Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Exigences de base en matière de sécurité pour les zones de sécurité de réseau

(Version 2.0)

PRATICIEN

Canada

AVANT-PROPOS

L'ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* est une publication NON CLASSIFIÉ publiée avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Pour obtenir plus d'information ou suggérer des modifications, veuillez communiquer avec le Centre d'appel du Centre canadien pour la cybersécurité (le Centre pour la cybersécurité) :

Centre d'appel
contact@cyber.gc.ca
Local : (613)-949-7048
Numéro sans frais : 1-833-CYBER-88

La présente version remplace toutes les versions précédentes de l'ITSP.80.022.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 12 janvier 2021.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Publication de la version 2.	12 janvier 2021

VUE D'ENSEMBLE

Le présent document décrit les modèles et les architectures de zones de sécurité de réseau et offre des conseils techniques sur la mise en œuvre des zones de sécurité de réseau.

L'orientation qu'il fournit est destinée aux solutions de technologie de l'information (TI) s'exécutant au niveau NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B[1] (c.-à-d., dont le niveau de sensibilité est faible ou partiel). Il convient de noter que les systèmes utilisés dans les domaines[2] PROTÉGÉ C[3] ou classifiés (c.-à-d., hautement sensibles) pourraient nécessiter d'autres considérations de conception qui dépassent la portée du présent document. Vous pouvez communiquer avec le Centre d'appel par courriel ou par téléphone pour obtenir des conseils sur les solutions cryptographiques pour les domaines PROTÉGÉ C ou classifiés.

Il incombe à votre organisation de définir les objectifs en matière de sécurité qu'il convient de fixer pour protéger ses services et ses données. Suivre les conseils formulés dans le présent document ne suffit pas pour sécuriser adéquatement un environnement informatique.

Ce document est destiné aux praticiens des TI qui sont familiers avec les principes, les normes et la terminologie de l'ingénierie des réseaux. Pour de plus amples conseils sur la sécurité de réseau, prière de communiquer avec notre Centre d'appel :

Centre d'appel
contact@cyber.gc.ca
(613)-949-7048
Numéro sans frais : 1-833-CYBER-88

[1] PROTÉGÉ A et PROTÉGÉ B sont des termes employés par le gouvernement du Canada pour décrire l'information personnelle et opérationnelle dont le niveau de sensibilité est faible ou partiel. La compromission de l'information PROTÉGÉ A pourrait porter préjudice à une entreprise ou à une personne, ou être source d'embarras. La compromission de l'information PROTÉGÉ B pourrait porter de sérieux préjudices à une entreprise ou à une personne (p. ex. perte de réputation ou d'un avantage concurrentiel).

[2] L'information ou les systèmes classifiés (p. ex. CONFIDENTIEL, SECRET, TRÈS SECRET) sont d'intérêt national (p. ex. économique, politique, militaire) pour le Canada. La compromission de l'information et des systèmes classifiés mettra en péril la sécurité nationale, causera un préjudice aux relations que le Canada entretient avec les autres pays ou conférera un avantage considérable à un pays étranger.

[3] PROTÉGÉ C est un terme employé pour désigner l'information opérationnelle ou personnelle hautement sensible. La compromission de l'information PROTÉGÉ C pourrait porter de graves préjudices à une entreprise ou à une personne (p. ex. perte de vie ou préjudice financier grave).

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

1 INTRODUCTION

Le présent document explique les zones de sécurité de réseau et leur utilisation lorsqu'une approche par couche est adoptée en ce qui concerne la sécurité. Il décrit également le modèle fonctionnel de ces zones. Ce modèle traite des principes et de la philosophie de conception à appliquer aux différentes zones de sécurité utilisées pour diviser une infrastructure de TI.

Pour vous aider à mettre en œuvre les zones de sécurité de réseau, le présent document abordera les problèmes liés à la configuration et à la gestion internes de chaque zone et de chaque point d'interface de zone (PIZ). Les objectifs et exigences en matière de sécurité compris dans la présente définissent la façon de connecter les zones entre elles. Ils indiquent également s'il convient ou non d'établir une connexion directe entre certaines zones pour maintenir le niveau de sécurité requis.

Les zones de sécurité de réseau posent les bases d'une architecture de sécurité équilibrée et multicouche qui peut prendre en charge toute une gamme de solutions de sécurité répondant aux besoins opérationnels de votre organisation. Ces zones proposent également une infrastructure réseau commune pour assurer la prise en charge de la prestation électronique de services, de l'interconnectivité et de l'interopérabilité. Si votre organisation partage une infrastructure commune pour la prestation électronique de services ou d'autres fins, vous devez vous conformer à toutes les normes de sécurité établies pour l'infrastructure en question.

Si vous mettez en œuvre des solutions informatiques dans un ministère ou organisme du gouvernement du Canada (GC), vous devez vous conformer aux politiques du Secrétariat du Conseil du Trésor du Canada (SCT), dont les suivantes :

- *Politique sur les services et le numérique* et *Directive sur les services et le numérique* [1][4];
- *Politique sur la sécurité du gouvernement* [2];
- *Directive sur la gestion de la sécurité* [3].

Si votre organisation n'est pas un ministère ou organisme du GC, vous pouvez vous reporter à ces politiques pour obtenir de plus amples renseignements.

1.1 RAPPORT AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS AUX TI

Comme pour tout projet ou solution de TI, il convient de tenir compte des activités de gestion des risques liés à la sécurité des TI décrites dans la publication ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [4] lors de la mise en œuvre des zones de sécurité de réseau. Ces activités sont décrites dans la figure 1.

L'ITSG-33 [4] décrit deux niveaux d'activités de gestion des risques liés à la sécurité des TI : les activités du niveau organisationnel (également appelé « niveau ministériel ») et les activités du niveau des systèmes d'information. Vous devriez inclure les activités de niveau organisationnel, lesquelles sont décrites à l'annexe 1 de l'ITSG-33 [4], dans les programmes de sécurité de votre organisation. Ce niveau d'activités vous aide à planifier, à gérer et à évaluer les risques liés

[4] Les numéros entre les crochets renvoient à des éléments de référence figurant à la section Contenu complémentaire du présent document.

à la sécurité des TI. Vous devriez tenir compte des activités du niveau des systèmes d'information, lesquelles sont décrites à l'annexe 2 de l'ITSG-33 [4], dans la gestion du cycle de vie des systèmes d'information, qui est réalisée dans le cadre du processus d'application de la sécurité dans les systèmes d'information (PASSI).

La mise en œuvre de zones de sécurité de réseau devrait s'aligner sur les activités actuelles de votre organisation en matière de gestion des risques liés à la sécurité des TI, notamment sur ce qui suit : la définition des besoins organisationnels en matière de sécurité des TI et de contrôles de sécurité, le déploiement des contrôles de sécurité, de même que la surveillance et l'évaluation du rendement des contrôles de sécurité. La mise en œuvre devrait également s'aligner sur les activités du niveau des systèmes d'information pour garantir la fiabilité de la solution. Plus précisément, vous devriez considérer les phases suivantes du PASSI : la phase de lancement, la phase de développement et d'acquisition, la phase d'intégration et d'installation ainsi que la phase d'exploitation et de maintenance.

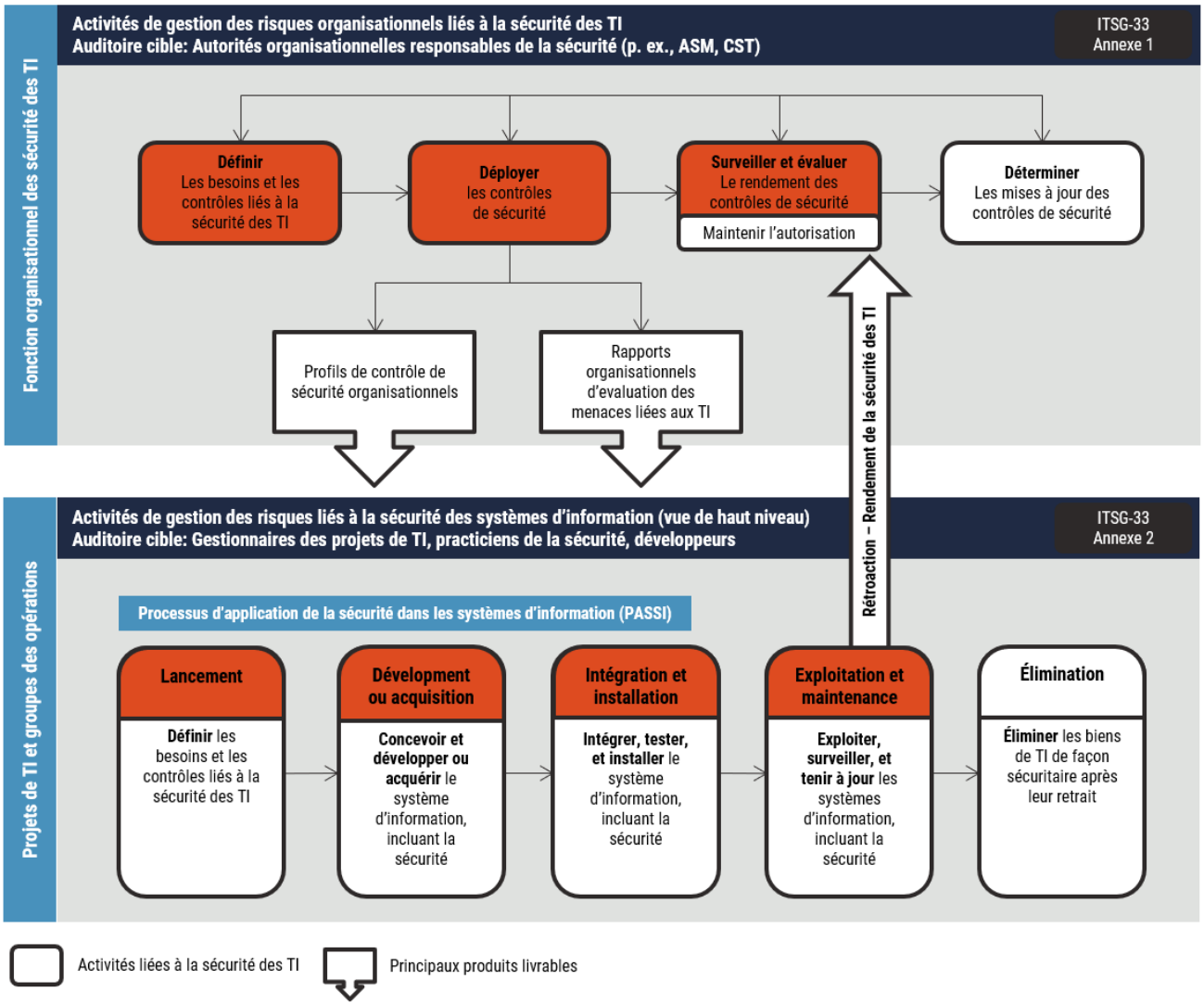


Figure 1 : Activités de gestion des risques liés à la sécurité des TI

2 ZONES DE SÉCURITÉ DE RÉSEAU

2.1 TYPES DE ZONES DE SÉCURITÉ DE RÉSEAU

Une zone est un environnement réseau dont le périmètre et les points de connexion sont clairement délimités. Le présent document défini les types de zones suivants :

- zone publique;
- zone d'accès public;
- zone de travail;
- zone d'accès restreint;
- zone d'accès très restreint;
- zone extranet d'accès restreint;
- zone de gestion.

La relation entre ces zones est illustrée dans le modèle de mise en œuvre de zone que l'on retrouve à la figure 5 du présent document (voir la sous-section 3.2.2).

2.1.1 ZONE PUBLIQUE

Une zone publique (ZP) est entièrement ouverte; elle englobe les réseaux publics tels qu'Internet, le réseau téléphonique commuté et d'autres réseaux fédérateurs et services publics de télécommunication. La mise en place ou l'application de restrictions et d'exigences visant cette zone est très difficile, voire impossible, car elle échappe normalement au contrôle que peut exercer le GC ou l'organisation. L'environnement de la ZP est présumé être extrêmement hostile. Tous les systèmes mis en œuvre dans la ZP, ou possédant des interfaces avec cette zone, doivent être renforcés contre les attaques.

Bien que la ZP est présumée être extrêmement hostile, une autorité de zone de sécurité de réseau (voir la sous-section 2.3 pour de plus amples renseignements) est autorisée à utiliser les services de sécurité offerts par les fournisseurs publics. En fait, cette démarche est même encouragée, car elle renforce la capacité de défense en profondeur. Vous ne devriez toutefois pas ignorer le niveau de menace d'une ZP au moment d'établir les exigences de base en matière de sécurité.

2.1.2 ZONE D'ACCÈS PUBLIC

Une zone d'accès public (ZAP) négocie les accès entre les systèmes opérationnels et la ZP. La ZAP est un environnement étroitement contrôlé qui protège les réseaux et les applications internes de l'environnement hostile de la ZP. Elle joue également le rôle d'un écran qui masque les ressources internes de la ZP et limite leur exposition.

Les interfaces de tous les services de l'organisation en ligne devraient être mises en œuvre dans une ZAP. Les services de serveur mandataire qui permettent aux employés d'accéder aux applications Web devraient être mis en œuvre dans une ZAP, de même que les passerelles de courrier électronique externe, d'accès à distance et d'extranet.

Les extranets qui se connectent par l'intermédiaire d'une ZAP diffèrent de ceux qui traversent une zone extranet d'accès restreint (ZEAR) (voir la sous-section 2.1.6). Ils s'en distinguent surtout par le degré de confiance à l'égard du partenaire qui

gère l'extranet. Les partenaires d'une ZEAR jouissent d'un degré de confiance très élevé et se connectent directement à une zone interne contrôlée par l'organisation.

2.1.3 ZONE DE TRAVAIL

La zone de travail (ZT) est l'environnement standard pour les activités courantes d'une organisation. Il s'agit de la zone où la plupart des systèmes d'utilisateur final, des serveurs d'applications et des serveurs de fichiers et d'impression sont installés. Lorsque les systèmes d'extrémité sont munis des contrôles de sécurité appropriés, cette zone peut convenir au traitement des renseignements sensibles. Toutefois, elle ne convient généralement pas aux grands dépôts de données sensibles ou aux applications essentielles.

Dans une ZT, le trafic n'est généralement pas restreint et peut provenir de sources internes (c.-à-d. d'autres zones dans l'organisation) ou d'autres sources externes autorisées (p. ex. l'accès distant, l'accès mobile et les extranets) par l'intermédiaire de la ZAP et de la ZEAR.

Dans une telle zone, le trafic malveillant peut toutefois provenir de sources hostiles internes, de codes hostiles non détectés importés de la zone publique ou de nœuds malveillants sur le réseau (p. ex. un hôte compromis, une connexion non autorisée à la zone).

2.1.4 ZONE D'ACCÈS RESTREINT

La zone d'accès restreint (ZAR) procure un environnement réseau contrôlé habituellement adapté aux services de TI essentiels (ceux pour lesquels on a établi des exigences moyennes en matière d'intégrité et de disponibilité, mais où une compromission des services entraînerait une interruption des activités). La ZAR convient également aux grands dépôts de données sensibles (p. ex. dans un centre de données).

La ZAR prend en charge l'accès aux systèmes de la ZP par l'intermédiaire de la ZT et de la ZAP. Toutes les entités de la couche réseau d'une ZAR sont authentifiées, soit explicitement, par la mise en œuvre d'un service d'authentification de l'entité homologue, soit implicitement, par une combinaison de mesures de sécurité matérielle et d'un contrôle rigoureux de la configuration. La ZAR réduit les menaces en provenance de l'intérieur du système en limitant les accès et en appliquant des mesures de surveillance administrative. Les services de confidentialité des données sont établis à l'intérieur de la ZAR pour les protéger de l'écoute clandestine par des nœuds non autorisés.

2.1.5 ZONE D'ACCÈS TRÈS RESTREINT

La zone d'accès très restreint (ZATR) procure un environnement réseau rigoureusement contrôlé habituellement adapté à l'exécution d'applications essentielles sur le plan de la sécurité (celles pour lesquelles on a établi des exigences strictes en matière de disponibilité et d'intégrité, et où une compromission constituerait une menace pour la santé ou la sécurité d'êtres humains). La ZATR convient aux très grands dépôts de données sensibles.

On ne peut accéder à une ZATR que depuis d'autres zones contrôlées par l'organisation (c.-à-d. les systèmes de la PZ ne peuvent pas y accéder). Toutes les entités de la couche réseau d'une ZATR sont authentifiées, soit explicitement par la mise en œuvre d'un service d'authentification de l'entité homologue, soit implicitement par une combinaison de mesures de sécurité matérielle et d'un contrôle rigoureux de la configuration. En règle générale, les exigences d'une ZATR à l'égard des

systèmes d'extrémité sont plus strictes que celles d'une ZAR. La ZATR impose également des contrôles plus rigoureux aux utilisateurs des systèmes pour contrer les menaces internes.

Les services de confidentialité des données, qui conviennent à la protection de l'information sensible, sont aussi établis dans une ZATR. Les services de confidentialité des données protègent le trafic de la zone contre l'écoute clandestine par des nœuds non autorisés. Ces services peuvent être mis en œuvre au niveau de la couche réseau ou de la couche physique.

2.1.6 ZONE EXTRANET D'ACCÈS RESTREINT

La zone extranet d'accès restreint (ZEAR) peut prendre en charge les services extranet en connexion directe avec des partenaires auxquels on accorde une très grande confiance. La ZEAR n'est pas nécessairement connectée par l'intermédiaire d'une ZAP (voir la figure 3 à la sous-section 3.2.1.3).

La mise en œuvre de la ZEAR doit être effectuée conformément au PASSI (voir l'annexe 2 de l'ITSG-33 [4]). Il pourrait être nécessaire de mettre en place des contrôles additionnels pour protéger adéquatement la zone connectée à la ZEAR. Les exigences et les pratiques liées à de telles zones devraient être élaborées au cas par cas et appliquées au moyen d'ententes avec les partenaires.

> **Remarque :** Dans le contexte du GC, les connexions entre les ministères et organismes du GC ne sont pas établies depuis une ZEAR. La ZEAR est réservée aux connexions avec des organisations à l'extérieur du GC (p. ex. des environnements TI impartis, des interfaces entre les gouvernements fédéral et provinciaux, des services intégrés avec des institutions financières).

2.1.7 ZONE DE GESTION

La zone de gestion (ZG) est une zone isolée dont la robustesse est similaire à celle d'une ZAR. La ZG offre aux administrateurs réseau un réseau d'administration dédié et isolé au moyen duquel ils peuvent configurer et surveiller les infrastructures du réseau. Sur le plan de la sécurité, cette zone permet aux administrateurs d'exécuter des opérations de commande et de contrôle tout en minimisant le risque d'interception ou de compromission.

Les ministères du GC peuvent gérer les zones à distance si des mécanismes approuvés par le GC ont été mis en place. Dans le contexte du GC, les zones ne devraient être gérées à distance que si le ministère utilise des hôtes de gestion approuvés, dédiés et renforcés qui s'authentifient sur une ZG depuis des emplacements approuvés par le GC. Les hôtes de télégestion devraient se connecter et s'authentifier par l'entremise d'une zone d'accès en télégestion (ZAT). La ZAT comporte les mêmes composants réseau et les mêmes caractéristiques qu'une ZAP, mais elle s'exécute sur une infrastructure isolée physiquement.

2.2 POINTS D'INTERFACE DE ZONE

La zone de démarcation entre les zones s'appelle la frontière (voir la figure 2 ci-dessous). La frontière contient les points d'interface de zone (PIZ) qui relient les points entre les zones. Le PIZ est le concept logique servant à décrire l'interface contrôlée qui relie deux zones. Il s'agit de l'interface réseau interzone.

Les PIZ appliquent les stratégies de communication entre les deux zones. Toutes les données doivent être transmises par un PIZ, lequel connecte exclusivement ces deux zones par l'intermédiaire d'une voie de communication.

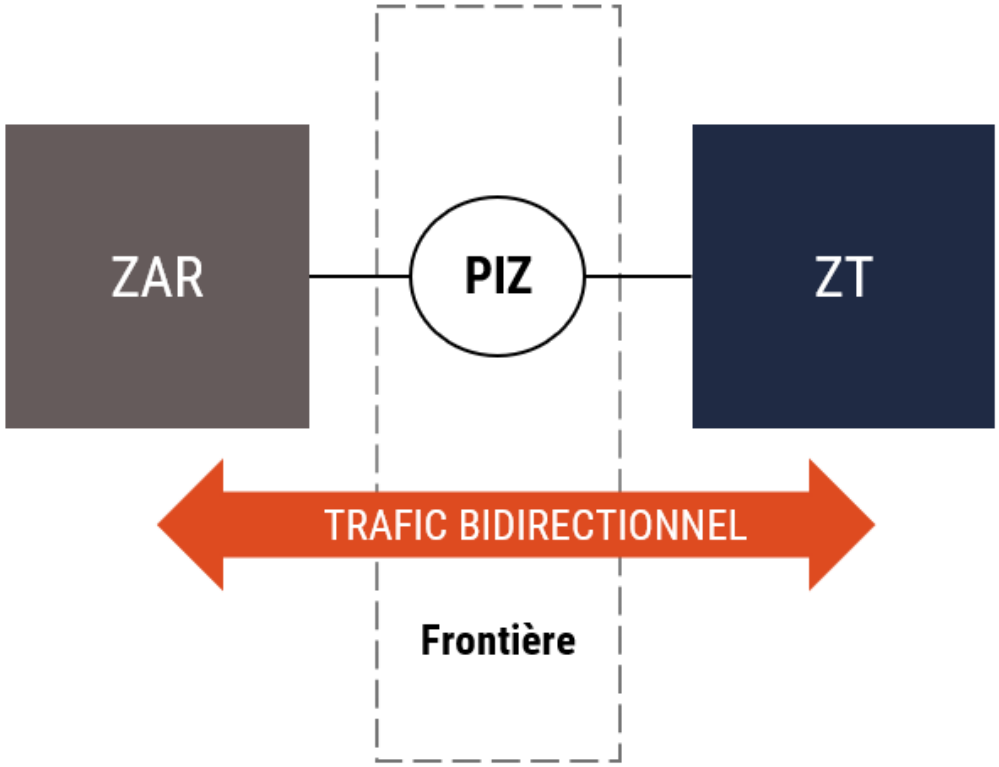


Figure 2 : Exemple de frontière de zone

2.3 AUTORITÉ DE ZONES DE SÉCURITÉ DE RÉSEAU

Chaque zone est attribuée à une autorité de zone de sécurité, qui est l'entité responsable du développement, de la mise en œuvre et de la maintenance des exigences et des pratiques en matière de sécurité. Tel qu'il est indiqué dans l'ITSG-33 [4], l'autorité de zone de sécurité de réseau est une des fonctions assumées par le coordonnateur de la sécurité des TI. Il incombe à l'autorité de zone de sécurité de réseau d'effectuer les tâches suivantes :

- passer en revue les stratégies et les normes de sécurité de la zone;
- recommander des stratégies et des normes de sécurité de zone aux fins d'approbation par le dirigeant principal de la sécurité;
- passer en revue les propositions et toute autre documentation sur la passation de marché, y compris les listes de vérification des exigences relatives à la sécurité, susceptibles d'avoir une incidence sur la ou les zones auxquelles il a été affecté;
- collaborer avec les gestionnaires de la prestation de programmes et de services pour s'assurer de répondre aux besoins en matière de sécurité des TI;
- prodiguer des conseils sur les contrôles de sécurité de zone et la mise en œuvre de tels contrôles;
- prodiguer des conseils aux gestionnaires de la prestation de programmes et de services sur l'incidence potentielle des changements apportés au réseau sur la posture de sécurité.

Des détails sur les tâches, les responsabilités et les rôles de l'autorité de zone de sécurité de réseau sont fournis aux annexes A à F du présent document.

Le contrôle de l'autorité de contrôle de sécurité de réseau émane de la propriété directe du réseau ou d'une entente officielle avec un fournisseur de services (p. ex. contrat, protocole d'entente) avec des niveaux de service définis garantissant le respect des exigences de base de la zone en matière de sécurité. Chaque zone devrait relever d'une autorité de zone de sécurité réseau qui lui est propre. Une même autorité peut toutefois être responsable de plusieurs zones.

3 MODÈLES DE ZONE DE SÉCURITÉ DE HAUT NIVEAU

3.1 VUE D'ENSEMBLE

La présente section décrit le modèle de mise en œuvre de zone (voir la figure 5 dans la sous-section 3.2.2) qu'il convient d'utiliser pour faciliter l'application des zones de sécurité de réseau dans votre ministère ou organisation. Vous pouvez appliquer les conseils fournis dans cette section dans des environnements à locataire unique ou multilocataires. Dans le cas d'un environnement multilocataire, vous devriez envisager d'ajouter des exigences additionnelles en ce qui a trait à la conception et la sécurité afin de répondre aux exigences en matière de confidentialité, d'intégrité et de disponibilité; ces exigences additionnelles ne sont pas prises en compte dans le présent document.

3.2 MODÈLE DE MISE EN ŒUVRE DE ZONE

3.2.1 PRINCIPES DES ZONES DE SÉCURITÉ DE RÉSEAU

Le zonage est une approche de conception logique qui sert à contrôler les accès et les flux de données de manière à les restreindre aux composantes et utilisateurs autorisés. Les zones établissent les périmètres du réseau et les exigences connexes en matière de protection des frontières au moyen des fonctions suivantes :

- définir les entités qui occupent les zones;
- déterminer les points d'entrée et de sortie distincts;
- filtrer le trafic réseau aux points d'entrée et de sortie;
- surveiller l'état du réseau;
- authentifier l'identité des entités de réseau;
- surveiller le trafic réseau aux points d'entrée et de sortie.

Une zone a été affectée à une autorité de zone de sécurité de réseau. L'autorité de zone de sécurité de réseau est responsable d'assurer l'élaboration, la mise en œuvre et le respect des exigences en matière de sécurité et des pratiques de la zone sous sa responsabilité. Les exigences et les pratiques en matière de sécurité s'ajoutent à celles des infrastructures réseau communes pour faciliter la prestation électronique de services, l'interconnectivité et l'interopérabilité.

Vous pouvez utiliser les zones pour mettre en œuvre une infrastructure réseau qui réduit les risques à la sécurité qui pèsent sur les processus opérationnels et l'information. Les zones sont séparées par des PIZ, lesquels sont mis en œuvre au moyen de dispositifs de sécurité et d'autres dispositifs réseau. Les zones peuvent être utilisées pour créer une architecture de défense en profondeur. Selon cette approche architecturale, les couches de protection sont ajoutées au réseau de manière à ce que seul un petit groupe d'utilisateurs et d'applications puissent accéder aux données sensibles (qu'elles soient stockées ou en cours de traitement).

L'architecture de défense en profondeur permet d'organiser les fonctions effectuées sur les données sélectionnées en des zones basées sur les besoins des utilisateurs, la sensibilité des données et l'environnement de menace attendu. Différentes zones procurent différents niveaux de sécurité aux processus opérationnels de chacune des zones. L'établissement de nouvelles exigences en matière de stratégie donnera lieu à la création d'une nouvelle zone. Par exemple, les zones

accessibles depuis Internet, lesquelles mettent l'accent sur l'accès des utilisateurs à Internet, exigent un plus grand nombre de contrôles, puisque ces zones comptent plus d'utilisateurs et comportent plusieurs types de données et une gamme d'applications. D'une zone à l'autre, la variété d'applications offertes aux utilisateurs diminue, le nombre d'utilisateurs pouvant accéder à ces applications est de plus en plus restreint et les fonctions pouvant être effectuées sont de plus en plus limitées. Le nombre de contrôles semblera diminuer à mesure que la variété des applications et des données diminue. Les niveaux d'assurance des contrôles mis en œuvre augmenteront toutefois en fonction de la sensibilité des données.

Les zones pour lesquelles l'ensemble des composantes sont entièrement sous le contrôle de votre ministère sont désignées « zones contrôlées ». Si votre ministère ne contrôle pas l'ensemble des composantes d'une zone, celle-ci est désignée « non contrôlée ». Vous devriez évaluer les zones non contrôlées dans le cadre du processus de gestion des risques de votre ministère ou de votre organisation.

3.2.1.1 SÉCURITÉ DES RÉSEAUX ET SÉCURITÉ DE L'INFORMATION

La sécurité des réseaux est le résultat des mesures prises afin de réduire la vulnérabilité aux menaces. Par sécurité de l'information, on entend les mesures prises pour réduire la vulnérabilité de l'information dans ses diverses formes (p. ex. papier et électronique) et ses divers états (p. ex. inactive, en transit).

La sécurité des réseaux et la sécurité de l'information concernent des problèmes différents, mais il y a un chevauchement. Par exemple, la sécurité des réseaux et la sécurité de l'information ont pour objet de protéger l'information électronique transmise d'un réseau informatique à l'autre. Compte tenu ce chevauchement, certains contrôles de sécurité offrent ces deux types de sécurité.

3.2.1.2 SÉCURITÉ DE L'INFORMATION ET CRYPTOGRAPHIE

Il est recommandé d'utiliser la cryptographie dans un environnement de faible menace, bien que le présent document ne comporte aucune exigence générale pour ce qui est de la cryptographie. Vous devriez procéder à une évaluation des menaces et des risques (EMR) pour déterminer s'il convient de mettre en place des mesures relatives à la sécurité de l'information dans votre environnement de TI.

La cryptographie constitue une mesure de protection efficace de la sécurité de l'information. Elle procure la confidentialité et l'intégrité des renseignements, tout en prenant en charge d'autres services de sécurité, comme la non-répudiation (qui empêche l'expéditeur de nier avoir transmis l'information en question). La cryptographie est aussi une mesure de sécurité de réseau efficace, puisqu'elle permet de prévenir certains types d'attaques (p. ex. l'écoute clandestine et l'attaque par réinsertion). Les avantages procurés par la cryptographie varient selon la couche de la pile réseau où elle a été mise en œuvre. Certaines solutions cryptographiques, comme les services d'infrastructure à clé publique (ICP), sont mises en œuvre sur la couche application.

D'autres solutions cryptographiques, comme le chiffrement de type 1, sont stipulées à des fins de sécurité de l'information, et non de sécurité de réseau. Ces types de solutions protègent l'information, et non le réseau. Comme la sécurité de réseau est axée sur la couche transport et les couches inférieures, elle ne tient pas compte de certaines solutions cryptographiques.

Pour de plus amples conseils sur les solutions cryptographiques, prière de communiquer avec le Centre d'appel du Centre pour la cybersécurité (voir la sous-section 5.1 pour les coordonnées).

3.2.1.3 OPTIONS DE MISE EN ŒUVRE DE RÉSEAU

La séparation et les fonctions de sécurité d'un PIZ ou d'une zone peuvent être mises en œuvre physiquement ou logiquement. Vous pouvez également combiner les méthodes de mise en œuvre physiques et logiques. Vous devriez utiliser les résultats du PASSI pour déterminer s'il convient d'utiliser la séparation physique ou logique dans les frontières des zones. En se basant sur le PASSI, les artéfacts de conception de la sécurité, comme le profil de contrôle de la sécurité de domaine applicable, l'évaluation des menaces et la catégorisation de la sécurité des systèmes d'information, sont développés afin d'aider à déterminer les exigences en matière de sécurité. Ces exigences indiquent le niveau d'assurance exigé par les mécanismes de sécurité réseau physiques et virtuels.

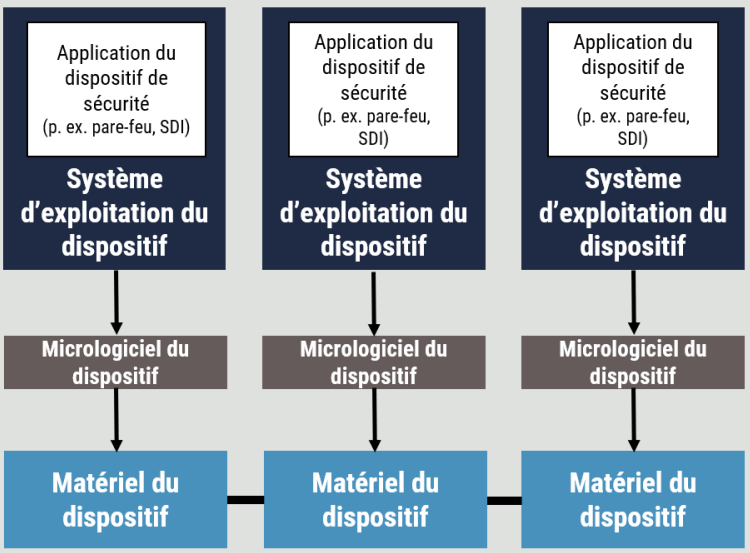
Séparation physique

La séparation physique est recommandée sur toutes les frontières de la zone démilitarisée (ZD), qui se trouve dans la ZAP et autour des ZG.

En ce qui concerne les zones et les PIZ, la séparation physique est démontrée dans les deux cas suivants :

- Un dispositif est connecté à un autre dispositif par l'entremise d'un support de communication physique (filaire ou sans fil);
- Un dispositif n'est pas connecté à d'autres systèmes.

Les mécanismes compris dans un dispositif permettent d'effectuer plusieurs opérations de sécurité ou peuvent offrir plusieurs appliances et fonctions de sécurité depuis la même plateforme. La figure 3 illustre le modèle de séparation physique.



Une appliance de sécurité physique installée sur un composant matériel distinct

Figure 3 : Modèle de séparation physique

Séparation logique

On peut utiliser la virtualisation pour assurer la séparation logique d'une frontière ou d'un périmètre de zone. La virtualisation est une technologie qui permet à un dispositif physique, comme des machines, des réseaux, des dispositifs de sécurité ou d'autres composants physiques, de se comporter comme deux ou plusieurs dispositifs, puisqu'elle virtualise et regroupe ces dispositifs en un seul système physique. La virtualisation d'un réseau combine les ressources et les fonctionnalités d'un réseau matériel et logiciel en une seule entité administrative logicielle. La figure 4 illustre le modèle de séparation logique.

Les mécanismes de sécurité mis en œuvre logiquement pourraient ne pas avoir les mêmes niveaux d'assurance que les systèmes physiques comparables. Les vulnérabilités du système d'exploitation de l'hôte et des hyperviseurs doivent également être prises en compte au moment de choisir les mécanismes de sécurité à mettre en œuvre logiquement.

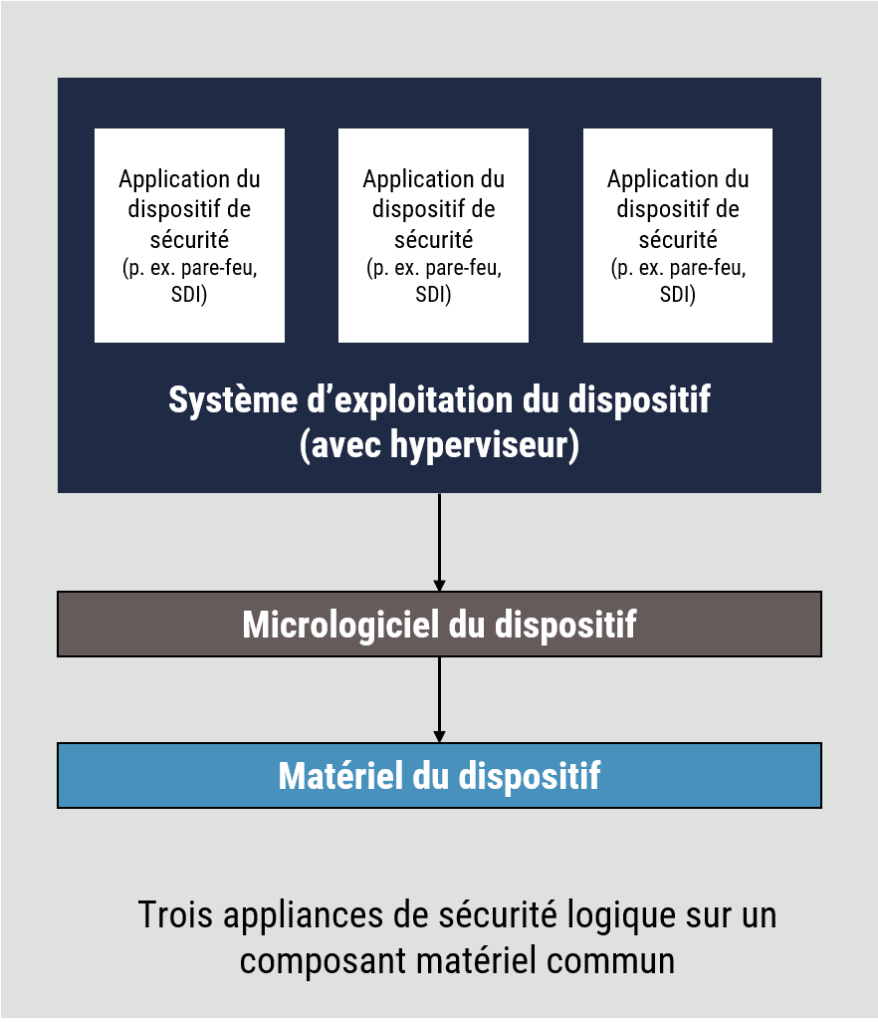


Figure 4 : Modèle de séparation logique

3.2.2 MODÈLE DE MISE EN ŒUVRE

Le modèle de mise en œuvre des zones de sécurité de réseau est illustré à la figure 5. Les ministères ou organisations peuvent mettre en œuvre plusieurs instances dans chaque type de zone selon leurs besoins opérationnels. Chaque zone contient un ou plusieurs réseaux routables distincts dans son périmètre. Chaque réseau routable distinct devrait être contenu dans une zone unique. Dans certaines circonstances, un système d'extrémité unique peut participer à plusieurs zones par l'intermédiaire d'interfaces distinctes. Voir la sous-section 4.2.1 pour une explication du système d'extrémité.

Le présent document établit les exigences de sécurité de base qui s'appliquent aux zones d'accès des réseaux : ZAP, ZT, ZAR, ZATR, ZG et PIZ. D'autres exigences de sécurité de base seront introduites ultérieurement lorsque le besoin s'en fera sentir. Une autorité de zone de sécurité de réseau peut modifier ces exigences et pratiques pour renforcer les exigences de base, pour répondre à des besoins opérationnels spécifiques, ou pour faire face à un environnement de menaces particulier. Certaines exigences devront toutefois être normalisées pour assurer l'interopérabilité du réseau.

Une zone ne correspond pas nécessairement aux secteurs d'activités ou aux fonctions de TI d'une organisation. Votre organisation peut mettre en œuvre plusieurs zones, tout comme vous pouvez mettre en œuvre plusieurs zones de sécurité matérielle. Certains secteurs d'activités ou certaines fonctions de TI pourraient également avoir des zones en commun.

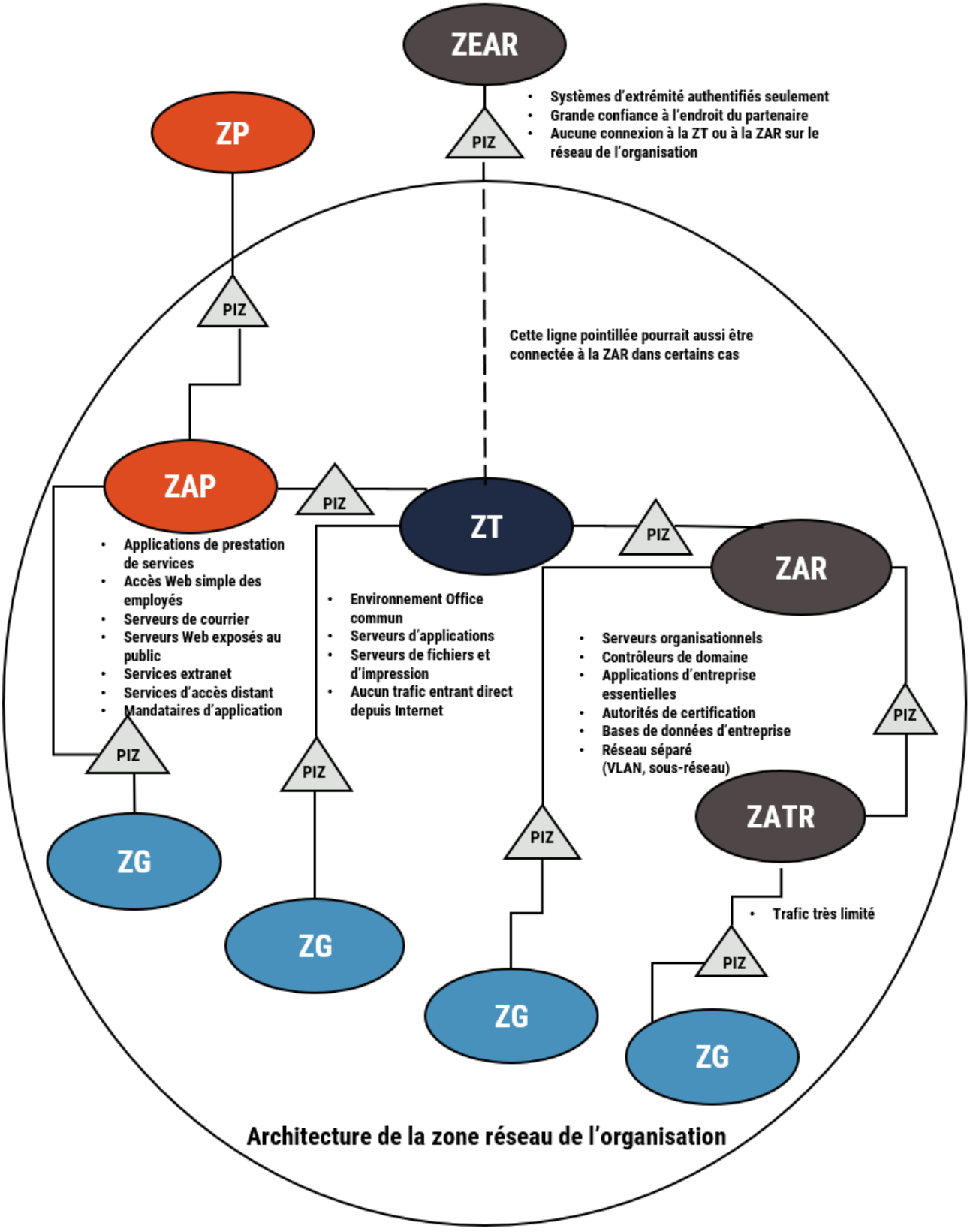


Figure 5 : Modèle de mise en œuvre d'une zone de sécurité de réseau

4 MODÈLES DE RÉFÉRENCE DES ZONES DE SÉCURITÉ DE RÉSEAU

4.1 VUE D'ENSEMBLE

La présente section comprend deux modèles de référence :

- modèle de référence général;
- modèle de référence fonctionnel.

Le modèle de référence général détermine les concepts techniques et la terminologie nécessaires à la prise en charge des exigences indiquées dans les annexes A à F du présent document. Le modèle de référence général décrit les composants d'une zone générique unique. Les modèles de référence détaillés, ainsi que les mesures de protection et les capacités des zones, sont inclus aux annexes A à E.

Le modèle fonctionnel explique les cinq principales fonctions de sécurité des zones. La structure de la présentation détaillée des exigences que l'on retrouve dans les annexes A à E s'appuie sur ces cinq fonctions.

4.2 MODÈLE DE RÉFÉRENCE GÉNÉRAL

Une zone générique comporte ces trois types de composants :

- système d'extrémité;
- interréseau;
- Système de frontière interne (SFI).

L'interréseau se compose d'un sous-système d'accès, d'un noyau et d'une interface de bordure.

La figure 6 ci-dessous illustre la topologie logique d'une zone générique, qui comprend trois composants principaux et les PIZ vers d'autres zones. Les PIZ, les systèmes d'extrémité et les SFI se connectent à l'interréseau par l'intermédiaire des interfaces de bordure (illustrés ci-dessous par de petits cercles à la figure 6). En règle générale, une instance de zone est composée d'un ou plusieurs interréseaux, ainsi que de systèmes d'extrémité et de SFI. Si une connectivité est requise entre deux interréseaux, la connexion devrait passer par un SFI (la nécessité d'une telle connexion dépend des besoins opérationnels). Les PIZ fournissent les interfaces réseau vers les autres zones. La figure 6 décrit également comment un système d'extrémité peut être partagé (c.-à-d., relié à des interréseaux de deux zones différentes). Les systèmes d'extrémité partagés doivent interdire tout trafic entre les zones.

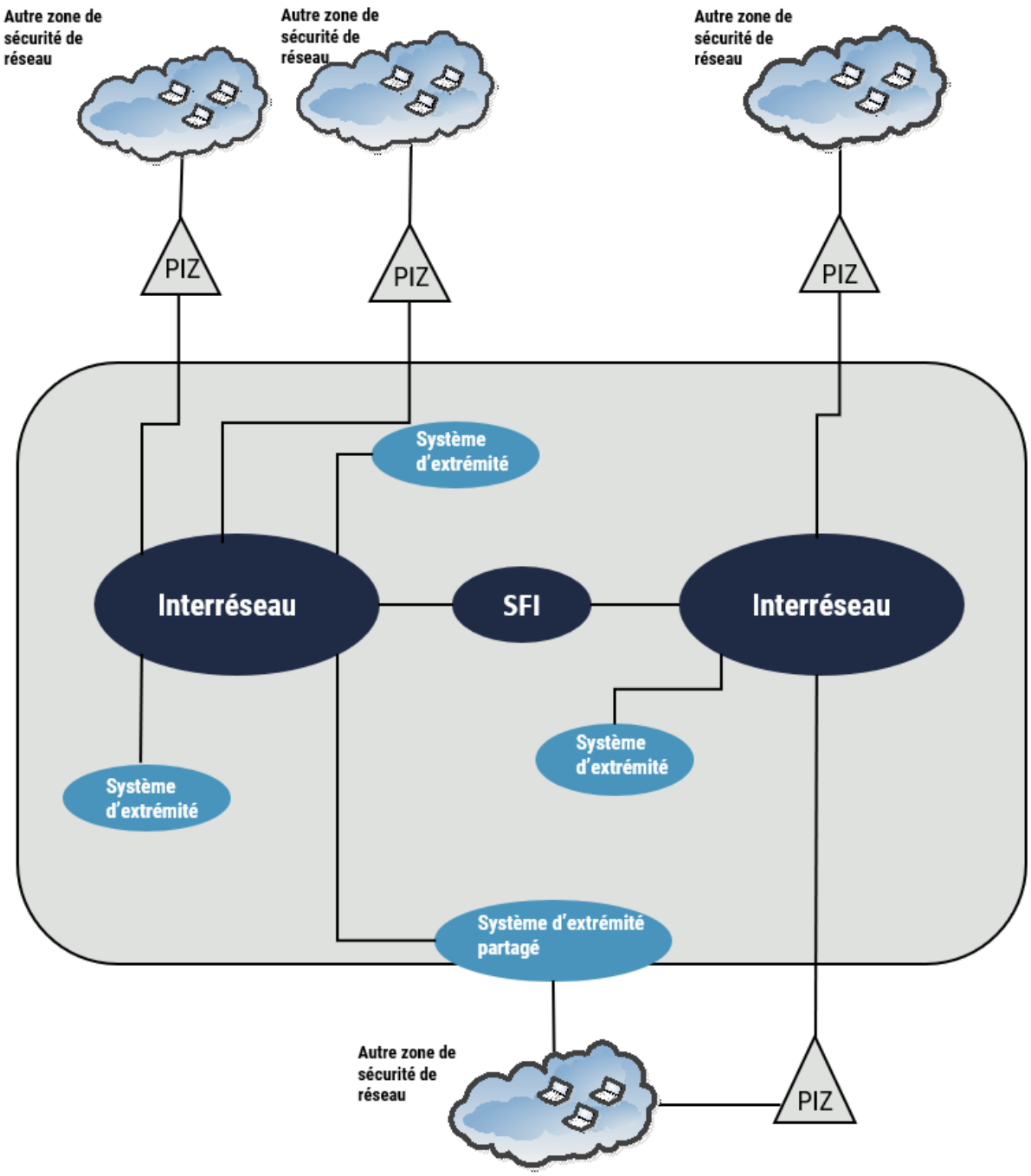


Figure 6 : Topologie logique de la zone de sécurité de réseau

Chaque composant et sous-système d'une zone est un concept logique qui comprend des fonctions et des caractéristiques particulières. Ces composants ne correspondent pas nécessairement aux dispositifs physiques. Par exemple, un dispositif physique unique pourrait incorporer les fonctionnalités de plusieurs composants de zone, ou un composant de zone unique

pourrait nécessiter plusieurs dispositifs physiques pour assurer la mise en œuvre de toutes ses fonctions et caractéristiques.

4.2.1 SYSTÈME D'EXTRÉMITÉ

Un système d'extrémité de zone est une plateforme informatique connectée à un interréseau, qui sert à établir ou interrompre une voie de communication. Bien qu'un système d'extrémité appartienne à une zone, sa sécurité relève d'un administrateur de système d'extrémité plutôt qu'une autorité de zone de sécurité de réseau. Un système d'extrémité se compose généralement d'un hôte unique, mais peut également se composer d'un réseau d'hôtes (p. ex. un réseau de stockage, une grappe de serveurs avec équilibrage de charge) connectés à l'interréseau. Les réseaux internes de ces systèmes d'extrémité complexes ne sont pas abordés dans le présent document et ne font l'objet d'aucune recommandation.

Les systèmes d'extrémité appartiennent à l'une des quatre catégories indiquées dans le tableau 1.

Tableau 1 : Catégories de systèmes d'extrémité

Catégorie de système d'extrémité	Description
Hôte simple	Système d'extrémité est composé d'un hôte unique.
Système d'extrémité mobile	Système d'extrémité (p. ex. un portable) qui se connecte parfois à la zone ou à une autre zone, comme une ZP.
Systèmes d'extrémité sans fil	Système d'extrémité qui se connecte à l'interréseau par l'entremise d'un sous-système d'accès sans fil à l'interréseau (un système d'extrémité qui comporte plusieurs interfaces avec l'interréseau est considéré un système d'extrémité sans fil si une de ces interfaces s'y connecte par l'entremise d'un sous-système d'accès sans fil à l'interréseau.
Système d'extrémité complexe	Système d'extrémité composé d'un groupe logique d'hôtes et d'un réseau privé interne entre les hôtes (p. ex. un réseau de stockage).

Si les systèmes d'extrémité utilisent des communications sans fil internes, vous devez appliquer des mesures de sécurité additionnelles pour éviter qu'on les utilise comme porte dérobée afin d'exploiter la zone.

S'il est nécessaire de connecter un système d'extrémité à deux zones ou plus simultanément, ce système d'extrémité fera office de système d'extrémité partagé (voir la figure 6 ci-dessus). Un réseau de stockage partitionné logiquement constitue un exemple de système d'extrémité partagé. Les systèmes d'extrémité partagés doivent être configurés et sécurisés de manière à interdire tout trafic entre les zones. Ils peuvent communiquer avec les zones auxquelles ils sont connectés, mais ces zones ne peuvent utiliser le système d'extrémité partagé pour acheminer du trafic entre elles. Les systèmes d'extrémité partagés doivent également respecter toutes les exigences de configuration des zones auxquelles ils se connectent. En raison de la séparation logique des systèmes d'extrémité partagés, les autorités de zone de chaque zone doivent comprendre les risques additionnels que pose chaque zone connectée et en tenir compte.

Un système d'extrémité distant est un système d'extrémité qui appartient à une ZP et communique logiquement avec une zone contrôlée par le GC ou une organisation par l'entremise ou en direction d'une ZAP. Un système d'extrémité distant n'est

pas considéré comme faisant partie d'une zone contrôlée par le GC ou une organisation. Par contre, si une zone contrôlée par le GC ou une organisation permet d'accéder à distance au réseau de ZP, les exigences de configuration de l'hôte des systèmes d'extrémité distants doivent respecter les exigences de sécurité de la zone contrôlée par le GC ou l'organisation.

4.2.2 INTERRÉSEAU

Les interréseaux offrent les services réseau qui permettent de connecter les systèmes d'extrémité, les SFI et les PIZ. Les interréseaux peuvent se composer d'une combinaison de réseaux locaux (LAN pour *Local Area Network*), de réseaux métropolitains ou de réseaux étendus (WAN pour *Wide Area Network*). Ils peuvent emprunter des supports multiples au niveau de la couche physique (p ex. un câble de cuivre ou la fibre optique) ou des liaisons sans fil (p. ex. un LAN sans fil, des liaisons sans fil fixes, des liaisons montantes). Les interréseaux offrent un service de distribution réseau (p. ex. de routage) entre les interfaces de bordure dans une zone. Un interréseau comprend les sous-systèmes mentionnés dans le tableau 2.

Tableau 2 : Sous-systèmes de l'interréseau

Sous-système	Description
Sous-système d'accès à l'interréseau	Procure les services de couche physique et de couche liaison de données qui connectent une interface de bordure au noyau de l'interréseau. La mise en œuvre de ces services comprend les ponts, le protocole Ethernet, les commutateurs de couche liaison de données (y compris les multiplexeurs) et les passerelles. Le sous-système d'accès à l'interréseau peut également fournir des services de couche réseau ou de couche supérieure. Un accès par réseau privé virtuel (RPV) serait mis en œuvre sur ces sous-systèmes. Un interréseau peut se composer de plus d'un sous-système d'accès à l'interréseau.
Noyau d'interréseau	Procure les principaux services réseau (p. ex. le routage fédérateur, la résolution d'adresses) à l'interréseau.
Interface de bordure	Frontière logique entre l'interréseau et un PIZ, un système d'extrémité ou un SFI. Parmi les exemples de mise en œuvre physique d'une interface de bordure, citons une carte d'interface réseau dans un système d'extrémité, un port d'interface sur un commutateur et la connexion entre ces derniers. Un interréseau peut comporter plus d'une interface de bordure.

Le sous-système d'accès à l'interréseau comprend les entités d'interréseau qui sont toujours sous le contrôle complet de l'autorité de zone de sécurité de réseau. À l'inverse, le noyau de l'interréseau peut intégrer des entités gérées pour le compte de l'autorité de la zone, sans être sous son contrôle direct.

Une zone contiendra au moins une instance ou un interréseau. Si une zone comprend plus d'un interréseau, les SFI fournissent la connectivité nécessaire entre les interréseaux. Une zone peut utiliser plusieurs interréseaux pour séparer le trafic et offrir une défense en profondeur additionnelle. Des interréseaux multiples peuvent également exister dans une zone lorsque des infrastructures réseau existantes sont combinées pour créer une zone.

4.2.3 SYSTÈME DE FRONTIÈRE INTERNE

Un SFI fournit une interface réseau entre deux interréseaux. Il agit également comme tampon pour la mise en œuvre du contrôle du trafic et des mesures de protection au niveau de la configuration de réseau. Un SFI se connecte aux interréseaux par l'intermédiaire d'interfaces de bordure.

Un SFI n'est requis dans une zone que si cette dernière comporte plus d'un interréseau et que si ceux-ci doivent être connectés entre eux. Entre autres exemples de SFI, notons les systèmes de protection périmétrique, comme les routeurs de filtrage, les coupe-feu, les systèmes de prévention des intrusions (IPS) et les produits de gestion unifiée des menaces (UTM).

Un SFI peut être un réseau en soi. En pareil cas, il ne constitue pas une zone distincte.

4.3 MODÈLE DE RÉFÉRENCE FONCTIONNEL

Le modèle de référence fonctionnel décrit comment les exigences liées aux zones sont structurées. Il établit et définit les différents types d'exigence. C'est sur cette structure que reposent les annexes A à E du présent document.

Le modèle de référence fonctionnel comprend les composants des exigences de sécurité illustrés au tableau 3.

Tableau 3 : Modèle de référence fonctionnel : Composants des exigences de sécurité

Composant des exigences de sécurité	Description
Exigences d'interface réseau	Ensemble des exigences de sécurité régissant les différents types d'interfaces autorisés avec les autres zones. Les exigences d'interface réseau précisent les contraintes appliquées aux frontières d'une zone. Elles portent sur des aspects tels que les interfaces permises vers d'autres zones, l'utilisation d'une infrastructure commune et le partage de systèmes d'extrémité avec d'autres zones.
Exigences de contrôle du trafic	Ensemble des exigences de sécurité régissant le flux du trafic réseau à l'intérieur de la zone, et entre la zone et les autres zones. Ces exigences portent sur les questions telles que les types de trafic, le contrôle de l'accès au réseau, les règles de non-interférence, la qualité du service, les règles de contenu du trafic et les contraintes de consommation de ressources.
Exigences de configuration de réseau	Ensemble des exigences de sécurité régissant la connexion des dispositifs à la zone. Ces exigences portent sur la gestion des associations entre entités de réseau, entités de liaison de données et les interfaces et nœuds matériels. Ces exigences prennent également en compte la gestion et le contrôle des supports de transmission physiques.
Exigences de configuration d'hôte	Les exigences de sécurité régissent la gestion des configurations du matériel et des logiciels chargés sur chaque hôte. Elles s'assurent que tous les hôtes fonctionnent à un niveau de sécurité connu sans constituer une menace pour les autres hôtes du réseau. Ces exigences ne portent pas sur la nature des logiciels permis sur un hôte, mais elles définissent plutôt les mesures nécessaires pour assurer la sécurité de la charge de logiciels de l'hôte (p. ex. configuration appropriée, application des correctifs).
Exigences de protection des données	Ensemble des exigences de sécurité régissant l'affectation et l'utilisation des services de sécurité en vue d'offrir des services de protection des données.

4.3.1 EXIGENCES D'INTERFACE RÉSEAU

Les exigences d'interface réseau précisent les contraintes appliquées aux frontières d'une zone. On peut se les représenter sous la forme d'un ensemble de règles de connexion applicable à une zone. L'annexe F du présent document est basée sur les exigences ci-dessous. Ces dernières appartiennent à l'une des catégories suivantes :

- les exigences applicables aux points d'interface de zone (voir la section 3.2.1), qui définissent les contrôles aux interfaces de la couche réseau avec les autres zones;
- les exigences applicables aux interfaces de l'infrastructure de communication sous-jacente (p. ex. les interfaces avec les entreprises de transmission de données);
- les exigences applicables aux interfaces des systèmes d'extrémité définissant les types de systèmes d'extrémité qui peuvent être rattachés à une zone de sécurité de réseau et les contraintes liées aux interfaces.

Les exigences d'interface réseau traitent des besoins suivants :

- délimiter le périmètre de zone pour veiller à ce que la portée des responsabilités de l'autorité de zone de sécurité de réseau soit claire;
- limiter les types d'interfaces prises en charge par une zone de façon à réduire l'environnement de menace auquel la zone est exposée.

4.3.2 EXIGENCES DE CONTRÔLE DU TRAFIC

Les exigences de contrôle du trafic prescrivent les mesures de protection qui contrôlent le flux de trafic à l'intérieur de la zone, et entre les zones. Elles spécifient également les capacités réseau qui devraient être présentes pour la mise en œuvre de mesures pour la gestion des plateformes, des applications et des systèmes. Les mesures de protection de contrôle du trafic sont illustrées au tableau 4.

Les exigences de contrôle du trafic précisent également les capacités réseau nécessaires pour prendre en charge les mesures de protection au niveau des plateformes, des applications et de la sécurité opérationnelle. Par exemple, une ZAR devrait pouvoir accepter l'association de sécurité IPSec entre deux interfaces de bordure et toute zone devrait pouvoir prendre en charge l'installation de détecteurs d'intrusion à certains de ses points.

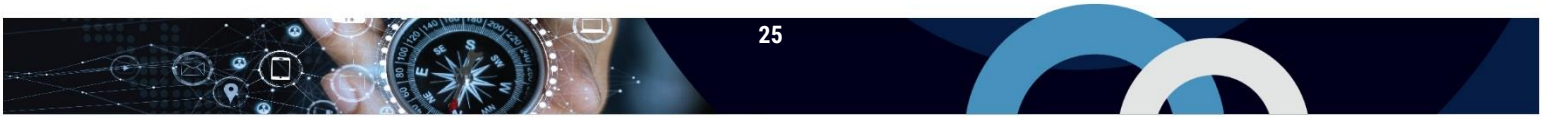


Tableau 4 : Mesures de protection de contrôle du trafic

Mesures de protection de contrôle du trafic	Description
Contrôle d'accès	Contrôle le trafic en fonction des adresses source et de destination et les types de service. Le contrôle de l'accès sert à limiter l'accès aux ressources sensibles, à restreindre les protocoles de transmission de données utilisés dans la zone, à empêcher que les communautés d'intérêts n'interfèrent les unes avec les autres, et à localiser l'incidence d'une défaillance de la sécurité.
Authentification de l'entité	Valide l'authenticité des entités et établit une association de sécurité entre elles. Le but premier de l'authentification de l'entité est de soutenir les contrôles d'accès.
Authentification de l'origine des données	Valide l'authenticité des entités qui participent à l'association de sécurité pendant toute la durée de vie de cette association. Dans le contexte du contrôle du trafic, l'authentification de l'origine des données sert principalement à soutenir les contrôles d'accès.
Vérification de l'intégrité des données	Vérifie que le trafic du réseau n'a pas été altéré ni répété. Elle sert à protéger les biens rattachés à la zone en veillant à ce que le contenu ne soit pas modifié entre sa source et sa destination.
Filtres de trafic	Filtrent ou bloquent le trafic d'après les propriétés du flux de données transmis, notamment sur le plan de l'état du protocole de contrôle du trafic (TCP), de la source et de la destination, de la conformité aux protocoles de communication autorisés, des types de données intégrés dans le flux de données et le contenu du flux de données. Par exemple, les filtres peuvent bloquer le trafic en provenance ou à destination d'adresses IP, d'adresses MAC ou de ports TCP interdits. Les filtres peuvent bloquer des protocoles non autorisés (p. ex. produits coupe-feu) et arrêter le trafic malveillant contenant des exploits ou des exploits possibles (p. ex. produits de prévention des intrusions). Ils servent aussi à filtrer les trafics porteurs de programmes malveillants (p. ex. et anti-logiciel malveillant) ou de contenus dangereux illicites (p.ex. filtres Web et de courriels).
Soutien à la détection des intrusions et à la vérification	Fournit les services et les attributs nécessaires pour soutenir la mise en œuvre de fonctions de sécurité comme la détection des intrusions, la vérification et la réaction aux incidents[5]. La journalisation du trafic et l'installation de capteurs de surveillance (p. ex. port miroir sur un commutateur) à certains points de connexion sont des formes possibles de ce soutien.
Sécurité liée à la résolution des adresses et des noms	Désigne un ensemble de mesures de sécurité visant à assurer l'intégrité de l'association entre les ressources et leurs identificateurs.
Encapsulation des ressources	Désigne les mécanismes permettant à la zone de masquer sa structure interne. Ces mécanismes comprennent la traduction d'adresses réseau et d'adresses de port, et le mappage des services. L'encapsulation des ressources prend en charge le contrôle de l'accès et la survivance.

[5] La détection des intrusions et la réaction à celles-ci constituent un important volet de la sécurité des systèmes informatiques et des réseaux. Toutefois, ces exigences de sécurité de base ne couvrent pas les processus de sécurité opérationnels, telle la détection des intrusions, sauf pour s'assurer que les mécanismes sont en place afin de garantir la disponibilité sur le réseau des informations dont ces processus ont besoin.

4.3.3 EXIGENCES DE CONFIGURATION DE RÉSEAU

Les exigences de configuration de réseau prescrivent les mesures de protection et les capacités nécessaires pour contrôler la connexion de dispositifs, tels que des systèmes d'extrémité ou du matériel de réseautage, à une zone ou leur retrait de cette dernière. Une zone offrant un très haut niveau de sécurité de réseau mettrait en œuvre des mécanismes permettant d'authentifier les interfaces de tous les réseaux et systèmes d'extrémité avant de leur permettre de participer aux communications. Une zone ayant un niveau de sécurité minimal devrait mettre en œuvre des mesures de protection destinées à empêcher le raccordement de dispositifs non autorisés.

Les mesures de protection du réseau comprennent ce qui suit :

- des contrôles administratifs (p. ex. identification des configurations, contrôle des changements, rapport sur les états des configurations et vérification des configurations);
- des mesures de sécurité matérielle;
- l'authentification;
- la journalisation des événements.

L'accès à une interface réseau est un préalable à toute attaque contre le réseau. Un auteur de menace peut accéder à l'interface réseau en connectant un dispositif non autorisé au réseau, en exploitant un hôte légitime ou en utilisant une interface externe. Les contrôles de configuration de réseau limitent la capacité d'un attaquant de connecter un dispositif non autorisé au réseau ou limitent sa capacité de le faire sans être détecté.

4.3.4 EXIGENCES DE CONFIGURATION D'HÔTE

Les exigences de configuration d'hôte régissent la configuration des hôtes connectés directement et indirectement à une zone. Ces exigences ne prescrivent pas de mesures pour protéger les biens gérés par l'hôte, mais plutôt les exigences minimales visant à garantir que les hôtes connectés à la zone ne peuvent pas compromettre la sécurité du réseau ou des systèmes d'extrémité en fournissant un point d'accès à un attaquant.

Les exigences de configuration d'hôte comprennent les mesures de protection suivantes :

- des contrôles administratifs (p. ex. gestion des configurations, gestion des vulnérabilités et vérification de la sécurité);
- des contrôles d'accès (y compris l'authentification des entités);
- des mesures de sécurité matérielle;
- des mesures de sécurité de plateforme;
- la journalisation des événements.

4.3.5 EXIGENCES DE PROTECTION DES DONNÉES

Dans le contexte du présent document, les exigences de protection des données prescrivent les mesures de protection et les capacités nécessaires à la protection de la confidentialité, de l'intégrité et de la disponibilité des données durant leur transmission.

5 SOMMAIRE

Le présent document fait mention des objectifs de sécurité, ainsi que des questions liées à la configuration et à la gestion, associés à l'application de l'architecture des zones de sécurité dans les réseaux d'un ministère ou d'une organisation.

Le modèle de référence fonctionnel mentionné dans la présente décrit comment les exigences liées aux zones sont structurées. Il établit et définit les différents types d'exigence. L'approche architecturale de la défense en profondeur repose sur ce modèle de référence dans la mesure où une mise en œuvre rigoureuse permet de protéger les données et les processus contre les cybermenaces.

Votre organisation peut utiliser les conseils prodigués dans le présent document pour mettre en œuvre un modèle de zone de sécurité de réseau offrant une approche structurée, qu'il est possible d'adapter à vos besoins en matière de sécurité.

5.1 COORDONNÉES

Pour de plus amples renseignements sur les zones de sécurité de réseau, communiquez avec nous par courriel à

Centre d'appel du
contact@cyber.gc.ca
Local : (613)-949-7048
Numéro sans frais : 1-833-CYBER-88

6 CONTENU COMPLÉMENTAIRE

6.1 LISTE DES ABRÉVIATIONS

Terme	Définition
COMSEC	Sécurité des communications (*Communication Security*)
CST	Centre de la sécurité des télécommunications
DDoS	Attaque par déni de service distribué (*Distributed Denial of Service*)
DNS	Service de noms de domaine (*Domain Name Service*)
DoS	Déni de service (*Denial of Service*)
DPS	Dirigeant principal de la sécurité
DSA	Agent de système d'annuaire (*Directory Service Agent*)
EAS	Évaluation et autorisation de sécurité
EMR	Évaluation des menaces et des risques
FIPS	Federal Information Processing Standards
FTP	Protocole de transfert de fichiers (*File Transfer Protocol*)
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
GSTI	Gestion de la sécurité des technologies de l'information
HTTP	Protocole de transfert hypertexte (*Hypertext Transfer Protocol*)
HTTPS	Protocole HTTPS (*Hypertext Transfer Protocol Secure*)
IAN	Réseau Internet (*Internet Area Network*)
ICMP	Protocole ICMP (*Internet Control Message Protocol*)
ICP	Infrastructure à clé publique
IP	Protocole Internet (*Internet Protocol*)
IPS	Système de prévention des intrusions
IPSec	Protocole IPSec (*Internet Protocol Security*)
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
KVM	Clavier-vidéo-souris (*Key-Video-Mouse*)
LAN	Réseau local (*Local Area Network*)
MAC	Contrôle d'accès au support (*Media Access Control*)
Min.	Ministère (dans les figures)
NTP	Protocole NTP (*Network Time Protocol*)
OSI	Modèle d'OSI (*Open Systems Interconnection*)

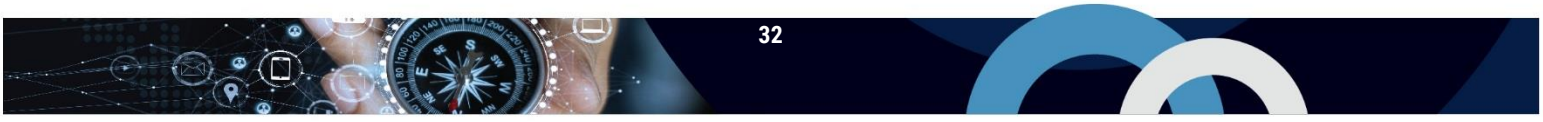
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PIZ	Point d'interface de zone
PoP	Point de présence
PVMC	Programme de validation des modules cryptographiques
RAE	Réseau d'accès externe
RPV	Réseau privé virtuel
RPVS	Réseau privé virtuel sécurisé
SCT	Secrétariat du Conseil du Trésor
SDI	Système de détection des intrusions (dans les figures seulement)
SFI	Système de frontière interne
SNMP	Protocole SNMP (*Simple Network Management Protocol*)
SSL	Protocole SSL (Secure Sockets Layer)
STI	Sécurité des technologies de l'information
TCP	Protocole de contrôle de transmission (*Transmission Control Protocol*)
TI	Technologies de l'information
TLS	Protocole TLS (*Transport Layer Security*)
URL	Adresse URL (*Uniform Ressource Locator*)
UTM	Gestion unifiée des menaces (*Unified Threat Management*)
VA	Évaluation des vulnérabilités (*Vulnerability Assessment*)
VLAN	Réseau local virtuel (*Virtual Local Area Network*) (dans les figures seulement)
ZAP	Zone d'accès public
ZAR	Zone d'accès restreint
ZAT	Zone d'accès en télégestion
ZATR	Zone d'accès très restreint
ZD	Zone démilitarisée
ZEAR	Zone extranet d'accès restreint
ZG	Zone de gestion
ZP	Zone publique
ZT	Zone de travail

6.2 GLOSSAIRE

Certaines définitions présentées dans le glossaire proviennent de sources reconnues, lesquelles sont indiquées dans les références.

Terme	Définition
Attaque par déni de service (DoS)	Attaque consistant à prévenir l'accès autorisé à une ressource du système ou à retarder les opérations et les fonctions du système [14].
Attaque par déni de service distribué (DDoS)	Attaque dans le cadre de laquelle plusieurs systèmes, généralement compromis, sont utilisés pour cibler un système particulier et causer un déni de service. Les victimes d'une attaque par DDoS sont à la fois le système d'extrémité ciblé et tous les systèmes utilisés de façon malveillante dans le cadre de l'attaque distribuée [7].
Authentification	Processus qui consiste à vérifier l'identité réclamée par une entité du système ou pour cette dernière [14].
Authentification à deux facteurs	Méthode d'authentification de l'utilisateur qui exige deux moyens (facteurs) différents de vérifier l'identité déclarée. Les trois facteurs les plus souvent utilisés sont : (1) quelque chose que vous connaissez (p. ex. un mot de passe), (2) quelque chose que vous avez (p. ex. un jeton d'authentification physique) et (3) quelque chose qui vous caractérise (p. ex. une caractéristique biométrique). Notons que l'authentification à deux facteurs ne s'applique qu'aux utilisateurs; on ne peut pas l'utiliser pour des dispositifs ou des entités homologues.
Authentification de l'entité homologue	Confirmation qu'une entité homologue au sein d'une association est bien l'entité déclarée [14].
Authentification robuste	Processus d'authentification faisant appel à la cryptographie – et particulièrement aux certificats à clé publique – pour vérifier l'identité déclarée d'une entité [14].
Autorisation	Privilège d'accès accordés à un utilisateur, un programme ou un processus [15].
Autorité de zone de sécurité de réseau	La ou les personnes qui sont responsables de la mise en place et de la gestion de la sécurité de la zone de sécurité de réseau et qui doivent rendre des comptes à cet égard.
Besoin de connaître	Principe selon lequel l'accès (y compris la connaissance) à de l'information sensible ne doit être donné qu'aux personnes qui doivent la connaître ou la posséder pour accomplir les tâches qui leur ont été assignées.
Chiffrement de bout en bout	Service de confidentialité reposant sur le chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou à la destination [9].
Code mobile	Module logiciel obtenu à partir de systèmes distants, transmis sur un réseau, téléchargé et exécuté sur un système local sans aucune installation ou exécution explicites de la part de l'utilisateur [14].
Coupe-feu	Passerelle créant entre deux réseaux une frontière qui sert à isoler, à filtrer et à protéger les ressources des systèmes locaux des connexions externes, par le contrôle du volume et des types de trafic autorisés à passer d'un réseau à l'autre.
Détection des intrusions	Service de sécurité qui surveille et analyse les événements réseau ou système afin de détecter toute tentative d'accès non autorisé aux ressources du système ou du réseau et d'émettre des alertes à cet égard en temps réel ou presque. (Définition adaptée du document [14]).

Terme	Définition
Domaine de sécurité	Contexte ou environnement défini par une politique de sécurité, un modèle de sécurité ou une architecture de sécurité visant un ensemble de ressources système et l'ensemble des entités système ayant droit d'accès à ces ressources [14].
Droit d'accès minimal	Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée — abusive ou accidentelle — d'un système d'information [15].
Encapsulation	Possibilité d'offrir aux utilisateurs une interface bien définie donnant accès à un ensemble de fonctions de façon à masquer leur fonctionnement interne.
Entité	Élément actif d'un système — par exemple, un processus automatisé, un sous-système, une personne ou un groupe de personnes — qui incorpore un ensemble précis de capacités [14].
Exigences de base en matière de sécurité	Fonctionnalités de sécurité minimales nécessaires pour se conformer aux exigences stipulées dans la *Politique sur la sécurité du gouvernement* du SCT [2], aux normes opérationnelles connexes et à la documentation technique.
Extranet	Extension contrôlée du réseau privé du GC, permettant de partager de l'information et des ressources pour des besoins opérationnels particuliers avec des partenaires spécifiques, tels que les autres gouvernements (nationaux ou étrangers), les entreprises du secteur privé et les organismes non gouvernementaux.
Extranet restreint	Extension contrôlée du réseau privé du GC, permettant de partager de l'information et des ressources pour des besoins opérationnels particuliers avec des partenaires n'appartenant pas au GC. Un tel extranet d'accès restreint peut se terminer dans une zone de sécurité contrôlée par le GC (contrairement à l'extranet générique, qui doit se terminer dans une ZAP). Les deux parties de confiance devraient convenir de la gestion et du contrôle de l'interface au préalable.
Frontière	Partie du périmètre d'une zone ou d'un réseau, qui sert de point de connexion entre deux zones ou réseaux.
Gardien	Une passerelle interposée entre deux réseaux (ou ordinateurs ou autres systèmes d'information) opérant à des niveaux de sécurité différents (l'un étant habituellement plus élevé que l'autre) et qui fournit une médiation fiable de tous les transferts d'information entre ces deux niveaux pour assurer qu'aucun renseignement sensible du premier niveau (le plus élevé) ne sera divulgué au second niveau (le moins élevé) ou pour garantir l'intégrité des données sur le système dont le niveau de sécurité est le plus élevé [14].
Gestion unifiée des menaces	Coupe-feu de réseau offrant dans un seul produit différentes fonctions, comme le filtrage des courriels, la protection contre les programmes malveillants, la détection ou la prévention des intrusions et le filtrage des contenus Web, en plus des fonctions traditionnelles d'un coupe-feu. (Définition adaptée du document [6]).
Hôte	Ordinateur connecté à un sous-réseau ou à un interréseau de communications, qui peut utiliser des services réseau pour échanger des données avec d'autres systèmes connectés au même sous-réseau ou interréseau [14].



Terme	Définition
Inspection dynamique	L'inspection dynamique intercepte les paquets au niveau de la couche réseau (comme dans les filtres de paquets), mais les données dérivées de toutes les couches de communication sont consultées et analysées pour renforcer la sécurité (plutôt que les couches 4 à 7 dans le cas des passerelles de la couche application). L'inspection dynamique accroît encore davantage le niveau de sécurité en intégrant les attributs de la couche liaison de données et de la couche application et des informations contextuelles consignées et mises à jour de façon dynamique. On obtient ainsi un référentiel de renseignements permettant d'évaluer les tentatives de communication ultérieures.
Interface	Frontière où transitent les communications entre deux systèmes. Il peut s'agir d'un connecteur matériel utilisé pour la connexion à d'autres dispositifs ou d'une convention permettant d'établir des communications entre deux systèmes logiciels. Il existe souvent entre les deux systèmes un composant intermédiaire servant à connecter leurs interfaces.
Interface de bordure	Point de l'interface de service sur la couche réseau à travers duquel un système d'extrémité, un SFI ou un PIZ est relié à l'interréseau d'une zone.
Internet	Réseau informatique mondial unique constitué d'un ensemble de réseaux commerciaux, gouvernementaux, éducatifs et autres qui partagent l'ensemble de protocoles spécifiés par le Conseil IAB (Internet Architecture Board) et l'espace de noms et d'adresses géré par la Société pour l'attribution des noms de domaines et numéros sur Internet. (Définition adaptée du document [14]).
Interréseau	Combinaison quelconque de réseaux locaux, métropolitains ou étendus fournissant tous les services réseau, ou certains d'entre eux, à une zone de sécurité de réseau.
Maliciel	Mot-valise formé de « malveillant » et de « logiciel ». Module logiciel (p. ex. bombe logique, intentionnellement inséré ou intégré dans un système informatique avec le dessein de causer des dommages. (Définition adaptée du document [14]).
Menace	Événement ou acte potentiel pouvant avoir l'une ou l'autre des conséquences suivantes : divulgation, destruction, enlèvement, modification ou interruption non autorisée d'information, de biens informatiques ou de services sensibles. Une menace peut être naturelle, délibérée ou accidentelle.
Nœud	Dispositif adressable connecté à un réseau informatique. S'il s'agit d'un ordinateur, on l'appelle plus souvent un « hôte ». Le terme *nœud* comprend également les dispositifs, comme les routeurs et les imprimantes, qui ne sont pas, à proprement parler, des « hôtes ».
Passerelle	Système intermédiaire servant d'interface entre deux réseaux informatiques [14].
Périmètre	Ligne de connexion imaginaire entourant un ensemble de composants de réseau, qui sert à décrire les limites externes d'un réseau.
Périmètre de sécurité	Frontière d'un domaine où s'applique une politique de sécurité ou une architecture de sécurité : par exemple la limite de l'espace dans lequel les services de sécurité protègent les ressources du système [14].
Plateforme	Matériel informatique précis ou combinaison donnée de matériel informatique, de système d'exploitation et/ou de compilateur (p. ex. ce programme a été transféré sur plusieurs plateformes). Le terme désigne également toute application logicielle de soutien nécessaire à la réalisation d'une activité (p. ex. ce programme offre une plateforme permettant d'effectuer une recherche dans les protocoles de routage).

Terme	Définition
Point d'interface de zone	Interface et point de connexion entre deux zones de sécurité de réseau à travers laquelle le trafic est acheminé.
Point de présence	Point de démarcation artificiel ou interface entre deux entités de télécommunications [5].
Prestation électronique de services	Prestation en ligne des services d'information et de transactions du GC aux citoyens, aux entreprises, aux autres gouvernements, aux organisations non gouvernementales et aux employés.
Protocole	Ensemble de règles (c.-à-d. formats et procédures) permettant de mettre en œuvre et de contrôler certains types d'association (p. ex., les communications) entre les systèmes. Une suite ordonnée d'étapes informatiques ou de télécommunications qui sont exécutées par deux ou plusieurs entités système pour réaliser un objectif commun [14].
Réseau privé virtuel (RPV)	Réseau informatique logique (c'est-à-dire artificiel ou simulé), à usage restreint, construit à partir des ressources d'un réseau physique (c'est-à-dire réel) relativement public (comme Internet), souvent en faisant appel au chiffrement (au niveau des hôtes ou des passerelles) et souvent en mettant sous tunnel des liaisons du réseau virtuel à travers le réseau réel. Dans le vocabulaire général, ce terme désigne souvent un réseau qui émule un réseau privé, même s'il passe par les infrastructures et les lignes du réseau public.
Réseau privé virtuel sécurisé (RPVS)	Réseau privé virtuel (RPV) utilisant la cryptographie (p. ex. IPsec) contrairement aux réseaux privés virtuels dont la sécurité est simplement fondée sur l'isolement logique (p. ex. commutation multiprotocole par étiquette ou réseau local Ethernet virtuel).
Sensible (information)	Une information est dite sensible si sa divulgation, sa contrefaçon, sa destruction ou sa perte peut entraîner des répercussions adverses sur les intérêts ou les activités de celui qui en est propriétaire ou qui l'utilise [14].
Séparation des tâches	Principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible ou essentielle sont réparties entre plusieurs entités (personnel, processus, etc.) afin d'aider à empêcher une infraction à la sécurité par une seule entité exerçant un contrôle sur l'ensemble de l'activité.
Services de mandataire	Fonction d'interréseau de service d'application pouvant être incorporée à un coupe-feu, et qui crée, pour le client, une duplication des services disponibles sur d'autres serveurs. Pour le client, le mandataire semble être le serveur lui-même, alors que pour le serveur, il se comporte comme le client. (Lorsqu'il est incorporé à un coupe-feu, un service mandataire est souvent appelé « passerelle d'applications.)
Sous-réseau	Portion d'un réseau, pouvant constituer un segment physique distinct, qui partage une adresse réseau avec d'autres portions du réseau, dont il se distingue par son numéro de sous-réseau. Le sous-réseau est au réseau ce que le réseau est à l'interréseau.
Système d'extrémité	Ordinateur connecté à un réseau qui, pour une instance de communication particulière, constitue la source ou la destination finale des communications.
Système d'extrémité partagé	Système d'extrémité connecté à deux ou plusieurs zones de sécurité de réseau, qui n'achemine pas le trafic entre les zones, mais qui satisfait aux exigences de configuration de toutes les zones auxquelles il est relié.
Système de frontière interne	Passerelle qui relie deux interréseaux ou plus dans une zone de sécurité de réseau.

Terme	Définition
Vérification de la sécurité	Revue et examen indépendants des enregistrements et des activités d'un système pour vérifier l'efficacité des contrôles système, pour assurer la conformité aux politiques établies et aux procédures opérationnelles, pour détecter les atteintes à la sécurité et pour recommander les modifications qui s'imposent aux contrôles, aux politiques et aux procédures [9].
Vulnérabilité	Lacune ou faiblesse dans les efforts de protection d'un réseau, d'un système ou d'un bien de TI [4].
Zone de sécurité de réseau	Environnement de réseau clairement délimité relevant d'une autorité de zone de sécurité de réseau et caractérisé par un niveau standard de vulnérabilité aux menaces. On distingue les types de zones d'après les exigences de sécurité s'appliquant aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte et au contrôle de la configuration du réseau.
Zone démilitarisée (ZD)	Partie d'un réseau située entre deux composants du réseau soumis à des politiques de sécurité (par exemple entre Internet et les réseaux internes) et permettant à un organisme d'héberger ses propres services Internet sans risquer l'accès non autorisé à son réseau privé.

6.3 RÉFÉRENCES

Numéro	Référence
[1]	Secrétariat du Conseil du Trésor du Canada. *Politique sur les services et le numérique* et *Directive sur les services et le numérique*. 1er avril 2020.
[2]	Secrétariat du Conseil du Trésor du Canada. *Politique sur la sécurité du gouvernement.* 1er avril 2012.
[3]	Secrétariat du Conseil du Trésor du Canada. *Directive sur la gestion de la sécurité.* 1er juillet 2019.
[4]	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie.* 30 juin 2015.
[5]	Centre canadien pour la cybersécurité. *Méthodologie harmonisée d'évaluation des menaces et des risques* (TRA-1). 23 octobre 2007.
[6]	Wikipédia. « Gestion unifiée des menaces ».
[7]	Webopedia. *IT Business Edge*. "DDoS attack – Distributed Denial of Service". 2015.
[8]	Department of Defense (É.-U.). *Department of Defense Instruction 8500.01: Cybersecurity*. 14 mars 2014.
[9]	International Organization for Standardization. *ISO 7498-2:1989 Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*. Février 1989.
[10]	SHIREY, Robert W. *The Internet Society*. "Request for Comments: 4949 – Internet Security Glossary, Version 2". Août 2007.
[11]	Committee on National Security Systems. National Counterintelligence and Security Center. *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009*. 26 avril 2010.
[12]	Centre canadien pour la cybersécurité. *ITSG-31, Guide sur l'authentification des utilisateurs pour les systèmes TI.*
[13]	Rekhter, Y., Moskowitz, B., Karrenberg, D. et al. *The Internet Society.* "Request for Comments: 1918 – Address Allocation for Private Internets". Février 1996.
[14]	Gendarmerie royale du Canada. *G1-026, Guide pour l'établissement des zones de sécurité matérielle.* Septembre 2005.
[15]	Secrétariat du Conseil du Trésor du Canada. *Ligne directrice sur la gestion de l'infrastructure à clé publique au gouvernement du Canada.* Janvier 2011.
[16]	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle sur la sécurité matérielle.* 18 février 2013.