendances

Le PDL est une technologie plus récente, qui consiste pour les fournisseurs à ajouter rapidement des fonctionnalités ou des facteurs de forme nouveaux. Les nouvelles fonctionnalités comprennent tout particulièrement les interfaces du portail de gestion et les flexibilités sur les plans de l'attestation et des politiques. Les facteurs de forme supplémentaires comprennent les appareils de passerelle virtuelle clé en main, les fonctions de réseau virtuel (FRV) et les images logicielles sur les marchés du nuage public.

Le PDL et les technologies définies par logiciel en général bouleverseront le marché des fournisseurs de matériel traditionnel.

Le PDL n'est généralement pas utilisé pour accéder aux applications SaaS telles que Microsoft Office 365, Salesforce ou ServiceNow. Ainsi, les PDL ne recoupent pas les PSI.

Applicabilité à SPC

- Mise à jour de leur cadre de sécurité réseau daté actuel
- Confirme au mandat qui consiste à offrir un accès à distance sécurisé aux utilisateurs finaux
- Consolidation des réseaux peut être facilitée à mesure que les composants des réseaux vieillissent

Tendance nº 3 – Microsegmentation

Qu'est-ce que la microsegmentation?

La microsegmentation est une capacité fondamentale qui prend en charge la ZTA. Par le passé, les clients étaient paranoïaques à propos des intrusions de l'extérieur touchant les périmètres de leur centre de données d'entreprise. Ils étaient convaincus d'avoir perdu le combat si une violation se produisait dans le sens nord-sud. La mentalité a maintenant évolué et les clients reconnaissent que des violations

puissent se produire et qu'elles se produisent et ils doivent chercher des moyens de réduire le plus possible les dommages. Avec la venue de l'automatisation et des logiciels plus performants, la microsegmentation a gagné un vaste public dans sa capacité d'atténuer les dommages causés par une intrusion lorsque le périmètre du centre de données a été compromis.

La microsegmentation réduit au minimum l'intrusion lorsqu'elle se produit inévitablement. Au lieu d'utiliser des adresses IP et des zones de sécurité pour établir des politiques de segmentation, les politiques sont basées sur des attributs logiques (et non physiques) et procurent un contrôle d'accès granulaire aux applications.

Analyse des tendances

La virtualisation des réseaux est courante depuis un certain nombre d'années déjà, agissant ainsi en tant que catalyseur de la microsegmentation. Elle devient de plus en plus courante et semble être la meilleure solution pour lutter contre la limitation du trafic est-ouest.

Des solutions de microsegmentation de réseau plus avancées assurent la surveillance et les flux de base, et émettent des alertes en cas d'anomalies. Elles évaluent également en permanence les niveaux relatifs de risque et de confiance du comportement observé au cours de la session réseau (par exemple, modèles de connectivité inhabituels, bande passante excessive, transferts de données excessifs et communication vers des URL ou des adresses IP avec de faibles niveaux de confiance). Si une session réseau représente trop de risques, une alerte peut être déclenchée ou la session peut être interrompue.

Applicabilité à SPC

- Confinement des violations provenant de l'intérieur du centre de données (trafic est-ouest)
- Intégration efficace dans une architecture de microservices
- Harmonisation avec les exigences d'automatisation
- Mise en œuvre et gestion beaucoup plus faciles
- Application de stratégies de segmentation cohérentes touchant les charges de travail sur place et dans le nuage
- Bonne adaptation aux charges de travail qui hébergent des conteneurs répondant aux exigences de conformité

Tendance nº 4 – Service d'accès sécurisé en périphérie

Qu'est-ce que le service d'accès sécurisé en périphérie (SASE)?

Les exigences des activités numériques et de l'informatique en périphérie bouleversent les systèmes de trafic traditionnels, transformant ainsi fondamentalement ce modèle et entraînant une convergence des marchés d'extrémité de RE et de la sécurité des réseaux vers le SASE. Le SASE combine généralement des produits et des services pour offrir de nombreuses capacités telles que le REDL, le contrôleur d'optimisation de réseau étendu, la passerelle Web sécurisée (PWS), les PSI, le pare-feu de prochaine génération (PFPG), la ZTA et le PDL.

Analyse des tendances

Au cours des prochains mois, il y aura un certain nombre d'offres dans ce domaine, mais elles seront basées sur des appareils spécialement conçus pour une distribution diversifiée, originaires du nuage, basés sur le nuage et optimisés pour fournir des services à très faible latence.

Il faut savoir qu'au cours de cette transition, il y aura une grande quantité de logiciels de diapositives et de contenu marketing, en particulier de la part des titulaires qui ne sont pas bien préparés au modèle de diffusion dans le nuage à partir de points de présence distribués.

L'inversion des modèles de réseautique et de sécurité réseau établis par cette technologie transformera le paysage concurrentiel et offrira aux entreprises l'occasion de réduire la complexité et permettra à leur personnel de TI d'éliminer les aspects banals des opérations de réseau et de sécurité réseau.

Le SASE permettra de consolider les solutions en matière de PSI, de PWS et de périmètre défini par logiciel, offrant ainsi un moyen transparent permettant aux utilisateurs de se connecter aux applications de type SaaS, aux sites Web sur l'Internet et aux applications privées (qu'elles soient hébergées sur place ou dans le nuage public de type IaaS) en fonction du contexte et de la politique.

Applicabilité à SPC

- Harmonisation avec SPC 3.0 – meilleure expérience de l'utilisateur final
- Capacité d'offrir une connectivité plus sûre et plus performante à l'échelle internationale
- Meilleure évolutivité – dépendance moindre à l'égard des solutions ponctuelles et des longs délais d'approvisionnement pour le matériel
- Consolidation des solutions en matière de PSI, de PWS et de PDL, offrant ainsi un moyen unifié aux utilisateurs du GC de se connecter aux applications de type SaaS, aux sites Web sur l'Internet et aux applications privées (qu'elles soient hébergées sur place ou dans le nuage public de type IaaS)

Tendance n° 5 – Orchestration et automatisation de la sécurité et intervention

Qu'est-ce que l'Orchestration et automatisation de la sécurité et intervention (OASI)?

L'OASI est une autre de ces nouvelles expressions à la mode qu'on entend autour de nous. La communauté des fournisseurs de sécurité est fière de faire la promotion de ce terme lors de la commercialisation de ses produits. Le fait est que l'automatisation et la correction complètes ne sont pas encore disponibles dans l'industrie et ne le seront pas avant quelques années. Les fournisseurs vantent leurs capacités en les qualifiant d'entièrement automatisées, mais en réalité, ils font l'une des deux choses suivantes :

- Exploitation des scripts externes en tant que modules complémentaires à leurs offres de base en tant que correctif
- Intégration avec d'autres produits pour fournir un ensemble de solutions d'automatisation plus robuste

Les outils d'OASI sont des technologies qui permettent aux organisations de recevoir des données provenant de diverses sources (principalement des systèmes de GIES) et d'appliquer des flux de travaux alignés sur les processus et les procédures. Les capacités supplémentaires comprennent des fonctions de gestion des cas et des incidents; la capacité de gérer les renseignements sur les menaces, les

tableaux de bord et les rapports; et des analyses qui peuvent s'appliquer à différentes fonctions. Les outils d'OASI améliorent considérablement les activités des opérations de sécurité comme la détection et la réponse aux menaces en fournissant une aide machine aux analystes humains pour améliorer l'efficacité et la cohérence des personnes et des processus.

Voici quels sont les aspects de l'OASI – dans le contexte des opérations de sécurité :

- Agrégation : La possibilité d'agréger ou d'ingérer des données provenant de plusieurs sources.
- Enrichissement : Que ce soit après l'identification de l'incident ou pendant la collecte et le traitement des données, les solutions d'OASI peuvent aider à intégrer les renseignements sur les menaces externes, effectuer des recherches contextuelles internes ou exécuter des processus pour recueillir des données supplémentaires en fonction d'actions définies.
- Orchestration : La complexité de la combinaison des ressources suppose la coordination des flux de travaux avec des étapes manuelles et automatisées, impliquant de nombreux composants et ayant un effet sur les systèmes d'information et souvent aussi les humains.
- Automatisation : Ce concept suppose la capacité des logiciels et des systèmes à exécuter eux-mêmes des fonctions, généralement pour influencer d'autres systèmes d'information et applications.
- Intégration : La réponse manuelle ou automatisée apporte une solution standard aux activités définies par programme.

Analyse des tendances

Le marché de l'OASI en est encore à ses tout premiers balbutiements. De nombreuses acquisitions ont eu lieu au cours des dernières années et cela devrait se poursuivre alors que les fournisseurs tentent d'améliorer la capacité de leurs plateformes existantes ou de les remplacer complètement. Les clients doivent être conscients de cette tendance et prévoir des mesures d'urgence si leur plateforme d'OASI actuelle est acquise par une autre entreprise.

Un certain nombre d'entreprises mettent en œuvre des outils d'OASI avec des cas d'utilisation principalement axés sur l'amélioration de l'efficacité de leurs analystes du COS afin qu'ils puissent traiter un plus grand nombre d'incidents tout en ayant plus de temps pour appliquer l'analyse humaine et accélérer les mesures d'intervention.

Applicabilité à SPC

- Harmonisation avec le mouvement de SPC qui consiste à accroître l'automatisation et l'orchestration
- Optimisation du COS
- Amélioration en matière de pénuries de personnel et de manque de compétences
- Surveillance des menaces et réponse
- Enquête sur les menaces et réponse
- Gestion des renseignements en matière de menace

Tendance nº 6 – Intelligence artificielle pour les opérations informatiques

Qu'est-ce que l'intelligence artificielle pour les opérations informatiques (AIOps)?

Les plateformes d'AIOps offrent la possibilité d'améliorer et, dans certains cas, de remplacer les plateformes des opérations de TI traditionnelles, principalement dans les domaines de la corrélation et de l'analyse d'événements. Elles exploitent les données volumineuses et les fonctionnalités d'apprentissage automatique pour analyser de vastes ensembles de données en réaction à la transformation numérique.

Voici certaines des capacités principales des plateformes d'AIOps :

- L'ingestion de données provenant de plusieurs sources, y compris l'infrastructure, les réseaux, les applications, le nuage ou les outils de surveillance actuels (pour l'analyse interdomaine);
- L'activation de l'analyse des données à l'aide de l'apprentissage machine en deux points :
  - L'analyse en temps réel au point d'ingestion (analyse en continu),
  - L'analyse historique des données stockées;
- Le stockage et l'accès aux données;
- La proposition de réponses normatives à l'analyse;
- Le déclenchement d'une action ou une étape suivante en fonction de la prescription (résultat de l'analyse).

Analyse des tendances

La tendance pour les plateformes d'AIOps repose sur une approche d'un gestionnaire de gestionnaires (GdG) en vertu de laquelle d'autres plateformes d'opérations de TI envoient leurs données à la plateforme d'AIOps afin qu'elle procède à une analyse agrégée et produise des rapports, menant ainsi à une gestion opérationnelle plus simplifiée et plus efficace. Idéalement, les organisations recherchent une approche indépendante du domaine des AIOps qui puisse répondre à la plupart de leurs besoins. Cependant, aucune plateforme n'est actuellement disponible pour répondre à tous les besoins des clients et une approche de solutions centrée sur le domaine est adoptée pour combler cette lacune.

Puisque ces plateformes misent sur les technologies d'IA, elles dépendent de très vastes ensembles de données pour montrer leur efficacité et elles ne sont pas destinées à être déployées de manière isolée ou cloisonnée. Autrement dit, plus la plateforme a accès aux données, plus elle a de valeur. Grâce à l'avènement des données volumineuses, l'AIOps affichera une meilleure valeur au fil du temps.

Applicabilité à SPC

- Service de production de rapports plus simple et mieux centralisé
- Meilleure visibilité des infrastructures des partenaires – ANS amélioré
- Bon cas d'utilisation pour un lac de données centralisé – les données des ministères partenaires peuvent alimenter la solution pour offrir une valeur supérieure

Tendance nº 7 – Services gérés en réseau – réseau étendu défini par logiciel

Qu'est-ce que le réseau étendu défini par logiciel (REDL)?

Le REDL est une approche définie par logiciel en matière de gestion des RE. Voici les principaux avantages :

- Elle permet un transport agnostique sur plusieurs protocoles tels que la MPLS, la 3G, la 4G et la LTE.
- Elle améliore le rendement des applications opérationnelles et augmente l'agilité et la réduction des coûts.
- Elle optimise l'expérience utilisateur et l'efficacité des applications SaaS et celles dans le nuage public.
- Elle simplifie les opérations grâce à l'automatisation et à la gestion en nuage.

Les fournisseurs de REDL gérés gèrent de manière opérationnelle les produits de REDL des clients, qui sont des appareils physiques ou des instances logicielles appartenant à l'entreprise ou comprises dans le service. Les produits de REDL gérés résident généralement dans les locaux du client, sont régis par un ANS et sont facturés sur une base mensuelle récurrente. Les fournisseurs proposent des services de REDL gérés indépendamment ou conjointement avec le transport RE. Pour être considéré comme un fournisseur de services de REDL gérés, le fournisseur doit proposer un point de contact unique (PCU) pour toute la gestion, y compris le transport RE, l'équipement des locaux du client du REDL et les fonctions logicielles requises.

Analyse des tendances

Les solutions de REDL sont désormais courantes et les options offertes aux entreprises en matière de services de REDL gérés évoluent parallèlement à la croissance de la technologie REDL. Les options de conception de RE hybride continueront de s'étendre (et continueront d'être affectées par les services de REDL gérés).

Les capacités de sécurité du REDL continueront de s'étendre au-delà du pare-feu de base, car de plus en plus de fournisseurs intègrent la gestion unifiée des menaces comme la PWS, le SDI/SPI, etc. De plus, les capacités d'optimisation et d'accélération du RE augmenteront au fur et à mesure qu'augmentera le nombre de fournisseurs qui intègrent des caractéristiques techniques du réseau afin d'améliorer la qualité du service et le débit.

Applicabilité à SPC

- Bonne solution de rechange relativement aux coûts à considérer lorsque les contrats de MPLS actuels devront être renouvelés
- Potentiel d'externalisation en tant que service géré
- Diversité des chemins pour la disponibilité et la réduction des coûts
- Bonne harmonisation avec le passage de SPC vers une « infrastructure définie par logiciel »
- Bonne solution de rechange pour les applications non sensibles à la latence
- Option envisageable pour les nouveaux sites construits dans des endroits éloignés

Tendance nº 8 – Internet des objets

Qu'est-ce qu'Internet des objets (IdO)?

La notion d'IdO est définie comme suit :

« Un réseau de choses physiques (objets) qui contiennent une technologie intégrée afin de détecter ou d'interagir avec leur état interne ou leur environnement externe et qui sont capables d'envoyer et de recevoir des données en direction ou en provenance d'une plateforme numérique distante. »

Analyse des tendances

Cinq tendances de l'IdO à incidence élevée

- **IA :** L'IA s'appliquera à un vaste éventail de renseignements de l'IdO, y compris la vidéo, les images fixes, la parole, l'activité du trafic sur le réseau et les données des capteurs.
- **IdO social, juridique ou éthique** : À mesure que l'IdO évolue, les problèmes de propriété et l'interprétation biaisée de ces données seront un sujet de préoccupation.
- **Courtage des données :** Les données du système d'IdO peuvent être vendues à des personnes ou utilisées par des personnes autres qui ne sont pas l'appareil ou le propriétaire qui les a créées.
- **Maillage de l'IdO :** Les couches de l'architecture périphérique se dissoudront pour créer une architecture davantage non structurée composée d'un vaste éventail d' » objets » et de services reliés à l'intérieur d'un maillage dynamique et flexible.
- **Gouvernance de l'IdO** : La gouvernance englobe la gestion opérationnelle des appareils de l'IdO, ainsi que les renseignements et les services fournis par les systèmes de l'IdO.

Applicabilité à SPC

- Surveillance de l'utilité et de la sécurité des biens immobiliers
- Surveillance des performances des appareils intelligents du GC
- Économies de coûts
- Sécurité
- Inspection à distance de l'ACIA
- Équipement d'inspection aux passages frontaliers
- Systèmes nationaux de vidéosurveillance

Tendance nº 9 – Réseau 5G privé

Qu'est-ce que le réseau 5G privé?

Un réseau 5G privé, également appelé réseau 5G local ou non public, est un réseau local qui fournit une bande passante dédiée à l'aide de la technologie 5G. La 5G est la prochaine version des réseaux de données sans fil 4G ou LTE. La 5G introduit une bande passante plus élevée en utilisant un spectre radio différent qui permettra également à un plus grand nombre d'appareils de se connecter

simultanément. Tous les principaux fournisseurs de services au Canada procèdent présentement à sa mise en œuvre. Un réseau privé 5G (local) est un réseau local qui fournit une bande passante dédiée à l'aide de la technologie 5G.

Les déploiements 5G privés et publics valident l'IdO. On s'attend à ce que les fournisseurs de services proposent des réseaux superposés sur le réseau public 5G permettant la création de RPV redirigés vers des réseaux privés. Il s'agit d'une solution de rechange au déploiement d'équipement 5G privé et cela offre la possibilité d'externaliser ce modèle de connectivité au lieu d'une solution intégrée au Canada.

Analyse des tendances

Avec la version 16, la 5G pourrait devenir la technologie de RL et de RE prédominante au monde au cours des 10 à 20 prochaines années, en particulier dans les nouvelles constructions. Les nouveaux bâtiments, usines, ports ou campus peuvent réduire considérablement leur utilisation des connexions filaires en mettant en œuvre la 5G privée. Les cinq prochaines années devraient voir un essor des mises en œuvre privées de la 5G dans des endroits qui bénéficieraient grandement d'une meilleure technologie sans fil en termes de vitesse, de capacité et de latence.

À court terme, la 5G offrira une bande passante plus élevée et des connexions à latence plus faible, dans de nombreux cas, sous forme de réseaux d'accès sans fil fixes et de premiers réseaux d'IdO.

Applicabilité à SPC

- Communications de l'IdO
- Nouvelles constructions dans des endroits éloignés (échelle internationale)
- Vidéo HD
- Améliorations des bâtiments du GC

Tendance n° 10 – Réseautique en nuages

Qu'est-ce que la réseautique en nuages?

Alors que de plus en plus de clients optent pour une approche en nuages pour offrir des services de TI, ils recherchent un moyen plus transparent de les gérer et de les exploiter. La réseautique en nuages fait référence à l'infrastructure réseau pour prendre en charge l'utilisation des services en nuage de plusieurs fournisseurs de nuage publics, y compris la connectivité aux fournisseurs et entre ceux-ci.

Les solutions de réseautique en nuages sont basées sur des logiciels et fournissent une politique de réseau cohérente entre plusieurs fournisseurs en nuage. Elles comprennent les réseaux superposés, la gestion des API des fournisseurs en nuage ou d'autres mécanismes. La réseautique en nuages ressemble à une structure Ethernet dans laquelle plusieurs composants sont gérés comme une seule structure et la stratégie est créée de manière centralisée.

Analyse des tendances

Bien que le calcul en nuages soit devenu plus courant, la réseautique en nuages en est aux premiers stades de son adoption. Un certain nombre d'organisations peuvent mettre en œuvre l'informatique en nuages sans la réseautique en nuages, et la plupart le font.

Entre temps, cependant, les organisations qui cherchent à mettre en œuvre des solutions de réseautique en nuages doivent recourir à des solutions de virtualisation de réseau sur plusieurs nuages

telles que Cisco ACI et VMware NSX pour combler les lacunes ou traiter les fonctionnalités opérationnelles essentielles lorsque les capacités d'origine du nuage n'offrent pas cette capacité.

Applicabilité à SPC

- Connectivité transparente et interface de gestion centrale entre plusieurs fournisseurs
- Capacité de production de rapports centralisée
- Réduction de la dépendance ou de l'asservissement aux fournisseurs
- Déplacement des ressources de stockage entre les fournisseurs lorsque les prix changent

Tendance nº 11 – Réseautique à la demande

Qu'est-ce que les services de réseau à la demande (RD)?

Les services de RD sont des services de transport du RE assurés par des fournisseurs de services de réseau (FSR) et des fournisseurs de services gérés (FSG). Ils sont généralement offerts par l'entremise d'un portail ou de l'API d'un fournisseur. Les changements de capacité et de configuration peuvent être effectués à la volée en temps réel et ne sont pas fixes. Les changements peuvent être effectués par le client à la demande et ne doivent pas faire l'objet d'un processus de commande interminable.

Ces services sont souvent basés sur une technologie définie par logiciel et permettent de modifier en temps réel les attributions des ports et de la bande passante. Les clients peuvent même ajouter et supprimer des points de terminaison de réseau, comme la connexion au nuage et les connexions avec l'extranet.

Analyse des tendances

Pour prendre en charge la connectivité en nuage et l'IdO, il existe une nouvelle génération de services de réseau à la demande qui offrent une agilité et une flexibilité accrues. À l'heure actuelle, le principal cas d'utilisation de ces nouvelles offres concerne la connectivité à de nouveaux points de terminaison, comme les services en nuage. Ils peuvent également prendre en charge une migration du trafic réseau en provenance de la MPLS vers les services Internet.

Les organisations qui désirent profiter de ces services cherchent principalement à optimiser les coûts et l'agilité. Les solutions de réseau à la demande commenceront à présenter des taux d'adoption plus élevés, en particulier en ce qui concerne les services de bande passante dynamique à mesure qu'ils continuent d'évoluer, puisqu'ils ajoutent une plus grande valeur aux entreprises en termes de vitesse et de flexibilité.

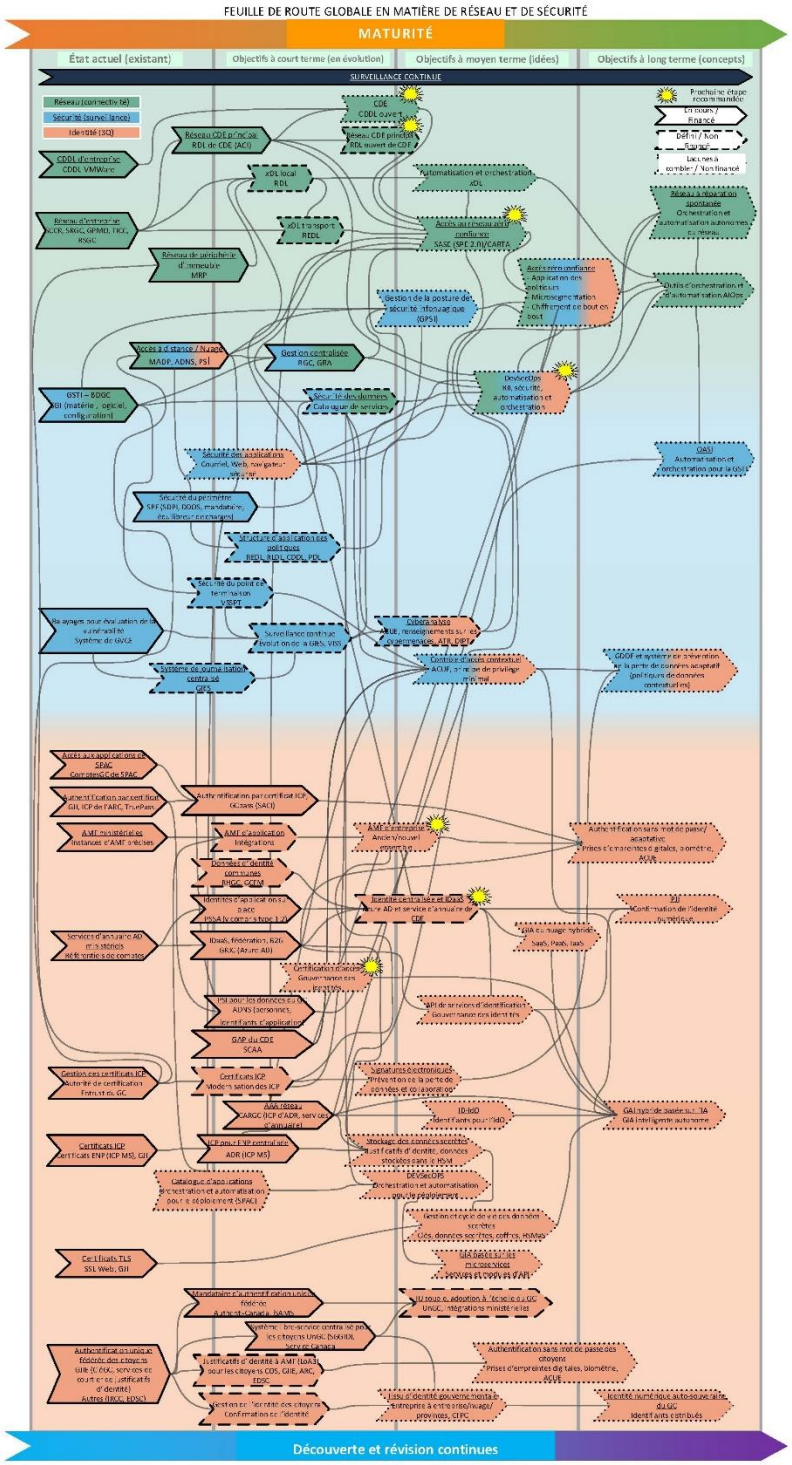
Les services vocaux et de données doivent représenter un élément clé lors de l'évaluation des services de réseau à la demande (RD).

Applicabilité à SPC

- Migration et consolidation simplifiées du réseau
- Approvisionnement à la demande du site utilisant un réseau périphérique et de la connectivité du nuage
- Meilleure expérience de l'utilisateur pour les services vocaux et de données

- Optimisation des coûts
- Meilleure planification des capacités

Annexe B : Feuille de route en matière de réseau et de sécurité



Annexe C : Projets en cours

*Voir la section 3 pour consulter le tableau des facteurs opérationnels

ADNS – Activation et défense du nuage sécurisé
Procure une connectivité sécurisée en nuage pour les charges de travail de niveau Protégé B. Doit être considéré comme faisant partie de toute exigence de connectivité du réseau externe, comme mentionné dans la section Connectivité. SPC est toujours en train de déterminer si les composants de PIF ou PAN d'ADNS résideront sur place ou dans le nuage, ce qui aura une incidence sur la solution de surveillance.

Résultat :

- Périmètre de réseau de point d'interconnexion fiable du gouvernement du Canada (PIF du GC) pour la connectivité au nuage afin de répondre à la demande en nuage sur le réseau à l'échelle du GC
- Points d'accès au nuage du gouvernement du Canada (PAN du GC) : périmètres de sécurité centralisé applicable aux environnements infonuagiques publics afin que les communications par Internet traversent des zones démilitarisées publiques et privées
- Connexion avec le fournisseur de services d'échange sur le nuage : connexion à haut débit et à faible latence des fournisseurs de services en nuage (FSN)
- Mise en œuvre d'un fournisseur de services de sécurité d'accès au nuage (PSI) afin de fournir des points d'application de la politique de sécurité
- Journalisation et gestion centralisés de tous les composants mis en œuvre pour prendre en charge le périmètre et le service du PSI, capturant les événements de sécurité pour le trafic sur le nuage et les transmettant à la GIES

Dépendances :

- Le personnel de SPC et du CST doit développer, déployer et exploiter le système d'ADNS
- Services déployés par le CST pour inspecter un volume élevé de trafic sur le réseau
- La GIES assurera la prédiction et la détection des cybermenaces
- Projet de réseau de gestion centralisé (RGC) pour fournir une solution de gestion de réseau d'entreprise
- Stratégie de gestion de l'identité, des justificatifs d'identité et de l'accès (GIJIA) par les SAM de la DGCSTI et de SPC afin de fournir une solution de contrôle d'accès pour le nuage
- Projet de sécurité du périmètre d'entreprise (SPE) de la DGCSTI : exploiter la solution des périmètres GCNet
- Solution élaborée et exploitée par le CST, le CCC et le COS

- Stratégies élaborées par les SAM de SPC pour : la gestion des adresses IP (GAIP), le serveur de noms de domaine (DNS), la gestion des systèmes/application des mesures de gestion des politiques des FSN

Pilier : Connectivité

Échéancier : Année 1

VSSPT – Visibilité, sensibilisation et sécurité de point de terminaison

Approche d'entreprise en matière de sécurité des points de terminaison améliorant la visibilité et la connaissance de tous les appareils d'extrémité sur les réseaux du GC et de SPC afin de fournir une connaissance de la cybersituation dans l'ensemble de l'entreprise du GC et de SPC. Découverte et évaluation automatisées des biens pour prendre en charge les correctifs du système d'exploitation et des applications, la gestion des devises et les exigences de renforcement

Résultat :

- Visibilité et surveillance d'au plus 900 000 points de terminaison du GC, offrant une protection au niveau de l'hôte
- Permet à l'entreprise d'obtenir et de consolider les données de différents ministères et partenaires afin de créer une vue d'entreprise
- Données devant aider à corriger et renforcer le système d'exploitation et les applications, identifier les périphériques non gérés
- Atténuation de la menace posée par les vulnérabilités du jour zéro
- Participation à la planification, aux prévisions et à la gestion du cycle de vie des activités de TI : repérer les systèmes désuets, les licences inutilisées

Dépendances :

- Disponibilité des ressources et des effectifs pour construire, déployer et exécuter le système VSSPT (visibilité, sensibilisation et sécurité de point de terminaison)
- Infrastructure suffisante pour héberger et exécuter les outils de VSSPT
- Organisations d'intervenants et de partenaires pour définir les exigences et assurer l'acceptation
- Le Comité tripartite sur la sécurité de la TI agira en tant que signataire des artefacts du projet
- Le SCT doit créer une politique du GC concernant les délais de production de rapports et de correctifs en ce qui concerne le système VSSPT

Pilier : Contrôle d'accès

Échéancier : Année 1

GVCE – Gestion de la vulnérabilité et de la conformité d'entreprise

Vulnérabilité, services et capacités en matière de conformité de l'entreprise fournissant une approche et une solution technologique unifiées pour la gestion des vulnérabilités.

Résultat :

- Analyse des vulnérabilités et de la conformité pour le centre de données d'entreprise, l'infrastructure et le périmètre de TI, le Wi-Fi, les réseaux et les postes de travail
- Évaluation automatisée et intégrée de la vulnérabilité et de la conformité de l'entreprise, y compris la production de rapports, pour évaluer en permanence l'exposition des systèmes et des infrastructures de TI et détecter les faiblesses
- Balayage d'au plus 500 000 adresses IP accessibles sur Internet, capacité de prendre en charge jusqu'à 2 000 000 adresses IP à l'avenir
- Mise en place d'un service de gestion de la conformité au sein du groupe de gestion de la sécurité de SPC

Dépendances :

- Disponibilité des ressources et des effectifs pour construire, déployer et exécuter la solution en matière de GVCE
- Organisation partenaire devant fournir les exigences
- Le Comité tripartite sur la sécurité de la TI fournit des réponses en tant que signataire
- Infrastructure de TI pour exécuter et héberger des outils en toute sécurité
- Le SCT crée une politique du GC pour la modification et la production de rapports sur les MV, les délais de réponse
- Déploiement du réseau de gestion de la sécurité, bande passante du réseau pour prendre en charge le déploiement de la GVCE partenaire

Pilier : Contrôle d'accès

Échéancier : Année 1

ADR – Authentification des dispositifs réseau

L'ADR fait partie du programme de sécurité de l'infrastructure d'entreprise de SPC pour mettre en œuvre un service d'authentification de dispositifs réseau d'entreprise qui comprend une authentification du réseau basée sur des certificats.

Elle centralise la gestion du cycle de vie des certificats d'entités qui ne sont pas des personnes (ENP) et fournit des rapports sur les transactions d'authentification, d'autorisation et d'audit (AAA) pour l'audit de sécurité, la conformité et l'amélioration des services.

Résultat :

- Automatisation de l'approvisionnement des certificats d'ENP et prestation de services AAA au GC, des capacités d'authentification réseau basées sur des certificats pour fournir une AMF
- Le service fournit des justificatifs d'identité des appareils à l'échelle du GC et un mécanisme d'authentification standard
- Infrastructure à clé publique (ICP) de confiance centrale pour fournir des certificats d'ENP consolidant plus de 52 solutions de certificats déjà existantes
- Amélioration des contrôles d'accès, de la gestion, de l'audit et de l'analyse judiciaire des données et l'historique d'accès au réseau associés aux utilisateurs et aux appareils
- Gestion centralisée de l'authentification des ENP aux points d'accès au réseau avec un service d'usager commuté à authentification distante (RADIUS)
- Validation du contrôle d'accès au réseau et amélioration de l'audit et du rapport d'utilisation des certificats du réseau
- Adoption plus poussée du chiffrement des données en transit sur les réseaux du GC améliorant la défense en profondeur

Dépendances :

- Acquisition de licences en vertu de l'accord d'entreprise avec Microsoft et participation et aide des fournisseurs
- Connectivité et débit adéquat entre les centres de données de SPC et les réseaux partenaires
- Contrôles d'accès aux services de gestion des privilèges et gestion des identités (gestion des identités et de l'accès, GIA) en place

Pilier : Contrôle d'accès

Échéancier : Année 2

MADP – Migration d'accès à distance protégé

Intégrer et rationaliser entièrement l'infrastructure d'accès à distance protégé (ADP) existante et consolider le processus de connexions ADP dans les centres de données d'entreprise (CDE). Transformer les services d'ADP en un service de données d'entreprise à partir d'un service ministériel.

Résultat :

- Consolidation des solutions d'accès à distance du client à la porte (en grande partie non structurées) dans l'ensemble du GC et des solutions d'accès à distance de porte-à-porte toujours mises à jour pour les bureaux distants en dehors de GCNet
- Prestation d'une gamme complète de services de collecte, d'analyse et de traitement des journaux pour répondre au mandat du COS de SPC qui consiste à

fournir des données en temps opportun pour détecter les menaces et intervenir en cas d'incident

- Rationalisation et déplacement des anciennes passerelles d'ADP des anciens centres de données vers le CDE en installant des passerelles au niveau des CDE pour prendre en charge le volume de trafic d'un ensemble de services ministériels
- Télétravail accru, réduction des coûts des locaux à bureaux et augmentation des possibilités d'emploi et présence dans les collectivités éloignées

Dépendances :

- Dotation en personnel : disponibilité de ressources qualifiées pour créer, déployer et exécuter la MADP
- Programme de consolidation des centres de données de SPC
- Espace physique de CDE pour héberger la solution de MADP
- Services d'annuaire : s'assurer que la nouvelle passerelle est capable d'authentifier les utilisateurs
- Les services des utilisateurs finaux d'ADP doivent configurer les points de terminaison pour migrer vers la nouvelle MADP
- Bande passante du réseau : des vitesses de connexion présentant un débit adéquat sont nécessaires

Pilier : Contrôle d'accès

Échéancier : Année 2

MRP – Modernisation du réseau périphérique

Le projet Éclaireur de MRP définira un service de réseau reproductible qui pourra être utilisé pour déployer la structure et les services du réseau d'entreprise dans l'ensemble du GC. L'infrastructure physique standard doit être de la plus haute qualité et de la dernière technologie pour prendre en charge tout service ou utilisateur du GC et permettre une véritable mobilité. Le projet Éclaireur de MRP jettera les bases pour permettre à tous les travailleurs du GC d'avoir accès aux plus de 3 500 emplacements du GC en tant que sites de travail potentiels. Il fournira les éléments de base pour la virtualisation et l'automatisation du réseau.

Résultat :

- Normalisation des services entraînant une offre de services simplifiée et une prestation améliorée des services : en entreprenant le projet Éclaireur, il sera possible de comprendre le catalogue de services qui sera offert dans le cadre du déploiement du projet Éclaireur de MRP et la meilleure méthode de prestation de services pour les clients du GC.
- Une infrastructure de réseau établie nécessaire pour permettre la prestation d'autres services et solutions : en utilisant une approche exploratrice, le projet sera en mesure de fournir une infrastructure de réseau d'entreprise qui pourra ensuite

être reproduite avec succès sur les 3 500 sites restants, plutôt que d'essayer de concevoir, de créer et de déployer en même temps.

Dépendances : Voir l'analyse de rentabilité de MRP pour la liste complète des dépendances

Pilier : Connectivité

Échéancier : Années 3 à 5

RGC – Réseau de gestion central

Améliore l'expérience des ressources de soutien en offrant un guichet unique afin de gérer en toute sécurité toutes les infrastructures et tous les services des partenaires situés dans les centres de données (CDE et centres déjà existants), améliorant ainsi la disponibilité et la fiabilité des services.

Résultat :

- Réduction de la complexité des utilisateurs en uniformisant les outils et un seul ordinateur portable pour gérer les anciens réseaux des partenaires.

Dépendances : Comment la connectivité se fera-t-elle?

Pilier : Approvisionnement

Échéancier : Années 3 à 5

SPE – Sécurité du périmètre de l'entreprise

La ZTA est une approche architecturale clé pour la stratégie en matière de réseau et de sécurité pour l'avenir et suppose que le périmètre du réseau est devenu un périmètre « virtuel ». SPC devra s'assurer que la conception et l'architecture du projet de SPE sont alignées sur les principes clés d'une ZTA.

Résultat :

- Périmètre de réseau modernisé capable de résister au paysage actuel des menaces et d'absorber les attaques de type DDoS
- Protection du périmètre du gouvernement du Canada, quelles que soient les frontières physiques et virtuelles
- Connectivité sécurisée de l'utilisateur final à partir de n'importe quel endroit
- Exploitation des principes architecturaux de la ZTA en gardant à l'esprit le principe de privilège minimal

Dépendances : Projets RGC, SPE, GAIP, DNS et ADNS

Pilier : Contrôle d'accès

Échéancier : Année 1 (en cours)

GIES – Gestion de l'information et des événements de sécurité

Solution de GIES d'entreprise du GC entièrement intégrée offrant une visibilité et une réponse automatisée aux cyberattaques. Elle permet une détection accélérée des menaces et une réponse aux incidents de sécurité.

Résultat :

- Permet au COS de SPC d'améliorer la prédiction des cybermenaces, d'augmenter la capacité de détection et de détecter et d'identifier des menaces plus complexes
- Soutient le mandat du COS de SPC qui consiste à fournir des renseignements opportuns et précis pour soutenir la détection des menaces et la réponse aux incidents de sécurité
- Système basé sur l'intelligence artificielle pour analyser l'analyse du comportement des utilisateurs et des entités (ACUE) afin d'améliorer les capacités de GIES basées sur des règles
- Exploite les flux de renseignements sur les cybermenaces (CTI) pour obtenir des renseignements contextuels afin d'aider à mettre à jour les contre-mesures de protection avant une attaque
- Capacité de collecte centralisée des journaux pour faciliter la détection des menaces, les enquêtes et l'accès à l'information, augmentant ainsi la couverture de GIES et la visibilité des journaux

Dépendances :

- Création, déploiement et exécution de la GIES
- Le Comité tripartite sur la sécurité de la TI fournit des réponses rapides en tant que signataires des artefacts du projet
- Infrastructure pour héberger la GIES en toute sécurité
- Projet de suivi des processus d'évaluation et d'autorisation de SPC en matière de cybersécurité et de sécurité informatique
- Harmonisation avec les exigences et les méthodologies de CCC

Pilier : Contrôle d'accès

Échéancier : Année 1

SACI – Service d'authentification centralisé interne

Le service d'authentification centralisé interne fournit une capacité d'authentification centralisée pour que l'authentification des utilisateurs finaux ne se fasse plus à chaque application d'entreprise du GC, offrant ainsi une solution d'authentification pangouvernementale.

Le passage à la ZTA entraînera des exigences de capacité accrues pour tous les composants de SACI, car le processus d'authentification et d'autorisation centralisée

de l'utilisateur final, de l'entité ou de l'appareil devient continu et multimodal. Ce programme devra être harmonisé avec la ZTA.

Résultat :

- Plateforme d'authentification consolidée et centralisée pour le gouvernement
- Réduction des solutions ponctuelles présentement utilisées
- Réduction du risque global au niveau de la sécurité grâce à un cadre d'authentification standard et contrôlé

Dépendances :

- Architecture de réseau de la nouvelle génération
- Compréhension des futurs services et cas d'utilisation à prendre en charge avec certaines estimations de capacité (p. ex., IdO)

Pilier : Contrôle d'accès

Échéancier : Année 1

Profils du milieu de travail numérique du GC

Série normalisée de profils d'expérience de l'employé qui se fondent sur les fonctions en vue d'établir un milieu de travail numérique normalisé, ainsi que des services connexes de TI centrés sur les employés qui seront schématisés et dispensés.

Il existe deux activités qui s'unissent autour de la définition de l'espace de travail numérique :

- Biens immobiliers de SPAC définit le milieu de travail de l'avenir, y compris les centres de collaboration
- Une offre de services uniformisée afin de réduire les délais d'exécution et de mieux s'aligner sur le lieu de travail physique de l'avenir.

Résultat :

- Tout employé du GC peut travailler à partir de n'importe quel bâtiment sans barrières ministérielles
- Expérience utilisateur améliorée
- Évitement des excédents
- Sélection optimisée des outils
- Achats mieux gérés au sein du ministère

Dépendances : S.O.

Pilier : Contrôle d'accès

Échéancier : Année à déterminer