Lignes directrices pour l'évaluation de la résilience de l'accès à Internet au Canada

Lignes directrices pour les utilisateurs à domicile, les travailleurs à distance, les petites entreprises, les entreprises et les FSI

V1.0 – 8 septembre 2023

PRÉPARÉES PAR :

Groupe de travail sur la résilience de l'Internet (GTRI) du Forum canadien pour la résilience des infrastructures numériques (FCRIN)

Le contenu de ce document est **TLP:CLEAR**

Table des matières

Figures

Historique des révisions

Le tableau suivant indique les dates des principales modifications apportées à ce document.

Auteurs	Date / Version	Remarques
Groupe de travail sur la résilience de l'Internet du FCRIN	8 sept. 2023 Version 1.0	TLP:CLEAR Version 1.0

1. Introduction

Les Canadiens et les entreprises canadiennes dépendent d'une connectivité à Internet fiable et de haute qualité, qui a été intégrée dans presque tous les éléments de la société et de l'économie. Tout comme l'électricité et l'eau courante, une connexion à Internet est désormais une nécessité de base. Les particuliers ont besoin d'être connectés pour toute une série de raisons personnelles, notamment pour l'accès aux services gouvernementaux, les opérations bancaires en ligne, ainsi que pour remplir leurs obligations professionnelles, en particulier le travail à distance. Les entreprises de toutes tailles, les gouvernements, les établissements d'enseignement et autres organisations dépendent également d'une connectivité ininterrompue pour mener leurs activités, qu'il s'agisse de fournir un accès à Internet à leurs employés ou, le cas échéant, pour offrir du commerce en ligne. Compte tenu de l'importance de ces services, toute perturbation peut avoir des répercussions négatives importantes sur l'économie.

Lorsqu'une panne de grande ampleur se produit, comme celle qui a touché l'ensemble du réseau Rogers en juillet 2022, de nombreux particuliers, de nombreuses entreprises et autres organisations n'ont pas en place de mesures appropriées leur permettant d'accéder à Internet en utilisant une méthode différente jusqu'à ce que le service soit rétabli. Les fournisseurs de services Internet (FSI) peuvent ne pas être en mesure de garantir la protection de leurs réseaux contre les pannes, qu'elles soient dues à une erreur humaine, à une cyberattaque, à une catastrophe naturelle ou à d'autres événements imprévus.

2. Qu'est-ce que la résilience de l'accès à Internet?

Tout d'abord, nous devons définir ce qu'est l'« accès à Internet ». L'accès à Internet désigne la capacité à se connecter à Internet à l'aide d'un appareil, tel qu'un ordinateur, un téléphone intelligent ou une tablette, par le biais d'un fournisseur de services Internet (FSI). Il permet aux utilisateurs d'accéder à des sites Web et à des services en ligne, et de communiquer avec d'autres personnes par le biais de diverses plateformes en ligne. L'accès à Internet peut être filaire ou sans fil, et peut être fourni par différentes technologies, notamment DSL, mobilité, câble, fibre, satellite en orbite basse ou satellite.

La résilience de l'accès à Internet est la capacité à fournir aux utilisateurs et aux applications un niveau acceptable de service Internet lorsqu'une panne survient. La résilience peut être obtenue en adoptant des pratiques exemplaires éprouvées pour minimiser les interruptions de connectivité. Un système résilient est un système capable de se remettre d'une défaillance et de maintenir ou de rétablir rapidement un niveau de service acceptable pour l'utilisateur.

Bien que les deux concepts soient liés, la résilience est plus qu'une simple redondance. La redondance consiste à dupliquer intentionnellement les composants d'un réseau en cas de défaillance. Le fait d'avoir deux connexions Internet distinctes provenant du même fournisseur et arrivant dans une petite entreprise est un exemple de redondance. Cette redondance ne suffirait toutefois pas à la protéger d'une panne du réseau du FSI. Pour que l'entreprise dispose d'une connectivité Internet résiliente, chacune des deux connexions à Internet doit être fournie par un FSI différent (ce qui représente une diversité de FSI). Si une panne survenait dans le réseau d'un FSI, l'entreprise pourrait utiliser la connexion distincte du second FSI pour s'assurer qu'elle ne perd pas sa connectivité.

Le présent document examine sept scénarios de résilience de l'accès à Internet, allant d'une simple connexion à Internet à domicile à une connexion à Internet d'entreprise complexe. Chaque scénario examine l'éventail des éléments qui peuvent influer sur la résilience globale de l'accès à Internet et propose des lignes directrices aux lecteurs qui souhaitent augmenter la résilience de leur accès à Internet et réduire le risque de perte de connectivité. L'objectif de ce document est de fournir aux personnes et aux organisations de toutes tailles des lignes directrices sous forme de conseils afin de réduire leurs risques et d'augmenter la résilience de leur connectivité à Internet.

3. Public cible

Si l'accès à Internet est omniprésent et influe sur la vie quotidienne de la plupart des gens, ce n'est pas tout le monde qui a besoin de se préoccuper de la résilience de l'accès à Internet. Le présent document s'adresse à des groupes particuliers d'utilisateurs au Canada, notamment les utilisateurs de connexions à Internet résidentielles, les télétravailleurs, les petites entreprises, les entreprises et les fournisseurs de services Internet (FSI), qui peuvent avoir un besoin accru de connectivité résiliente en raison du caractère essentiel de leurs activités en ligne. Ces groupes sont confrontés à des défis différents pour maintenir la résilience de l'accès à Internet, et ce document fournit des lignes directrices et des recommandations pour les aider à atténuer ces défis. Pour les autres utilisateurs qui n'entrent pas dans ces catégories, le document peut tout de même fournir des renseignements utiles sur les pratiques exemplaires pour maintenir une connexion Internet stable, mais l'accent est mis sur ceux qui ont un plus grand besoin de résilience en matière d'accès à Internet.

Le présent document s'adresse aux groupes suivants au Canada :

- utilisateurs canadiens de connexions à Internet résidentielles
- télétravailleurs
- petites entreprises
- entreprises
- fournisseurs de services Internet (FSI)

Pour simplifier le présent document, nous incluons dans la catégorie FSI les fournisseurs suivants :

  - fournisseurs de services Internet résidentiels
  - fournisseurs de services Internet commerciaux
  - fournisseurs de services de transit Internet

4. À propos du Forum canadien pour la résilience des infrastructures numériques (FCRIN)

Le Forum canadien pour la résilience des infrastructures numériques (FCRIN)[1] est une collaboration publique-privée volontaire, consensuelle et axée sur l'action qui a été créée pour améliorer la résilience des infrastructures numériques essentielles du Canada, ce qui se traduit par une économie numérique digne de confiance pour les Canadiens et une industrie de la cybersécurité prospère.

Innovation, Sciences et Développement économique Canada (ISDE) a créé le FCRIN en 2020, en partie pour appuyer la Stratégie nationale sur les infrastructures essentielles du Canada. Dans le cadre de cette stratégie, ISDE est le ministère fédéral responsable du secteur des infrastructures essentielles des technologies de l'information et des communications (TIC). Le FCRIN réunit les principaux partenaires fédéraux et l'industrie pour améliorer la résilience des infrastructures numériques.

[1] https://ised-isde.canada.ca/site/gestion-spectre-telecommunications/fr/savoir-plus/comites-intervenants/conseils-comites/forum-canadien-pour-resilience-infrastructures-numeriques-fcrin

4.1. Collaborateurs

Accenture
IAN ZWIREK
LORRIE CHAN

CIRA
JACQUES LATOUR

Internet Society
HOSEIN BADRAN

Centre canadien pour la cybersécurité
ELIAS SREIH

CANARIE
MARK WOLFF

NEXICOM
BRUCE BUCHANAN

SÉCURITÉ PUBLIQUE CANADA
ROBERT PITCHER

TorIX
KEVIN BLUMBERG

5. Scénarios de résilience de l'accès à Internet

Les sections suivantes décrivent sept scénarios de résilience de l'accès à Internet pour différents types d'utilisation d'Internet, en commençant par le scénario le plus basique d'accès à Internet résidentiel et en augmentant la complexité jusqu'aux scénarios de résilience pour les entreprises et les grands fournisseurs de réseau Internet.

Chaque scénario comprend l'objectif de résilience, la tolérance aux pannes de l'utilisateur ou de l'organisation mise en avant, ou encore des recommandations pour augmenter la résilience. L'objectif de ces scénarios est d'éduquer les lecteurs et de leur fournir les bonnes questions à poser pour déterminer le niveau de résilience de leur accès à Internet et prendre les bonnes mesures pour l'améliorer.

Il est important de noter que la mise en œuvre des lignes directrices présentées dans le présent document peut avoir un coût. En outre, ces recommandations ne sont pas obligatoires et peuvent ne pas s'appliquer dans tous les cas.

Il est essentiel de comprendre que la résilience de l'accès à Internet peut nécessiter un investissement important en temps et en ressources. Si des mesures peuvent être prises pour augmenter la résilience de l'accès à Internet, il est important de reconnaître que ces mesures peuvent avoir un coût. La mise en place d'une infrastructure d'accès à Internet résiliente peut nécessiter des ressources supplémentaires en matériel, en logiciels et en personnel.

Scénario 1 : Résilience de l'accès à Internet résidentiel

Public : Utilisateurs canadiens d'Internet résidentiel

Les Canadiens n'ont jamais été aussi dépendants d'un accès à Internet de haute qualité. La disponibilité relativement élevée du haut débit offre aux Canadiens de nouvelles possibilités de participer à notre démocratie et à notre économie, et de rester en contact avec leurs amis et leur famille.

Alors que la vie quotidienne se déroule de plus en plus en ligne, une connectivité ininterrompue pour les utilisateurs d'Internet résidentiel est devenue de plus en plus importante. Alors que le gouvernement travaille avec les fournisseurs de services Internet (FSI) pour améliorer la résilience, de nombreux Canadiens peuvent s'interroger sur les mesures qu'ils peuvent prendre pour réduire le risque de subir des pannes de leur connectivité à Internet.

Discussion

De nombreux utilisateurs d'un accès à Internet résidentiel ne disposent pas d'une connectivité résiliente, soit parce qu'ils n'ont pas de méthode de secours pour se connecter à Internet, soit parce que la méthode de secours sur laquelle ils comptent est fournie par le même FSI que celui qui leur fournit leur connexion principale. Dans ce scénario et les suivants, un « FSI » est défini

comme une organisation qui fournit des services pour l'accès à Internet et son utilisation. Les FSI peuvent être organisés sous différentes formes : commerciaux, appartenant à la collectivité ou à but non lucratif. Les FSI vendent généralement des services d'accès à Internet aux particuliers, aux entreprises et aux gouvernements. Au Canada, les exemples de FSI comprennent notamment Rogers, Bell, TELUS et TekSavvy.
La *Figure 1* illustre un point unique de défaillance de l'accès à Internet pour un utilisateur d'Internet résidentiel. Dans cet exemple, si la connexion tombe en panne, l'utilisateur n'a pas d'autre moyen de se reconnecter jusqu'à ce que le FSI corrige le problème, ce qui risque d'entraîner une panne de longue durée.

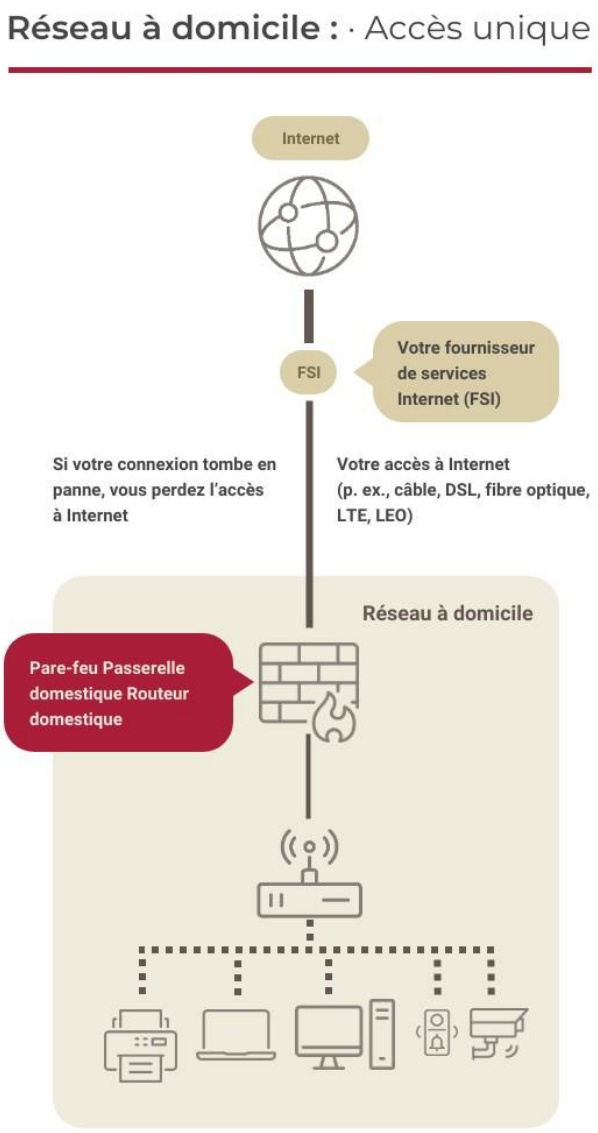

Figure 1 – Panne d'une seule connexion Internet – utilisateur privé

Objectif de résilience

L'utilisateur domestique doit évaluer le niveau de résilience dont il a besoin en fonction de l'usage qu'il fait d'Internet. Le besoin de résilience de l'accès à Internet est différent si l'on accède à des services Internet tels que la voix sur IP, le courriel, les services bancaires et gouvernementaux en ligne, les jeux, les services de diffusion en continu, et pour surveiller des appareils à distance, notamment des caméras de sécurité, des moniteurs pour animaux de compagnie, des détecteurs de chute pour les personnes âgées et des capteurs pour alarmes médicales.

Le présent document ne traite pas de la préparation des personnes aux situations d'urgence. Veuillez consulter le document suivant d'ISDE sur les mesures à prendre pour rester connecté en cas d'urgence en matière de télécommunications.

- Mesures à prendre pour rester connecté – Télécommunications d'urgence : comment nous nous préparons, réagissons et travaillons avec nos partenaires pendant une crise ou une catastrophe (canada.ca)

Tolérance aux pannes

La tolérance aux pannes pour les utilisateurs d'un accès à Internet résidentiel peut avoir un éventail très large. Si un utilisateur n'utilise pas Internet pour son travail et n'en a pas besoin pour assurer sa sécurité personnelle, il peut généralement tolérer une panne de plusieurs heures. Si l'utilisateur doit avoir un accès à Internet pour son travail, ou si un membre de sa famille doit faire l'objet d'une surveillance des chutes ou doit communiquer en permanence des données provenant de capteurs médicaux, sa tolérance aux pannes est faible et il ne peut pas faire face à une panne de longue durée.

Recommandations pour l'augmentation de la résilience

- Installez une alimentation électrique de secours pour votre modem ou votre passerelle et votre point d'accès sans fil qui, selon sa capacité, alimentera les services Internet pendant une durée déterminée en cas de panne de courant. Les pannes de courant sont l'une des raisons les plus fréquentes pour lesquelles un ménage perd son accès à Internet résidentiel, comme l'a illustré tempête de verglas de l'ouest du Québec et de l'est de l'Ontario survenue du 5 au 6 avril 2023.
- Si le budget et la disponibilité le permettent, utilisez un téléphone intelligent comme point d'accès sans fil mobile et achetez un service Internet mobile auprès d'un FSI différent de celui qui fournit la connexion Internet câblée. Le service de données mobiles doit disposer d'un volume de données suffisamment important afin de pouvoir être utilisé pour les activités en ligne prévues pendant une panne. Les services de diffusion en continu et les caméras de sécurité utiliseront beaucoup plus de données que les détecteurs de chute et les capteurs pour alarmes médicales.
- Déterminez les points d'accès Wi-Fi publics locaux qui pourraient être utilisés, par exemple à votre bibliothèque publique.

- Entendez-vous avec un voisin qui a acheté un service Internet auprès d'un autre FSI. Par exemple, un utilisateur d'Internet résidentiel qui subit une panne peut s'organiser pour utiliser temporairement la connexion Internet d'un voisin par Wi-Fi jusqu'à ce que la connectivité soit rétablie chez lui. S'il est disponible, utilisez l'accès Wi-Fi pour invité afin de séparer votre utilisation de celle de votre voisin.

Scénario 2 : Résilience de l'accès à Internet pour les travailleurs à distance

Public : Travailleurs à distance à temps partiel ou à temps plein; organisations qui offrent une option de travail hybride ou à distance à leurs employés

Le travail à distance est devenu de plus en plus courant pour les Canadiens. Des organisations de toutes tailles et de presque tous les secteurs permettent à certains de leurs employés de travailler au bureau une partie du temps, et à distance le reste du temps.

Pour les Canadiens qui travaillent à distance, à temps partiel ou à temps plein, et qui ont un besoin crucial d'accéder à Internet, le fait d'avoir une seule connexion Internet à la maison – et donc un seul point de défaillance – signifie qu'en cas de panne, leurs activités de travail en ligne seront interrompues jusqu'à ce que leur FSI rétablisse le service.

Que vous soyez travailleur autonome, propriétaire d'une entreprise ou gestionnaire d'une équipe de travailleurs à distance à temps partiel ou à temps plein, les recommandations suivantes vous aideront à adopter une posture plus résiliente en matière d'accès à Internet.

Discussion

Pour établir une connexion à Internet résiliente, si l'option de disposer de services de fournisseurs d'accès Internet différents et diversifiés est disponible, alors il est possible d'utiliser une méthode de secours fiable pour se connecter à Internet. L'une des mesures que les employeurs et les petites entreprises peuvent prendre pour améliorer la résilience consiste à équiper les travailleurs d'un téléphone intelligent doté d'un service Internet mobile acheté auprès d'un exploitant de réseaux mobiles (ERM) différent du FSI qui fournit les services Internet à domicile. De nombreuses entreprises regroupent les services des FSI et des ERM; l'élément clé est de garantir que ces services soient diversifiés et ne dépendent pas d'un seul point de défaillance, comme décrit ci-dessous.

Bien que cela engendre des coûts d'exploitation et de la complexité supplémentaires pour le propriétaire d'entreprise, équiper les télétravailleurs d'un téléphone intelligent et d'un forfait de données mobiles leur permettrait de créer un point d'accès sans fil et de remettre en ligne leurs appareils de travail le plus rapidement possible en cas de panne. Ils pourraient alors effectuer des travaux de base en ligne pendant un nombre d'heures déterminé, jusqu'à ce que la panne de la connexion à Internet filaire soit résolue.

Qu'est-ce qu'un exploitant de réseaux mobiles (ERM)?
Un ERM est un fournisseur de services de communications sans fil qui possède ou contrôle tous les éléments nécessaires pour vendre et fournir ces services à un utilisateur final. Les services fournis par un ERM comprennent l'affectation de spectre radio, l'infrastructure du réseau sans fil et l'infrastructure de liaison terrestre. Les ERM sont également appelés « fournisseurs de services sans fil », « fournisseurs de communications sans fil », « entreprises cellulaires » ou « opérateurs de réseaux mobiles ». Au Canada, les exemples d'ERM comprennent notamment Rogers, Bell et TELUS.

Dans ce scénario, certains types de travailleurs à distance n'ont besoin d'accéder qu'à un ensemble de services en ligne de base en cas de panne. Par exemple, si un travailleur à distance peut accéder à son courriel, à un réseau privé virtuel (RPV), à sa ligne de voix sur IP et à des pages Web pendant la panne, il pourra continuer à assumer ses responsabilités professionnelles de base. Ce type de travailleur n'aura pas besoin d'accéder à l'éventail complet des services, tels que la vidéoconférence et les transferts de fichiers volumineux.

Étant donné que la connexion à Internet mobile secondaire est destinée à fournir une connectivité professionnelle en cas de panne d'Internet résidentiel, l'employeur peut soit fournir un téléphone intelligent à l'employé à cette fin, soit l'employé peut fournir le sien et se faire rembourser par l'employeur un pourcentage des frais mensuels. Bien que cela puisse augmenter les frais d'exploitation des organisations et des travailleurs autonomes utilisant Internet, c'est un moyen simple d'améliorer la résilience pour ceux qui doivent avoir accès à Internet. Ce scénario est illustré dans la *Figure 2*.

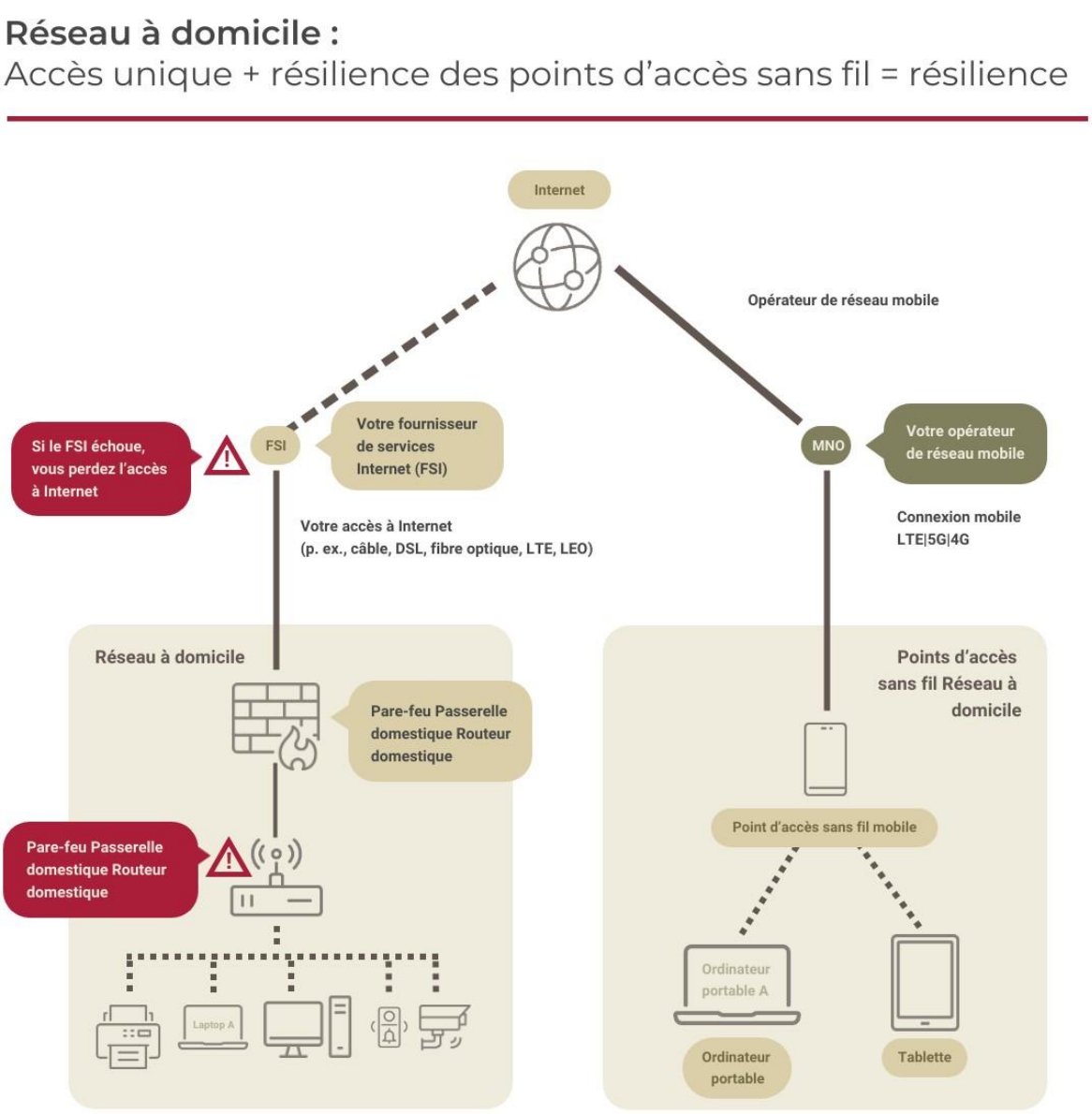

Figure 2 – Réseau domestique, accès unique et résilience du point d'accès sans fil

Il est toutefois important de noter que l'utilisation d'une connexion Internet mobile comme solution de secours ne permet pas dans tous les cas d'assurer la résilience de l'accès à Internet pour les travailleurs à distance. Par exemple, dans le cas peu probable où un utilisateur a acheté une offre groupée auprès d'un seul fournisseur de services qui comprend des services non diversifiés pour les services Internet à domicile et mobiles, une panne du réseau du fournisseur de services pourrait compromettre les deux sources de connectivité, ce qui laisserait l'utilisateur sans deuxième option pour une connectivité de secours. Ce scénario est illustré dans la *Figure 3*.

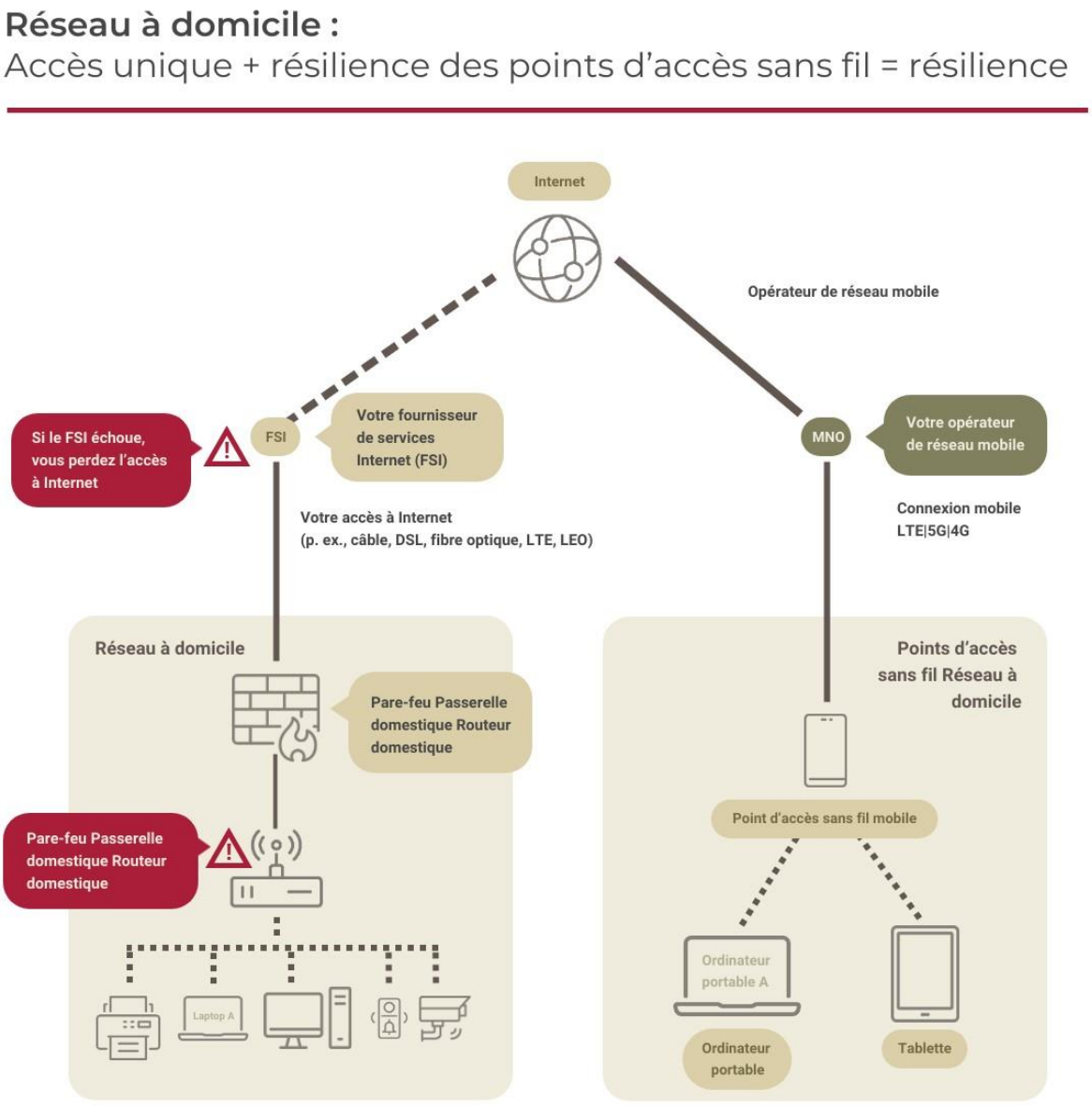

Figure 3 – Accès à Internet à domicile et mobile groupés : pas de résilience

Malheureusement, pour assurer la résilience de l'accès à Internet, il ne suffit pas de s'assurer que le fournisseur d'accès filaire ne soit pas le même que le fournisseur d'accès sans fil. Imaginez un scénario dans lequel un utilisateur achète un service d'accès à Internet auprès d'un FSI qui dépend d'un autre FSI pour fournir les services à son domicile. Par exemple, un travailleur à distance pourrait acheter un forfait mobile auprès d'un fournisseur de services et une connexion Internet auprès d'un autre fournisseur de services, avant de découvrir que le premier fournisseur fait partie des services du deuxième fournisseur de services. Dans ce scénario, le fait d'avoir un accès à Internet résidentiel fourni par deux fournisseurs différents

peut sembler favoriser la résilience, mais comme les deux accès reposent en fait sur une infrastructure partagée, la résilience n'est donc peut-être pas aussi bonne que l'utilisateur l'avait espéré.

Qu'est-ce que le service de transport? Qui le fournit?
Un fournisseur de services transport offre des connexions physiques directes entre deux points d'un réseau. Dans la plupart des cas, pour le dernier kilomètre (au domicile), le fournisseur de transport est le même que le FSI, mais pas toujours. C'est là que la compréhension de la différence entre un fournisseur de transport et un FSI peut aider à évaluer la résilience d'un accès à Internet.

Les fournisseurs de transport vendent généralement leurs services aux FSI. Certains réseaux d'entreprise font également appel à des fournisseurs de transport pour accéder aux services informatiques en nuage.

De nombreux utilisateurs de l'accès à Internet résidentiel au Canada dépendent également de fournisseurs de services transport, comme ceux qui achètent des services Internet auprès d'un fournisseur de services indépendant tel que TekSavvy. Dans ce scénario, TekSavvy peut acheter des services de réseau en gros à d'autres FSI, qui lui fournissent des installations de transport.

Au Canada, les fournisseurs de services de transport sont par exemple Rogers, Bell, Beanfield, Zayo et Hiboo Networks.

Dans ce scénario, si une panne survient chez le fournisseur du réseau de services de transport, le travailleur à distance peut utiliser son téléphone intelligent comme point d'accès sans fil temporaire jusqu'à ce que la panne soit résolue. Si le téléphone intelligent est fourni par le même fournisseur de réseau de services transport, la panne risque de toucher à la fois la connexion à Internet résidentielle et la connexion à Internet mobile de secours, laissant le travailleur sans accès à Internet. Ce scénario est illustré dans la *Figure 4*. Pour les utilisateurs d'Internet, connaître les bonnes questions à poser à leur FSI, y compris quelle entreprise fournit les services de transport dans leur région, peut les aider à évaluer le niveau de résilience de leur accès à Internet.

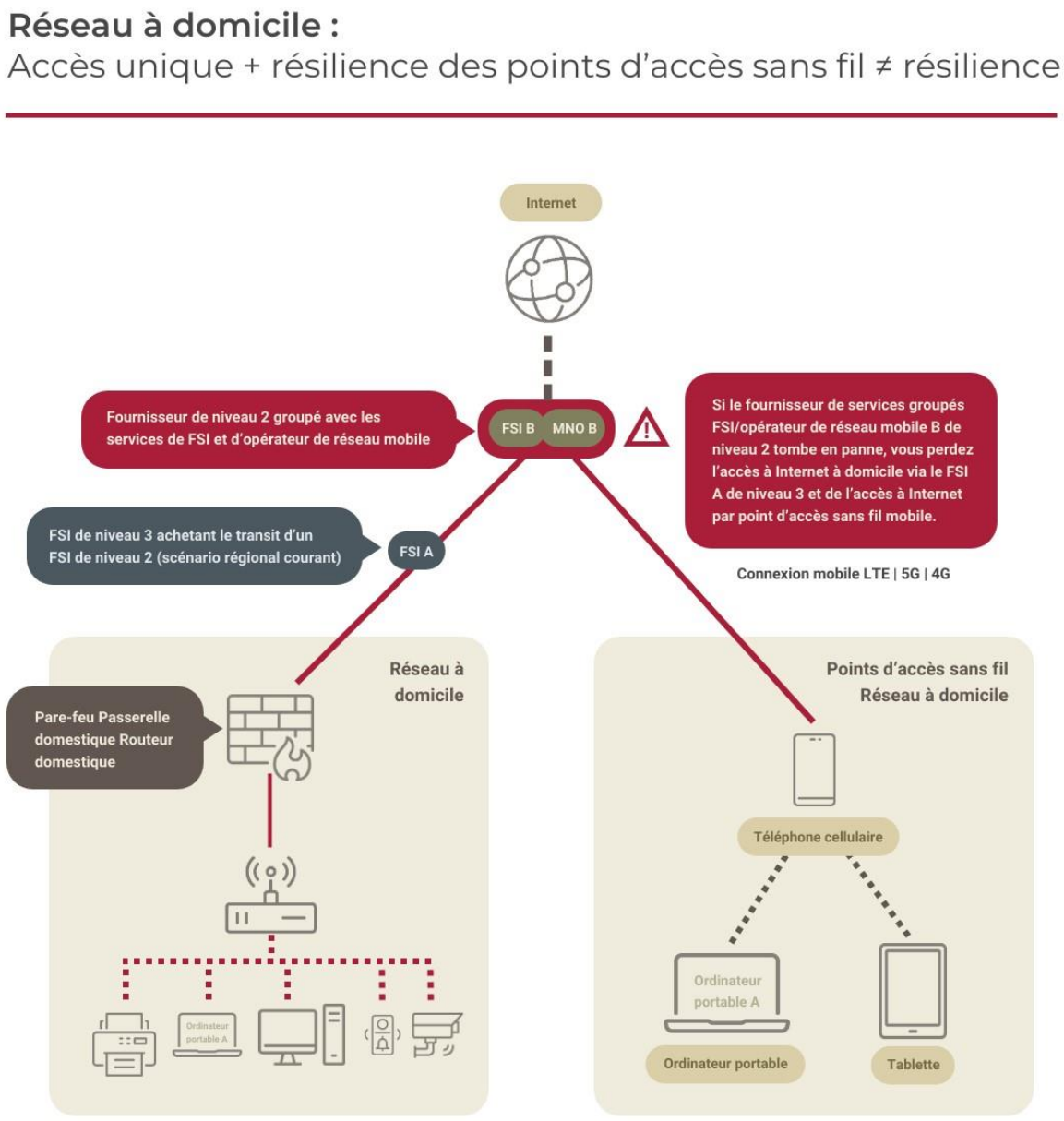

Figure 4 – Fournisseur commun de services de transport et mobiles : pas de résilience

Objectif de résilience

Garantir l'accès aux services Internet de base, tels que le courriel et la voix sur IP (VoIP), la vidéoconférence et l'accès aux services de base du réseau d'entreprise par RPV afin que le travailleur à distance puisse continuer à exercer ses activités professionnelles de manière limitée jusqu'à ce que la panne soit résolue.

Tolérance aux pannes

La tolérance aux pannes pour les travailleurs à distance nécessitant une résilience à des fins professionnelles dépend de la nature des activités que l'utilisateur doit effectuer. Une période d'indisponibilité de courte durée peut être acceptable pour certains travailleurs à distance, tandis que d'autres types de travailleurs, selon la nature de leurs responsabilités professionnelles, peuvent avoir besoin de se connecter immédiatement à un autre service Internet mobile.

Recommandations pour l'augmentation de la résilience

- Installez une alimentation électrique de secours pour le modem ou la passerelle et les points d'accès sans fil qui, selon sa capacité, alimentera les services d'accès à Internet pendant une durée déterminée en cas de panne de courant.
- Utilisez un téléphone intelligent fourni ou subventionné par l'employeur comme point d'accès sans fil mobile. Les employeurs peuvent se concerter avec leurs employés pour s'assurer que leur FSI résidentiel est différent de celui de leur fournisseur de services mobiles.
- Veillez à ce que le téléphone intelligent soit fourni par un FSI différent de celui qui fournit les services Internet filaires résidentiels et qu'il dispose d'une allocation mensuelle de données qui permettra de prendre en charge la quantité minimale de données que le travailleur utiliserait généralement pour effectuer les fonctions de base de son travail pendant une période de huit heures.
- Une autre solution consiste à acheter une carte eSIM pour un téléphone intelligent en vue d'une utilisation temporaire en cas d'urgence. L'achat et l'installation de la carte eSIM d'un fournisseur en ligne peuvent nécessiter un accès à Internet de courte durée.
- Les utilisateurs ruraux peuvent obtenir la résilience en utilisant différentes technologies, par exemple un mélange de services large bande, sans fil, à orbite terrestre basse (OTB) et de satellite. Le coût de ces services pourrait être pris en compte dans l'évaluation de la résilience.

Scénario 3 : Résilience de l'accès à Internet pour les petites entreprises équipées de systèmes de point de vente (PDV)

Public : Petites entreprises

Les petites entreprises canadiennes et leurs employés comptent de plus en plus sur une connectivité ininterrompue pour faciliter le paiement des biens et des services. Pouvoir recevoir à tout moment des paiements de la part de leurs clients au moyen des systèmes de point de vente (PDV) est une priorité absolue. Lorsqu'il y a une panne d'Internet, la connexion avec le fournisseur de PDV est également interrompue. En l'absence d'une autre forme de connectivité, l'entreprise ne sera pas en mesure de traiter les transactions financières des clients utilisant toute forme de paiement électronique pendant une panne, y compris les cartes de débit, les cartes de crédit et les paiements.

Les employés de l'entreprise ne pourront pas non plus s'acquitter de certaines de leurs responsabilités professionnelles s'ils n'ont pas accès à la navigation sur le Web et au courriel. Selon la taille de l'entreprise et ses besoins particuliers, elle peut recourir à différentes méthodes pour parvenir à la résilience. Chacune de ces méthodes nécessite une diversité des FSI qui se connectent aux systèmes essentiels tels que les PDV.

Discussion

Pour améliorer la résilience de l'accès à Internet, une petite entreprise peut utiliser un point d'accès sans fil de téléphone intelligent fourni par un ERM différent (comme indiqué dans le scénario 2) de celui qui fournit la connexion à Internet principale. Si la connexion à Internet principale est interrompue, l'entreprise peut basculer vers la connexion du point d'accès sans fil du téléphone intelligent afin que le système de point de vente reste connecté et que les paiements puissent continuer à être traités. Il s'agit d'une approche similaire à la résilience recommandée pour les travailleurs à distance, qui est illustrée dans la *Figure 2*.

Toutefois, certaines petites entreprises peuvent souhaiter disposer d'une méthode automatisée pour reprendre la connexion à Internet en cas de panne. Ces solutions sont possibles, mais nécessitent une attention particulière en fonction de l'objectif de résilience et de la tolérance aux pannes. Les professionnels locaux du réseautage et des TI peuvent aider à la mise en œuvre de ces systèmes. En général, les solutions de basculement automatisées sont plus coûteuses que les solutions de basculement manuelles.

Objectif de résilience

Garantir l'accès aux services en ligne d'entreprise de base, tels que les activités des points de vente, afin que le travailleur puisse continuer à exercer ses fonctions de manière limitée jusqu'à ce que la panne soit résolue.

Tolérance aux pannes

La tolérance aux pannes est faible pour les petites entreprises qui ont besoin d'un accès résilient aux services Internet de base pour leurs employés. Chaque minute de période d'indisponibilité a des répercussions sur l'entreprise, car ses activités seront limitées ou interrompues. Dans ce scénario, comme la petite entreprise doit se reconnecter à Internet manuellement à l'aide d'un téléphone intelligent doté d'une connexion de données mobiles, une période d'indisponibilité de courte durée (moins de 30 minutes) peut être acceptable avant que l'entreprise puisse se reconnecter et que les employés puissent reprendre leurs activités professionnelles.

Les petites entreprises qui ont une très faible tolérance aux pannes d'Internet peuvent avoir besoin de solutions de basculement automatisées complexes, également connues sous le nom de solutions d'« hébergement multiple ».

Recommandations pour l'augmentation de la résilience

- Installez une alimentation électrique de secours pour le modem ou la passerelle et les points d'accès sans fil qui, selon sa capacité, alimentera les services d'accès à Internet pendant une certaine durée en cas de panne de courant.
- Utilisez un téléphone intelligent comme point d'accès sans fil mobile pour assurer la connectivité des PDV et d'autres systèmes en cas de panne de la connexion principale.
- Les entreprises peuvent collaborer avec leurs fournisseurs de PDV pour mieux comprendre comment les terminaux de PDV atteignent leur FSI.
- Veillez à ce que les employés soient formés pour s'assurer que les systèmes d'entreprise fonctionnent correctement en utilisant le point d'accès sans fil de secours.
- Veillez à ce que le téléphone intelligent dispose d'une allocation mensuelle de données permettant de prendre en charge l'éventail complet des activités en ligne requises par l'entreprise, telles que le traitement des paiements.
- Les entreprises peuvent mettre en œuvre une solution d'« hébergement multiple », qui leur permet de connecter leur réseau local à plusieurs connexions à Internet en même temps. Si une connexion à Internet tombe en panne, leurs appareils basculent sur une connexion fournie par un autre FSI. Communiquez avec un professionnel du réseautage et des TI pour déterminer si cette solution vous convient, à vous et à votre entreprise.
- Utilisez un exploitant de réseaux mobiles (ERM) différent du FSI qui fournit les services d'accès à Internet primaires à l'entreprise. Reportez-vous au scénario 2 ci-dessus pour des recommandations sur la manière de sélectionner des fournisseurs distincts qui amélioreront la résilience.

Scénario 4 : Résilience de l'accès à Internet pour les petites entreprises offrant des services par le biais d'Internet

Public : Petites et moyennes entreprises vendant des biens et des services en ligne

Au XXI^{e} siècle, de nombreuses entreprises ne dépendent plus d'emplacements traditionnels et d'appareils de PDV physiques pour faire des affaires. Même celles qui offrent leurs services dans un environnement de vente au détail traditionnel proposent souvent un portail complémentaire en ligne pour l'achat de biens et de services. Les solutions de commerce électronique reposent sur une connectivité ininterrompue pour faciliter les ventes, les retours et la communication avec les clients.

Les petites et moyennes entreprises qui proposent à leurs clients des services de commerce électronique par le biais d'Internet à partir de leur infrastructure sur place sont peut-être à la recherche de nouveaux moyens d'assurer une connectivité permanente et ininterrompue afin d'éviter les pertes de ventes et de favoriser la continuité des activités. Les lignes directrices suivantes illustrent quelques moyens permettant aux propriétaires de petites entreprises d'améliorer la résilience de leurs activités en ligne.

Discussion

Les propriétaires de petites et moyennes entreprises qui vendent des services en ligne devraient commencer par étudier la possibilité d'un double accès à Internet, qui offre une certaine résilience s'il est configuré de manière à éviter un point de défaillance unique. Pour ce faire, chaque connexion à Internet doit être fournie par un FSI différent afin d'augmenter la résilience de l'accès. Le fournisseur de services de transit utilisé par chaque FSI doit également être diversifié. Pour une discussion approfondie sur ce point et des suggestions sur la manière de garantir la diversité et la résilience de votre connectivité, reportez-vous au scénario 2 ci-dessus.

Dans ce scénario, si une panne survient sur la connexion à Internet principale, la connexion de secours fournie par le second FSI assurera la connectivité jusqu'à ce que la connexion principale puisse être rétablie.

Cette architecture résiliente peut être configurée de manière à ce que le système puisse basculer manuellement ou automatiquement vers la connexion à Internet de secours, en fonction des besoins particuliers de l'entreprise.

La *Figure 5* illustre une architecture d'accès à Internet résiliente avec un double accès à Internet pour les petites entreprises.

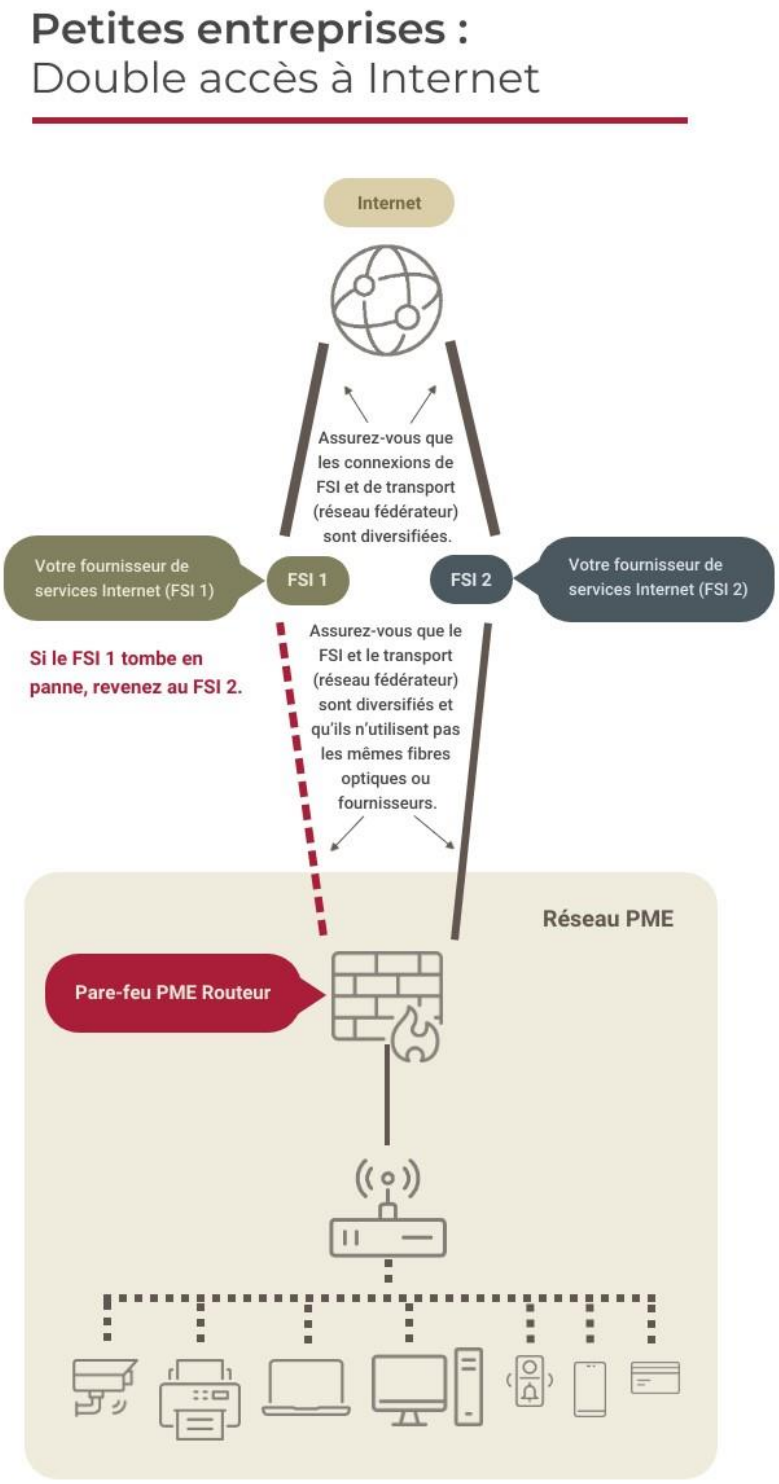

Figure 5 – Résilience des petites entreprises avec double accès à Internet

Dans la *figure 5* ci-dessus, il est recommandé aux propriétaires de petites entreprises de communiquer avec leurs deux fournisseurs de services de TI ou, au besoin, leurs FSI pour comprendre et s'assurer de la diversité du chemin emprunté par leurs connexions pour atteindre Internet.

Il convient de noter que le niveau de complexité peut être considérablement augmenté pour les solutions de basculement immédiat lorsque les services sont offerts sur Internet, et qu'une attention particulière est requise pour garantir que les services en ligne sont correctement disponibles en cas de basculement de l'accès à Internet. Communiquez avec un professionnel du réseautage et des TI pour déterminer si cette solution vous convient, à vous et à votre entreprise.

Objectif de résilience

Les entreprises peuvent s'assurer que leurs employés ont accès aux services en ligne de base nécessaires à leurs activités, tels que le courriel, la voix sur IP et les services de PDV, et que les clients peuvent accéder aux services en ligne fournis par l'entreprise (tels que les services de commerce électronique). De plus en plus d'organisations déplacent leurs présences en ligne vers le nuage pour atteindre leurs objectifs de résilience.

Tolérance aux pannes

La tolérance aux pannes pour les petites entreprises de ce type est faible, car chaque minute de période d'indisponibilité se traduit par une perte de productivité et de revenus. Pour assurer la continuité des services dans ce scénario, le passage à la connectivité à Internet de secours doit être immédiat en cas de défaillance du service principal.

Recommandations pour l'augmentation de la résilience

- Les entreprises peuvent mettre en œuvre une solution d'« hébergement multiple », qui leur permet de connecter leur réseau local à plusieurs connexions Internet en même temps. Si une connexion à Internet tombe en panne, leurs appareils basculent sur une connexion fournie par un autre FSI. Communiquez avec un professionnel du réseautage et des TI pour déterminer si cette solution vous convient, à vous et à votre entreprise.
- Dans ce cadre, les entreprises peuvent étudier les options permettant d'automatiser le passage de la connexion principale à la connexion de secours afin d'éliminer toute période d'indisponibilité. Elles peuvent également collaborer avec un professionnel du réseautage pour mettre en place des mesures garantissant que la connexion de secours est fonctionnelle grâce à des essais réguliers et automatisés. Le propriétaire d'entreprise pourra ainsi s'assurer que le système de secours est fonctionnel et éviter que la connexion ne bascule sur un service en panne.
- Les entreprises qui proposent des solutions de commerce électronique à leurs clients peuvent examiner les options de services basés sur le nuage, qui offrent souvent un temps de disponibilité, une résilience et une diversité de réseaux supérieurs.

Scénario 5 : Résilience de l'accès à Internet pour les entreprises

Public : Organisations de taille moyenne et grande qui gèrent leurs propres réseaux d'entreprise afin d'assurer la connectivité entre les utilisateurs, les appareils et les applications

Alors que de nombreuses petites entreprises peuvent se contenter d'une connexion à Internet résiliente et d'une poignée d'appareils connectés tels que des ordinateurs portables et des terminaux de PDV, les organisations plus importantes ont généralement des besoins plus sophistiqués en matière de technologies de l'information qui les obligent à élaborer un réseau d'entreprise sécurisé et hautement fiable.

Alors qu'un réseau d'entreprise peut soutenir son organisation et ses utilisateurs en offrant une connectivité et des applications fiables et sécurisées aux utilisateurs, une panne d'Internet peut interrompre brutalement les activités, ce qui peut avoir de graves conséquences pour l'entreprise. La discussion ci-dessous contribuera à promouvoir un accès à Internet plus résilient pour les réseaux d'entreprises de toutes tailles.

Discussion

Les mêmes principes d'accès à Internet résilient qui s'appliquent aux petites entreprises s'appliquent également aux moyennes et grandes entreprises et à d'autres organisations, telles que les universités et les ministères, afin d'assurer la continuité des activités. Comme pour les petites entreprises, il est essentiel pour ces organisations d'éviter un point de défaillance unique en disposant d'au moins deux connexions à Internet et en utilisant différents FSI pour ces connexions. Le réseau doit être configuré pour basculer automatiquement vers la connexion de FSI de secours (p. ex., par le biais de solutions de REDL) afin que la résilience puisse être assurée avec une période d'indisponibilité minimale en cas de panne.

Pour les entreprises qui souhaitent s'interconnecter directement à la structure Internet afin d'augmenter leur résilience et leur connectivité avec d'autres réseaux locaux, le réseau d'entreprise doit être configuré en tant que système autonome (AS). Un AS se voit attribuer son propre numéro d'identification, appelé « numéro de système autonome » (ASN), et dispose d'un éventail précis d'adresses IP routables. Pour que sa politique de réseautage soit connue des autres systèmes autonomes sur Internet, le réseau doit également être équipé de routeurs qui prennent en charge le protocole BGP (« Border Gateway Protocol »). Ces routeurs gèrent des tables de routage qui leur permettent de déterminer le chemin le plus rapide vers d'autres AS sur Internet.

Lorsque ces exigences sont satisfaites, l'organisation peut améliorer la résilience de son réseau en cas de panne. Les employés peuvent continuer à accéder à Internet et les utilisateurs externes ne subissent pas de perturbation notable des services offerts par l'entreprise par le biais d'Internet. Les travailleurs à distance connectés en utilisant des réseaux privés virtuels (RPV) sont également protégés, car ils sont automatiquement réacheminés vers un autre

chemin d'accès en cas de panne. La *Figure 6* illustre la résilience pour les moyennes et grandes entreprises.

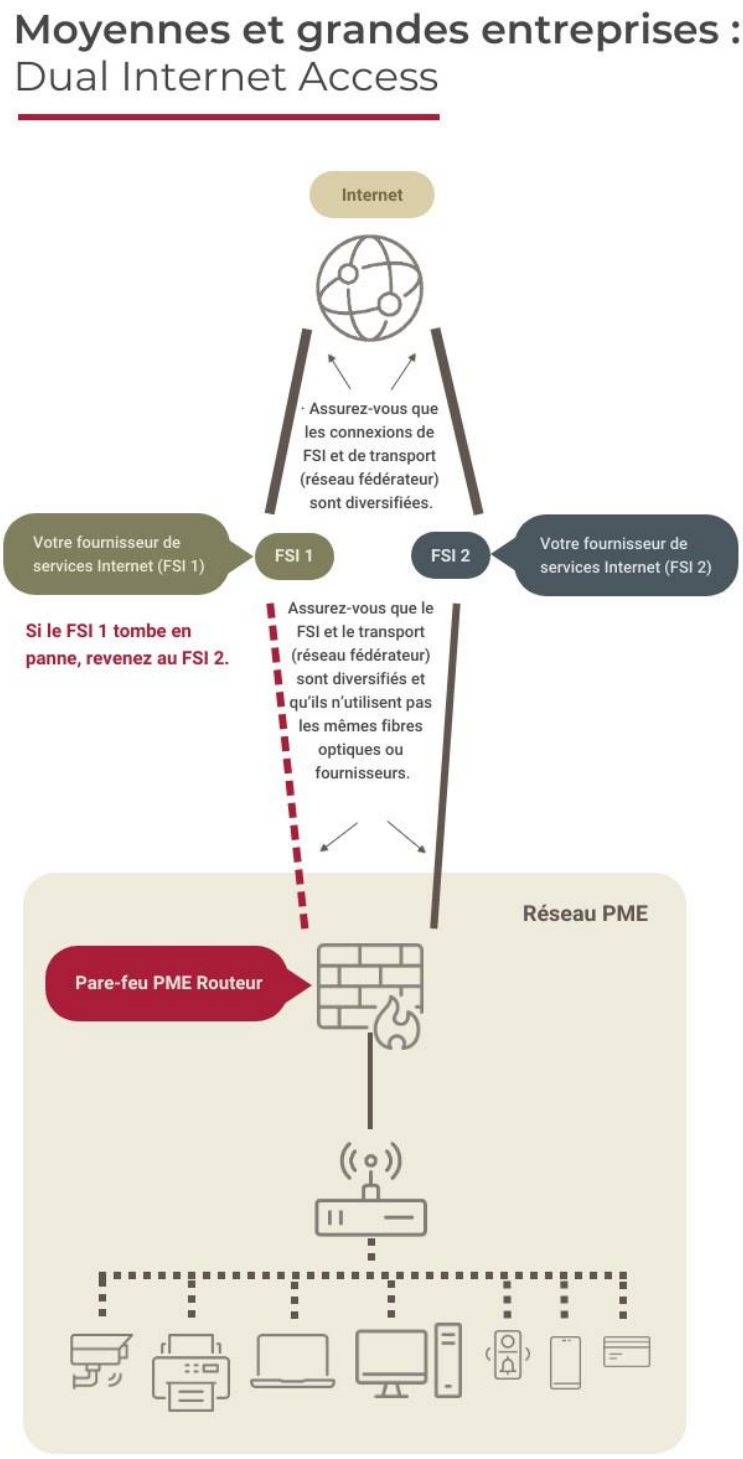

Figure 6 – Résilience pour les moyennes et grandes entreprises

Objectif de résilience

Veiller à ce que les employés aient un accès immédiat à l'ensemble des services en ligne nécessaires pour mener des activités professionnelles normales, sans interruption, et veiller à ce qu'il n'y ait pas de perturbation des services offerts aux clients ou aux partenaires par le biais d'Internet (tels que les services de commerce électronique).

Tolérance aux pannes

La tolérance aux pannes pour ces entreprises est faible, car chaque minute de période d'indisponibilité se traduit par une perte de productivité et de revenus. Pour assurer la continuité des services dans ce scénario, la connectivité à Internet de secours doit être immédiate en cas de panne du service principal.

Recommandations pour l'augmentation de la résilience

- Les organisations peuvent mettre en œuvre une solution d'« hébergement multiple » exploitant le système autonome et le protocole BGP, qui leur permet de brancher leur réseau local à plusieurs connexions à Internet en même temps. Si une connexion à Internet tombe en panne, leurs appareils basculent sur une connexion fournie par un autre FSI. Communiquez avec un professionnel du réseautage et des TI pour déterminer si cette solution vous convient, à vous et à votre entreprise.
- Dans ce cadre, les organisations peuvent étudier les options permettant d'automatiser le passage de la connexion principale à la connexion de secours afin d'éliminer toute période d'indisponibilité. Elles peuvent également collaborer avec un professionnel du réseautage pour mettre en place des mesures garantissant que la connexion de secours est fonctionnelle grâce à des essais réguliers et automatisés. Cela permettra à la direction de s'assurer que le système de secours fonctionne correctement et d'éviter que la connexion ne bascule vers un service en panne.
- Mettez en œuvre une infrastructure de réseautage autonome et réalisez un appairage (échange de trafic) avec un point d'échange Internet (IXP). Cela pourrait permettre une connectivité de RPV presque locale aux FSI des employés, et aux utilisateurs de l'entreprise d'accéder à des services d'IXP locaux tels que des fournisseurs d'informatique en nuage en périphérie.
- Les entreprises qui proposent des solutions sur place pour le courriel et la gestion de l'information peuvent examiner les options de services informatiques en nuage, qui offrent souvent un temps de disponibilité et une résilience supérieurs.
- Les grandes organisations peuvent avoir besoin d'évaluer la posture de résilience de leur infrastructure, de leurs points de terminaison et de leurs applications, afin de mettre en évidence les domaines à améliorer; cela peut inclure le déploiement de solutions de surveillance de la couche réseau ou d'applications afin de fournir une visibilité, de développer des connaissances et d'orienter le processus décisionnel.

Scénario 6 : Résilience de l'accès à Internet pour les FSI (régionaux) de niveau 3

Public : Fournisseurs de services Internet (régionaux) de niveau 3

Alors qu'une poignée de grands FSI résidentiels se partagent la plupart des abonnés à Internet au Canada, un large éventail de FSI plus petits s'efforce également de fournir des services Internet aux résidents, souvent dans les collectivités rurales, éloignées et autochtones, qui sont traditionnellement mal desservies en matière de services de télécommunications.

Dans le cadre de ce travail, les professionnels du réseautage qui gèrent ces petits FSI cherchent souvent à améliorer la résilience de leurs réseaux. Dans de nombreux cas, ces petits FSI dépendent de fournisseurs plus importants pour l'infrastructure de liaison terrestre principale et sont le seul moyen de faciliter l'accès à Internet dans les collectivités qu'ils desservent. Les lignes directrices suivantes visent à fournir aux FSI régionaux de petite taille des idées novatrices sur la manière dont ils peuvent renforcer leurs activités pour être plus résilients.

Discussion

Il est essentiel pour les FSI de parvenir à la résilience. Pour ce scénario, le terme « FSI de niveau 3 » est défini comme un réseau, généralement un FSI régional, qui achète uniquement des services de transit Internet auprès d'un autre FSI de niveau 2 pour accéder à Internet et qui dessert une région géographique particulière au Canada. Dans ce qui suit, vous verrez que les exigences particulières varient en fonction du type de FSI, les exigences régionales de résilience de niveau 3 différant de celles des FSI nationaux de niveau 2. Pour une analyse complète des différences entre les fournisseurs des niveaux 1, 2 et 3, veuillez consulter l'annexe A à la fin du présent document.

Afin de garantir la résilience pour les utilisateurs du réseau, les réseaux des FSI de niveau 3 doivent répondre à plusieurs exigences architecturales principales. Tout d'abord, ils doivent éviter tout point de défaillance unique dans leurs réseaux. Ils peuvent y parvenir en faisant appel à au moins deux FSI de niveau 1 ou 2 différents pour les services de transit Internet. Pour garantir la diversité du transport, les différents FSI ne doivent pas utiliser la même infrastructure de fibre optique ou d'autres réseaux. Le réseau doit être configuré pour basculer automatiquement vers la connexion de FSI de secours afin d'assurer la résilience avec une période d'indisponibilité minimale en cas de panne, comme cela est consigné dans les solutions ASN et d'hébergement multiple. Les FSI de niveau 3 doivent également veiller à la diversité de leurs fournisseurs de services de transit afin d'éviter un point de défaillance unique.

Souvent, le réseau des FSI de niveau 3 n'a pas accès aux services de transport tels que la fibre noire et les services de longueur d'onde. Les FSI de niveau 3 ne sont souvent desservis que par un seul FSI de niveau 2 et n'offrent que des services de transit Internet. Cela a donc des répercussions importantes sur la résilience des FSI de niveau 3.

Qu'est-ce que le transit Internet? Quelle est la différence avec le transport Internet?
Le transit Internet est une considération importante pour la résilience des FSI. Un fournisseur de transit Internet (FTI) vend l'accès à Internet mondial aux FSI et à certains réseaux d'entreprises et de gouvernements connectés à Internet. Le transit Internet est la relation commerciale par laquelle un FSI fournit à ses utilisateurs un accès à Internet mondial. Lorsqu'un utilisateur visite un site sur Internet, comme les sites de médias sociaux ou son compte bancaire en ligne, son FSI envoie le trafic sur Internet jusqu'à sa destination par le biais du réseau d'un FTI. Le FTI facture des frais au FSI de l'utilisateur pour ce service.

Certains grands FSI de niveau 2 vendent également des services de transit Internet; toutefois, cela peut réduire la résilience Internet si le FSI qui fournit ces services subit une panne.

Les FSI de niveau 3 qui peuvent réaliser un appairage à des IXP peuvent considérablement améliorer leur résilience par rapport à leur dépendance vis-à-vis des FTI en fournissant à leurs utilisateurs un accès à des réseaux locaux. Les FSI de niveau 3 ne font généralement pas d'appairage avec les IXP canadiens en raison du manque d'options de connexion.

En plus de ces exigences, pour participer activement au réseautage sur Internet, le réseau doit être configuré avec un système autonome (AS). Pour que sa politique de réseautage soit connue des autres systèmes autonomes sur Internet, le réseau doit également être équipé de routeurs à l'échelle d'Internet pour le routage complet d'Internet qui prennent en charge le protocole BGP (« Border Gateway Protocol »). Ensemble, ces éléments peuvent contribuer à promouvoir la stabilité et la résilience du réseau en veillant à ce que les routeurs puissent s'adapter aux défaillances de routage. En présence d'un échec de routage, le réseau peut se reconfigurer et trouver un nouveau chemin viable.

Un FSI de niveau 3 doit s'assurer que les FSI de niveau 2 sont résilients les uns par rapport aux autres en veillant à ce que les fournisseurs de services de transit IP utilisés par les FSI de niveau 2 soient diversifiés, comme illustré dans la *Figure 7*. Il s'agit d'une exigence essentielle pour la résilience d'Internet au Canada. Par exemple, si les deux FSI de niveau 2 utilisent les mêmes fournisseurs de transit, l'exigence de diversité peut ne pas être respectée et les internautes canadiens ne seront pas protégés en cas de perturbation du transit IP (par exemple, à la suite d'une attaque DDoS ou d'une panne).

En outre, l'appairage avec des réseaux partenaires aux IXP est une autre pratique exemplaire qui contribue à accroître la résilience des FSI de niveau 3 au Canada. L'appairage réduit la congestion, garantit le temps de fonctionnement et contribue à repousser les cyberattaques. La résolution des requêtes DNS est également essentielle pour les infrastructures de TI modernes.

Le fait de disposer de divers chemins par le biais du transit et des IXP pour résoudre les problèmes liés aux domaines .CA et à d'autres domaines de premier niveau contribue également à l'augmentation de la résilience.

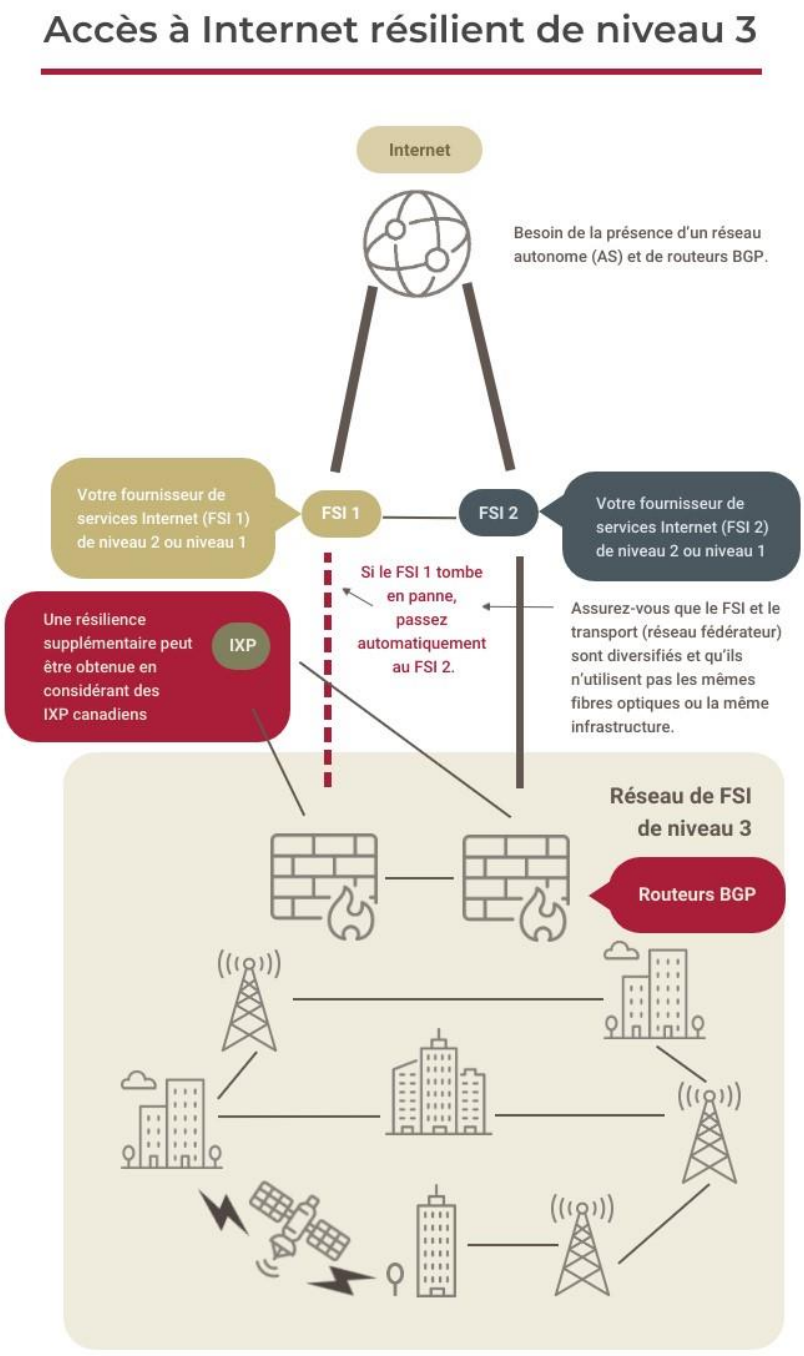

Figure 7 – Résilience des FSI régionaux/de niveau 3

Objectif de résilience

Veiller à ce que tous les clients et employés des FSI de niveau 3 aient un accès immédiat à l'ensemble des services en ligne nécessaires pour mener des activités professionnelles normales, sans interruption, et veiller à ce qu'il n'y ait pas de perturbation notable des services offerts aux clients ou aux partenaires par le biais d'Internet.

Tolérance aux pannes

La tolérance aux pannes des FSI de niveau 3 est extrêmement faible, car chaque minute d'indisponibilité se traduit par des abonnés mécontents, ainsi qu'une perte de productivité et de revenus. Pour assurer la continuité des services dans ce scénario, la connectivité à Internet de secours doit être immédiate en cas de défaillance du service principal.

Recommandations pour l'augmentation de la résilience

- Un FSI régional de niveau 3 doit s'efforcer de disposer de deux connexions à Internet fournies par divers fournisseurs de niveau 1 ou 2 utilisant des services de transport séparés et distincts (c'est-à-dire que les FSI de niveau 3 ne doivent pas utiliser la même fibre ou les autres infrastructures de réseau que leurs fournisseurs de secours). Dans la mesure du possible, les FSI de niveau 3 doivent réaliser un appairage avec l'IXP le plus proche afin de réduire la congestion, de maintenir le temps de fonctionnement et d'atténuer les effets délétères des cyberattaques ainsi que des pannes de réseau causées par des catastrophes naturelles ou des erreurs humaines.
- Le passage de la connexion principale à la connexion de secours doit être automatisé et immédiat afin d'éviter les périodes d'indisponibilité. Par exemple, un ASN consacré et un routage BGP correctement configuré permettront de garantir la reprise des activités de routage normales en cas de rupture du chemin d'accès à Internet public.
- Recherchez un service de transport diversifié vers le point d'échange Internet (IXP) le plus proche afin d'augmenter la résilience du FSI de niveau 3 en accédant directement à un service d'infrastructure essentiel tel que la résolution DNS.
- Adoptez des pratiques exemplaires essentielles, telles que le protocole MANRS (reportez-vous à l'annexe A) et le filtrage à l'entrée de réseau (BCP38), qui n'autorise que le trafic provenant de sources Internet prévues.

Scénario 7 : Résilience de l'accès à Internet pour les FSI de niveau 2

Public : Grands fournisseurs de services Internet (niveau 2)

Au Canada, une petite poignée de grands FSI achète des services de transit auprès de FSI de niveau 1 et distribue ensuite cet accès aux utilisateurs finaux. Bien que ces grands FSI de niveau 2 exploitent des réseaux sophistiqués et compte des millions d'abonnés, ils ne sont pas à l'abri des pannes. Les lignes directrices suivantes visent à améliorer la résilience des activités d'un FSI de niveau 2 sur Internet au Canada.

Discussion

Pour ce scénario, un « FSI de niveau 2 » est défini comme un FSI qui achète des services de transit auprès d'un FSI de niveau 1 et qui réalise un appairage avec des points d'échange Internet (IXP). Les grands FSI de niveau 2 comprennent Bell, TELUS et Rogers.

La communauté Internet canadienne a consacré beaucoup de temps à construire le cœur de l'infrastructure Internet au Canada, avec un solide réseau d'IXP dans le but d'attirer de grands fournisseurs de contenu, de grandes entreprises hyper-évolutives et des fournisseurs d'infrastructures essentielles. De nombreux FSI de niveau 2 se connectent à ces IXP et réalisent un appairage avec eux, ce qui augmente leur résilience. L'augmentation du nombre de FSI de niveau 2 qui réalisent un appairage avec les IXP canadiens est une recommandation architecturale principale pour accroître la résilience. Reportez-vous à https://cira.ca/ixp pour obtenir une liste des IXP canadiens.

Alors que les FSI de niveau 2 s'appuient souvent sur des conduits de transit nord-sud qui passent par les États-Unis, en réalisant un appairage avec tous les IXP canadiens, les FSI de niveau 2 augmentent la résilience en interconnectant le réseau ensemble localement au Canada, en réduisant la congestion, en garantissant le temps de fonctionnement et en aidant à repousser les cyberattaques à la périphérie du réseau. La résolution des requêtes DNS est également essentielle pour les infrastructures de TI modernes. Le fait de disposer de divers chemins par le biais du transit et des IXP pour résoudre les domaines racine, .CA et .COM et autres domaines de premier niveau (résolution DNS) contribue également à l'augmentation de la résilience.

L'absence relative de FSI de niveau 2 chez les IXP canadiens augmente la dépendance à l'égard du nombre limité de chemins qui existent actuellement pour acheminer le trafic à l'échelle du pays. Bon nombre de ces chemins obligent le trafic à quitter le Canada et à passer par les États-Unis pour arriver à destination; dans l'ensemble, le manque d'appairage réduit la résilience d'Internet au Canada.

Objectif de résilience

Veiller à ce que les abonnés et les employés du FSI aient un accès immédiat à l'ensemble des services en ligne nécessaires pour mener des activités professionnelles normales, sans interruption, et veiller à ce qu'il n'y ait pas de perturbation des services offerts aux clients ou aux partenaires par le biais d'Internet.

Tolérance aux pannes

La tolérance aux pannes des FSI de niveau 2 est extrêmement faible, car chaque minute d'indisponibilité se traduit par des abonnés mécontents, une perte de productivité et de revenus, ainsi que de la satisfaction des clients. Pour assurer la continuité des services dans ce scénario, la connectivité à Internet de secours doit être immédiate en cas de défaillance du service principal.

Recommandations aux FSI de niveau 2 pour l'augmentation de la résilience

Les fournisseurs de niveau 2 devraient tenir compte des recommandations suivantes pour augmenter la résilience de leurs réseaux.

- Adoptez des pratiques exemplaires essentielles, telles que le protocole MANRS pour réduire les risques de routage (reportez-vous à l'annexe A) et le filtrage à l'entrée de réseau (BCP38) qui n'autorise que le trafic provenant de sources Internet prévues, afin de se protéger contre les attaques par déni de service distribué qui peuvent provoquer des interruptions de service.
- Veillez à ce qu'au moins deux FSI différents assurent le transport en utilisant des installations distinctes afin d'éviter tout point de défaillance unique, et configurez le réseau pour qu'il bascule automatiquement vers le FSI de secours en cas de panne de la ligne principale.
- En tant que pratique exemplaire, les FSI de niveau 2 devraient réaliser un appairage avec l'IXP le plus proche afin de réduire la congestion, de maintenir le temps de fonctionnement et d'atténuer les effets délétères des cyberattaques ainsi que des pannes de réseau causées par des catastrophes naturelles ou des erreurs humaines.
- Dans le cadre de l'appairage avec un IXP local, les FSI de niveau 2 devraient élaborer une politique d'appairage permissive qui favorise l'interconnexion avec un large éventail de fournisseurs de DNS, d'infrastructures essentielles et d'autres exploitants de réseaux.

6. Conclusion

La dépendance des Canadiens, des entreprises canadiennes, des gouvernements et des organisations de tous les secteurs à l’égard d’un accès à Internet fiable et de haute qualité n’a jamais été aussi grande. Quelle que soit son ampleur ou sa durée, une panne d’Internet a des répercussions négatives. Les personnes ne peuvent pas accéder aux services en ligne essentiels et les travailleurs à distance ne peuvent pas faire leur travail. Pour les entreprises, les interruptions importantes d’Internet peuvent nuire à leur réputation et entraîner des pertes de revenus. Le présent document contribuera à améliorer la résilience d’Internet au Canada et encouragera les personnes, les entreprises, les gouvernements et les autres exploitants de réseaux à mettre en œuvre collectivement des pratiques exemplaires éprouvées afin de réduire le risque de pannes et leurs répercussions sur l’économie canadienne.

Annexe A – Éléments de résilience supplémentaires

A.1. Dépendance des fournisseurs de transport à l'égard des services de transit Internet

Le « transit Internet », qui est défini comme la relation commerciale par laquelle un FSI fournit à ses utilisateurs un accès à Internet mondial, dépend d'une certaine forme de transport pour fonctionner. Par conséquent, la plupart des réseaux sont conformes à une infrastructure en fibre optique. En général, les FSI ne possèdent pas l'entièreté de leur réseau de transport, mais dépendent de nombreux fournisseurs de transport pour l'infrastructure de transport nécessaire à l'exploitation de leurs réseaux.

Le transit Internet peut être constitué de plusieurs fournisseurs de transport et de FTI, et les FTI peuvent utiliser plusieurs fournisseurs de transport. Les utilisateurs et les professionnels des TI ne sont souvent pas conscients que de nombreux éléments du transit dépendent du transport, ce qui rend la résilience de la connexion à Internet difficile à évaluer.

Il est essentiel de comprendre les dépendances entre le transit et le transport Internet pour évaluer la résilience d'un service Internet, qui est illustrée dans la *Figure 8*.

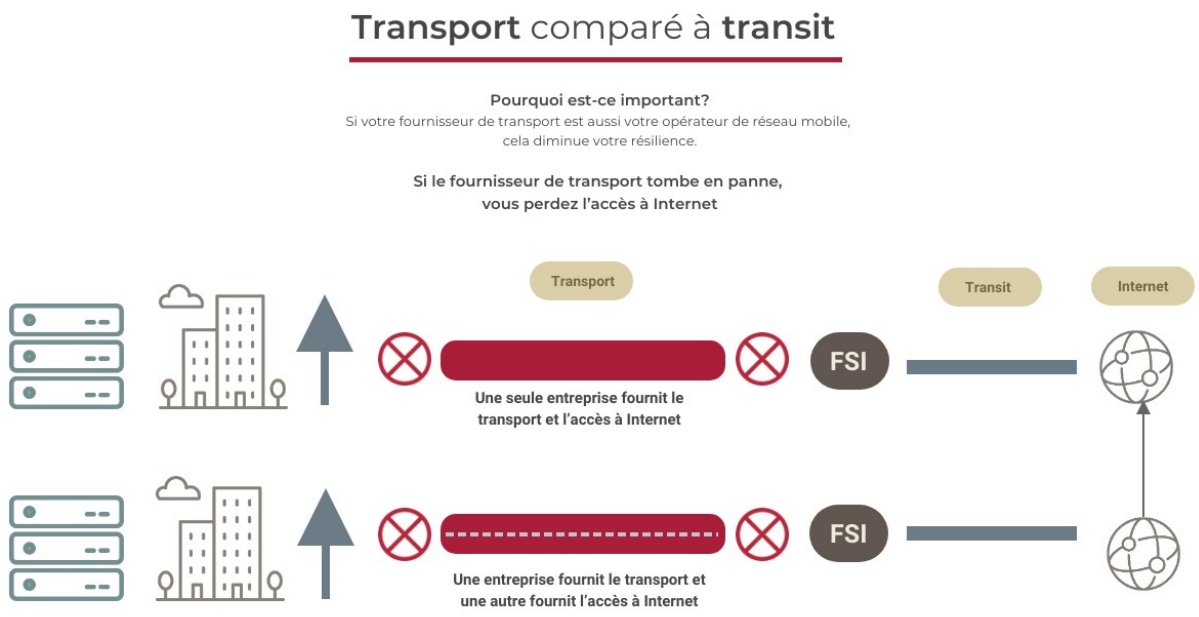

Figure 8 – Comparaison du transport et du transit

A.2. Diversité

Dans le contexte du réseautage, la diversité consiste à disposer de deux méthodes indépendantes de connexion à Internet fournies par des FSI différents. Si l'une de ces connexions subit une panne, la deuxième connexion peut être utilisée comme secours.

La diversité est une exigence essentielle de la résilience d'Internet. Pour les utilisateurs de l'accès à Internet résidentiel et les travailleurs à distance, une connectivité diversifiée peut être obtenue en disposant d'une connexion à Internet résidentielle auprès d'un FSI et d'une connexion à Internet mobile auprès d'un ERM distinct. Pour une entreprise de taille moyenne, la diversité peut être obtenue en ayant deux connexions à Internet distinctes provenant de deux FSI différents, chacun utilisant des fournisseurs de services de transit et de transport différents.

L'infrastructure physique utilisée pour fournir des services Internet, comme le câblage en fibre optique, doit également respecter les principes de diversité. Par exemple, dans un immeuble d'habitation, le câblage en fibre optique de deux FSI différents ne doit pas passer par le même conduit dans l'immeuble. Si le câblage est installé de cette manière, les clients des deux FSI perdront le service si le conduit est endommagé pour quelque raison que ce soit. En outre, tout utilisateur qui dépend d'une connexion à Internet de secours provenant d'un second FSI, comme un travailleur à distance, ne pourra pas utiliser l'une ou l'autre connexion. De même, si la fibre optique de deux FSI est installée dans le même puits d'entretien, une coupure de service pour les deux pourrait se produire si, par exemple, les câbles physiques étaient accidentellement coupés pendant les travaux d'entretien de la route.

A.3. Évitement des points de défaillance uniques

Un « point de défaillance unique » est une partie d'un système qui, si elle cesse de fonctionner, entraînera l'arrêt du fonctionnement de l'ensemble du système. Pour certains utilisateurs d'Internet résidentiel, par exemple ceux qui n'ont pas de téléphone intelligent doté d'un forfait de données mobiles, leur connexion à Internet est un point de défaillance unique. Si elle cesse de fonctionner, c'est tout le système d'accès au réseau du FSI et à Internet qui s'arrête, et il n'y a pas d'autre option pour accéder à Internet. Pour les entreprises et autres organisations, les réseaux sont conçus pour éviter un point de défaillance unique. Par exemple, une grande entreprise dispose généralement d'une connexion à Internet secondaire qui prend automatiquement le relais dans le cas d'une panne de la connexion principale, assurant ainsi la continuité des activités.

Les principales questions à poser pour éviter ou atténuer un point de défaillance unique sont les suivantes :

- Quels sont les FSI qui fournissent des services à l'endroit où je me trouve?
- Quels sont les fournisseurs de transport qui desservent ma région?

- Ai-je un point de défaillance unique? Qui dois-je appeler pour vérifier si j'ai un point de défaillance unique?
- La vitesse, la latence et la couverture locale répondent-elles à mes besoins? Souvent, la lenteur des débits peut être aussi grave que l'absence d'accès à Internet.
- Existe-t-il des services Internet secondaires disponibles localement, tels que des services sans fil fixes, par satellite en orbite basse (OTB), mobiles LTE fixes ou Wi-Fi?
- Quel système de surveillance avez-vous mis en place pour détecter tout point de défaillance unique? Qu'avons-nous fait pour mettre à l'essai la redondance et la résilience?

A.4. Comparaison des basculements manuel et automatique

Le « basculement » est le processus qui consiste à passer à une autre connexion à Internet lorsque la connexion à Internet principale subit une panne. Cette autre connexion doit être installée, disponible et vérifiée pour garantir qu'elle fonctionne correctement. Un basculement automatique se produit lorsque l'autre connexion ou la connexion de secours prend le relais dès le début d'une panne. Dans le cas d'un basculement manuel, l'utilisateur doit se connecter manuellement à l'autre service Internet lorsque la panne se produit.

Questions à poser :

- Pendant combien d'heures ou de jours puis-je fonctionner en cas de panne d'Internet?
- Ai-je une autre connexion à Internet ou une connexion de secours?
- Mon réseau prend-il en charge le basculement automatique de l'accès à Internet (la plupart du matériel ne le fait pas)?
- Ma connexion doit-elle basculer automatiquement sur l'autre connexion lorsque le FSI éprouve une panne?
- Est-ce que j'effectue des essais réguliers de toutes mes applications internes, y compris les applications essentielles, en utilisant l'autre connexion à Internet, afin de m'assurer qu'elles fonctionnent toutes correctement?
- Ai-je installé une alimentation électrique de secours à utiliser en cas de panne de courant?
- Ai-je installé une solution de protection contre les logiciels malveillants?
- Ai-je un contrat de service en vigueur avec du soutien technique disponible rapidement?

A.5. Points d'échange Internet (IXP)

Les « points d'échange Internet » sont des lieux physiques où différents réseaux se connectent pour échanger du trafic Internet par le biais des infrastructures de commutation communes. Ils constituent un élément principal de l'écosystème d'Internet et représentent un moyen essentiel d'augmenter l'accessibilité et la qualité de la connectivité dans les collectivités locales. Les IXP sont généralement dispersés à l'échelle des pays pour permettre aux réseaux locaux d'échanger de l'information de manière efficace en éliminant la nécessité d'échanger le trafic Internet local à l'étranger.

Les IXP échangent du trafic Internet de la même manière que les carrefours aéroportuaires nationaux et régionaux échangent des passagers. Les compagnies aériennes échangent les passagers nationaux en des points pratiques à l'intérieur du pays, plutôt que de les échanger dans des aéroports internationaux à l'étranger. De même, les IXP acheminent le trafic Internet local et régional localement, plutôt que par l'entremise de réseaux internationaux. À mesure que les pays et les villes établissent leurs propres IXP, une plus grande partie du trafic Internet local est échangée et acheminée localement, ce qui réduit les coûts et les ralentissements de réseau, augmente les vitesses de téléversement du contenu et encourage la croissance et la distribution du contenu Internet local. Les IXP permettent également de se conformer aux règlements locaux et régionaux actuels et futurs en matière de confidentialité des données.

Les IXP offrent des avantages importants, notamment la réduction des coûts d'accès à Internet pour les utilisateurs finaux grâce à la réduction des coûts d'exploitation des fournisseurs de services Internet (FSI) et la mise à disposition d'un accès à Internet plus abordable pour un plus grand nombre d'internautes locaux dans un pays particulier ou une région particulière. En outre, les IXP peuvent garantir que le trafic entre les expéditeurs et les destinataires locaux utilise des connexions locales peu coûteuses, plutôt que des liaisons internationales onéreuses. Les économies réalisées peuvent être considérables, de l'ordre de 20 % ou plus dans certains pays, car le trafic local peut représenter une part importante du trafic Internet global d'un FSI.

A.6. Réseaux autonomes et protocole BGP

Pour qu'un réseau participe pleinement au réseautage Internet mondial, il doit disposer d'un numéro d'adresse de système autonome attribué par un registre Internet régional (RIR) mondial comme ARIN (www.arin.net).

Un « réseau autonome » ou « système autonome » (AS) est un ensemble de préfixes de routage du protocole Internet (IP) connectés, sous le contrôle d'un ou de plusieurs exploitants de réseaux agissant au nom d'une seule entité administrative ou domaine, qui présente une politique de routage commune et clairement définie à l'Internet. Chaque AS se voit attribuer un numéro de système autonome (ASN), à utiliser dans le cadre du routage BGP (Border Gateway Protocol). Les ASN sont attribués aux registres Internet locaux (RIL) et aux organisations qui sont les utilisateurs finaux par leurs registres Internet régionaux (RIR) respectifs, qui reçoivent à leur tour des blocs des ASN à des fins de réattribution de l'IANA (Internet Assigned Numbers Authority). L'IANA tient également un registre des ASN réservés à un usage privé (et qui ne doivent donc pas être annoncés à l'Internet mondial).[2]

A.7. Hiérarchisation des FSI

Les FSI sont classés selon un modèle à trois niveaux en fonction du type de services Internet qu'ils fournissent. Ces niveaux sont décrits ci-dessous.

[2] https://fr.wikipedia.org/wiki/Autonomous_System

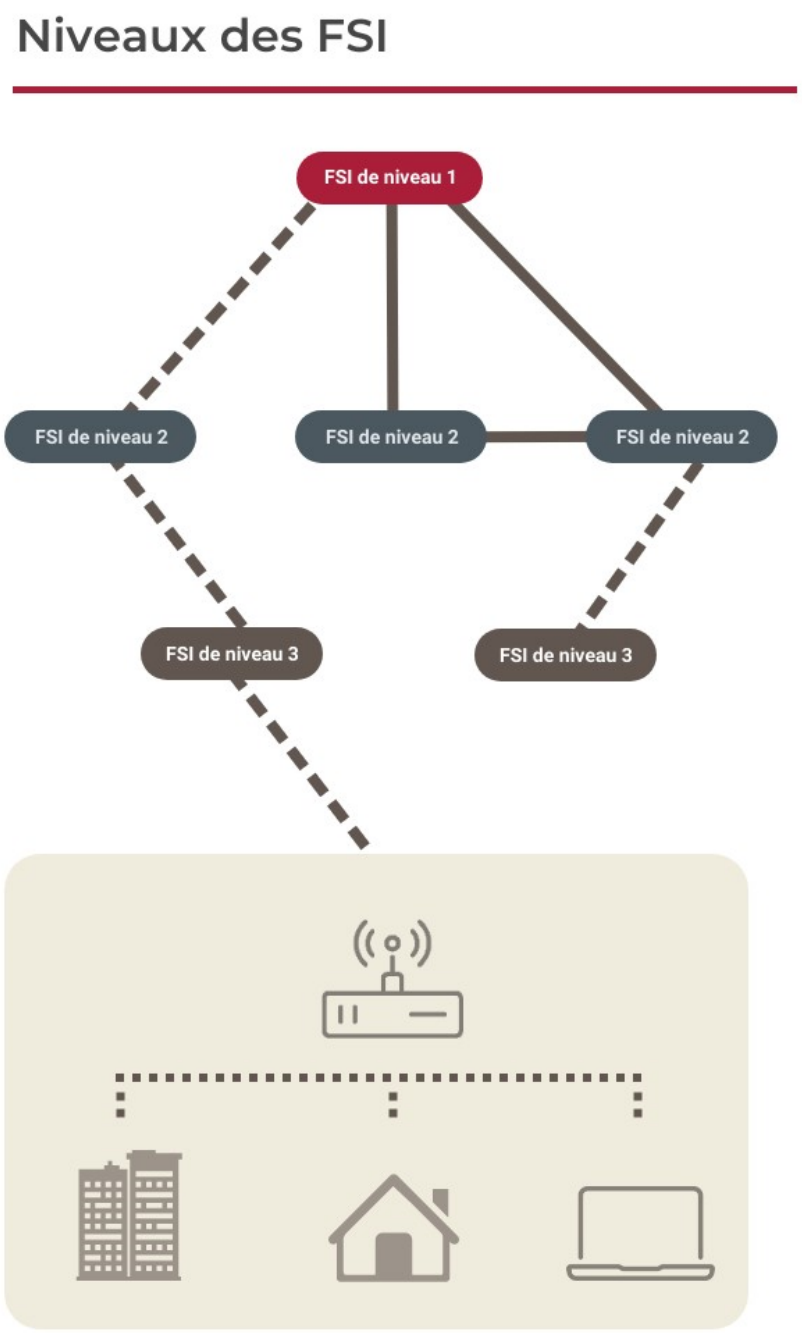

Figure 9 – Diagramme de hiérarchisation des FSI

FSI de niveau 1

Un « réseau de niveau 1 » est un réseau IP (protocole Internet) qui peut atteindre tous les autres réseaux sur Internet uniquement par le biais d'une interconnexion sans contrepartie financière (également connue sous le nom d'« appairage gratuit »). Les réseaux de niveau 1 peuvent échanger du trafic avec d'autres réseaux de niveau 1 sans payer de frais pour l'échange de trafic dans un sens ou dans l'autre. En revanche, certains réseaux de niveau 2 et tous les réseaux de niveau 3 doivent payer pour transmettre du trafic sur d'autres réseaux.[3]

FSI de niveau 2

Un « réseau de niveau 2 » est un FSI qui effectue l'échange de trafic avec d'autres réseaux, mais qui achète également des services de transit IP pour atteindre une partie d'Internet. Les FSI de niveau 2 sont les plus courants, car il est beaucoup plus facile d'acheter des services de transit auprès d'un réseau de niveau 1 que d'entrer en concurrence avec lui et d'essayer de devenir un exploitant de niveau 1. Parmi les grands FSI canadiens de niveau 2, on retrouve Bell, Rogers et TELUS.[4]

FSI de niveau 3

Le terme « FSI de niveau 3 » est utilisé pour décrire les réseaux qui achètent uniquement des services de transit IP auprès d'autres réseaux (en particulier, des réseaux de niveau 2) pour atteindre Internet. Ces FSI régionaux sont généralement de petite taille et achètent des services de transit auprès de grands réseaux de niveau 2 ou de réseaux de niveau 2 régionaux. Ils ne réalisent généralement pas d'appairage avec les IXP canadiens (absence de transport). Les réseaux 307net et CTAL sont des exemples de réseaux de niveau 3 au Canada.

A.8. MANRS : Pratiques exemplaires pour la sécurité du routage

« Mutually Agreed Norms for Routing Security » (normes mutuellement convenues pour la sécurité du routage – MANRS) est une vaste initiative mondiale qui fournit des correctifs cruciaux pour réduire les menaces les plus courantes en matière de routage. MANRS propose des mesures particulières par le biais de quatre programmes : Exploitants de réseaux, Points d'échange Internet, Réseaux de diffusion de contenu et fournisseurs d'informatique en nuage et Fournisseurs d'équipements. La section suivante donne un aperçu général de MANRS à l'intention des professionnels canadiens du réseautage qui cherchent à mettre en œuvre des mesures pour améliorer la résilience d'Internet au Canada. Pour obtenir des renseignements plus détaillés sur MANRS, y compris des recommandations particulières, consultez le site https://www.manrs.org/ (en anglais seulement).

Aperçu général de MANRS

La sécurité de l'infrastructure Internet mondiale, qu'il s'agisse de DNS ou de routage, comporte des défis importants; l'utilité des mesures de sécurité dépend des mesures coordonnées de nombreuses parties.

[3] https://en.wikipedia.org/wiki/Tier_1_network (en anglais seulement)

[4] https://en.wikipedia.org/wiki/Tier_2_network (en anglais seulement)

Les mesures attendues et avancées ci-dessous soulignent un ensemble de recommandations précieuses pour la sécurité et la résilience globales du système de réseautage mondial ainsi que pour l'exploitant de réseaux lui-même.

Les mesures attendues définissent un « ensemble » minimal, c'est-à-dire un ensemble de recommandations qui devraient être mises en œuvre par les exploitants soutenant MANRS.

- Empêcher la propagation d'information de routage incorrecte
    - L'exploitant de réseaux définit une politique de routage claire et met en œuvre un système qui garantit l'exactitude de ses propres annonces et des annonces de ses clients vers les réseaux adjacents avec une granularité de préfixe et d'ASN.
    - L'exploitant de réseaux peut communiquer les annonces qui sont correctes à ses réseaux adjacents.
    - L'exploitant de réseaux fait preuve de diligence raisonnable lorsqu'il vérifie l'exactitude des annonces de son client, en particulier qu'il détient légitimement l'ASN et l'espace d'adressage qu'il annonce.
- Empêcher le trafic avec des adresses IP usurpées
    - L'exploitant de réseaux met en œuvre un système qui permet la validation de l'adresse source au moins pour les réseaux clients simples raccordés à un seul fournisseur, leurs propres utilisateurs finaux et leur infrastructure. L'exploitant de réseaux met en œuvre un filtrage anti-manipulation pour empêcher les paquets dont l'adresse IP source est incorrecte d'entrer et de sortir du réseau.
- Faciliter la communication et la coordination opérationnelles au niveau mondial entre les exploitants de réseaux
    - L'exploitant de réseaux tient à jour des renseignements sur les personnes à contacter qui sont accessibles dans le monde entier.

Le contenu de ce document a été élaboré au cours des réunions du Groupe de travail sur la résilience d'Internet du FCRIN entre 2022 et 2023.

TLP:CLEAR

Version 1.0 – 8 septembre 2023

Préparé par le Groupe de travail sur la résilience d'Internet du Forum canadien pour la résilience des infrastructures numériques