



Conseils en matière de sécurité des TI

Établissement des zones de sécurité dans un réseau

**Considérations de conception relatives
au positionnement des services
dans les zones**

ITSG-38

Mai 2009



Page intentionnellement laissée en blanc.



Avant-propos

Le document *Établissement des zones de sécurité dans un réseau* est une publication NON CLASSIFIÉ diffusée avec l'autorisation du chef du Centre de la sécurité des télécommunications Canada (CSTC).

Pour de plus amples renseignements ou pour proposer une modification, prière de communiquer avec les Services à la clientèle de la Sécurité des TI du CSTC, par courriel à l'adresse itsclientservices@cse-cst.gc.ca ou par téléphone au 613-991-7654 ou 613-991-8495.

Date d'entrée en vigueur

Le présent document entre en vigueur au mois de mai 2009.

Gwen Beauchemin
Directrice, Gestion de la mission de la Sécurité des TI



Page intentionnellement laissée en blanc.



Résumé

Le présent document vise à aider les architectes de réseau et les spécialistes de la sécurité à positionner correctement les services (par exemple, service de noms de domaine, service de courrier électronique et service mandataire) au sein des zones de sécurité de réseau.

Un service est un concept logique représentant une série d'exigences fonctionnelles au sein d'une architecture des technologies d'information. Ces exigences fonctionnelles peuvent être simples, par exemple la résolution des noms de domaine, ou complexes, par exemple le traitement et la transmission des courriels. La mise en œuvre matérielle des services peut prendre plusieurs formes, par exemple, un processus unique tournant sur un serveur, des processus multiples tournant sur une machine virtuelle, ou encore des processus distribués tournant sur une grappe de serveurs.

Les concepts utilisés dans le présent document proviennent du document Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22), qui explique le concept des zones de sécurité de réseau et indique les exigences de sécurité de base pour les différentes zones.

Les zones de sécurité de réseau décrites dans le document ITSG-22 qui sont également abordées dans le présent document sont :

- *Zone publique*
- *Zone d'accès public*
- *Zone de travail*
- *Zone d'accès restreint*

En vue de faciliter la détermination du positionnement approprié des services, deux architectures de zones logiques types sont illustrées : une architecture de zones pour réseau de services Internet et une architecture de zones pour réseau ministériel.

Le réseau de services Internet est principalement utilisé pour assurer la prestation d'applications opérationnelles non classifiées (de niveau Protégé B ou inférieur) auprès du grand public via Internet.

Le réseau ministériel est principalement utilisé pour assurer la prestation des applications opérationnelles non classifiées (de niveau Protégé B ou inférieur) auprès des fonctionnaires.

Le présent document accompagne le guide Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22). Le présent document décrit les processus de conception appropriés, mais ne vise pas à imposer une conception spécifique pour tous les réseaux du GC. Les exemples présentés dans les présentes lignes directrices doivent être traités uniquement comme des exemples et ne devraient pas être reproduits intégralement dans une conception de réseau réelle.



Établissement des zones de sécurité dans un réseau (ITSG-38)

Page intentionnellement laissée en blanc.



Historique des révisions

N° de document	Titre	Date de publication
<i>ITSG-38</i>	<i>Établissement des zones de sécurité dans un réseau</i>	<i>Mai 2009</i>



Page intentionnellement laissée en blanc.



Table des matières

1	Introduction	1
1.1	Contexte	1
1.2	Objet.....	1
1.3	Portée.....	2
1.4	Audience	2
2	Établissement de zones.....	3
2.1	Zone	4
2.1.1	Zone publique	4
2.1.2	Zone d'accès public	4
2.1.3	Zone de travail	5
2.1.4	Zone d'accès restreint	5
2.2	Point d'interface de zone (PIZ)	5
2.2.1	Mise en œuvre matérielle des périmètres (ou PIZ)	7
3	Services	9
4	Positionnement des services.....	13
4.1	Exemple de réseau de services Internet	13
4.2	Exemple d'architecture de zones de réseau ministériel.....	15
4.3	Contextes spécifiques du réseau ministériel et du réseau de services Internet	17
4.3.1	Zone publique	18
4.3.2	Zone d'accès public	18
4.3.3	Zone de travail	20
4.3.4	Zone d'accès restreint	21
4.3.5	Zone d'accès restreint de gestion	22
4.3.6	Zone d'accès restreint du service Internet du palier Applications	23



Page intentionnellement laissée en blanc.



Liste des tableaux

Tableau 1 : Liste des services.....	9
Tableau 2 : Emplacement des services dans un réseau de services Internet.....	15
Tableau 3 : Emplacement des services dans un réseau ministériel.....	17

Liste des figures

Figure 1 : Exemple d'architecture fondée sur les zones du guide ITSG-22.....	3
Figure 2 : Points d'interface de zone.....	6
Figure 3 : Fonctionnement d'un PIZ de ZAP.....	6
Figure 4 : Périmètre formé de deux PIZ.....	6
Figure 5 : Périmètre.....	7
Figure 6 : Périmètres, PIZ et mise en œuvre équivalente sur le plan matériel.....	7
Figure 7 : Situation contextuelle d'une architecture de réseau de services Internet.....	14
Figure 8 : Situation contextuelle d'une architecture de réseau ministériel.....	16
Figure 9 : Architecture des zones d'un réseau ministériel.....	18
Figure 10 : Architecture des zones d'un réseau de services Internet.....	18
Figure 11 : Flux de communications au sein d'un réseau ministériel.....	20
Figure 12 : Architecture du réseau de services Internet.....	22



Page intentionnellement laissée en blanc.



Liste des acronymes et abréviations

CSTC	Centre de la sécurité des télécommunications Canada
DNS	Service de noms de domaine
FSI	Fournisseur de services Internet
HTTP	Protocole de transfert hypertexte
HTTPS	Protocole de transfert hypertexte sur protocole Secure Sockets Layer
IDS	Système de détection d'intrusion
IP	Protocole Internet
IPS	Système de prévention des intrusions
ITSG	Conseils en matière de sécurité des TI
PIZ	Point d'interface de zone
RPV	Réseau privé virtuel
RTPC	Réseau téléphonique public commuté
SFTP	Protocole de transfert de fichiers sécurisé
SSH	Secure Shell Protocol
STI	Sécurité des technologies de l'information
TCP	Protocole de contrôle de transmission
TI	Technologies de l'information
TLS	Couche de sécurité pour le transport
UDP	Protocole de données d'utilisateur
VCP	Voix de communication protégée
VoIP	Protocole Voix sur IP
ZAP	Zone d'accès public
ZAR	Zone d'accès restreint
ZT	Zone de travail



Page intentionnellement laissée en blanc.



1 Introduction

1.1 Contexte

L'un des éléments de la conception d'une infrastructure de sécurité des TI repose sur le concept de l'établissement de zones, qui permet de rassembler les éléments de TI similaires (matériel, logiciels, données) en groupements logiques comportant des politiques de sécurité et des exigences de sécurité identiques.

Une zone, dans le contexte du présent document, est un concept servant à définir des exigences standard de sécurité de base qui, si elles sont adoptées par les ministères du GC, permettront d'assurer l'uniformité des mesures de sécurité mises en œuvre pour les réseaux de ces ministères. Une zone délimite dans un environnement réseauté une aire logique comportant un niveau de sécurité spécifique. Les zones définissent les frontières d'un réseau et les exigences connexes en matière de défense du périmètre. À cette fin, les zones permettent de :

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

Le présent document accompagne le guide du CSTC, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22)*, qui décrit le concept de zone de sécurité de réseau et stipule les exigences de sécurité de base spécifiques pour les différentes zones.

1.2 Objet

Le présent document vise à aider les architectes de réseau et les spécialistes de la sécurité à positionner correctement les services d'infrastructure (par exemple, service de noms de domaine, service de courrier électronique, service mandataire) au sein des zones de sécurité de réseau. Pour illustrer le positionnement correct des services d'infrastructure, nous utiliserons deux architectures représentatives de zones logiques :

- architecture de réseau de services Internet;
- architecture de réseau ministériel.

Le réseau de services Internet est principalement utilisé pour assurer la prestation d'applications opérationnelles non classifiées (de niveau Protégé B ou inférieur) auprès du grand public via Internet.

Le réseau ministériel est principalement utilisé pour assurer la prestation des applications opérationnelles non classifiées (de niveau Protégé B ou inférieur) auprès des fonctionnaires.



1.3 Portée

La portée du présent document se limite aux zones de sécurité de réseau, aux points d'interface de zone (PIZ), aux périmètres et aux services d'infrastructure nécessaires à l'établissement de zones dans le cadre d'une architecture logique qui ne restreint pas la conception matérielle.

Le présent document décrit les zones suivantes, explicitées dans le guide ITSG-22 [1]:

- Zone publique (ZP);
- Zone d'accès public (ZAP);
- Zone de travail (ZT);
- Zone d'accès restreint (ZAR).

1.4 Audience

Ce document s'adresse aux architectes de réseau et aux spécialistes de la sécurité à l'emploi du gouvernement fédéral canadien.



2 Établissement de zones

L'établissement de zones permet d'atténuer les risques associés à un réseau ouvert en segmentant les services d'infrastructure en groupements logiques comportant des politiques de sécurité et des exigences de sécurité identiques. Les zones sont séparées par des périmètres (points d'interface de zone) concrétisés par des dispositifs de sécurité et autres dispositifs de réseau.

L'établissement de zones est une approche de conception logique servant à contrôler les accès et les flux de données et à restreindre aux seuls composants et utilisateurs autorisés en vertu des politiques de sécurité. Une nouvelle zone est définie par un groupement logique de services assujettis aux mêmes contraintes de sécurité en fonction des exigences opérationnelles. Lorsqu'un nouveau jeu de contraintes de sécurité est établi, une nouvelle zone doit être créée.

Le guide *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22)* décrit sept zones distinctes; toutefois le présent document couvre uniquement les quatre zones les plus couramment utilisées, illustrées à la

Figure 1 :

- Zone publique (ZP);
- Zone d'accès public (ZAP);
- Zone de travail (ZT);
- Zone d'accès restreint (ZAR).

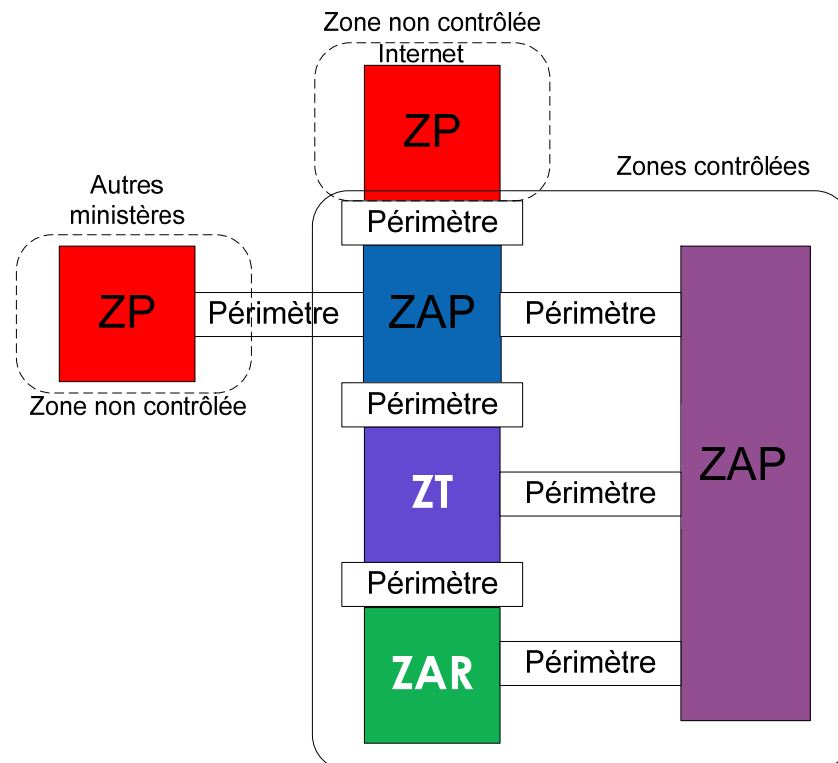


Figure 1 : Exemple d'architecture fondée sur les zones du guide ITSG-22



Établissement des zones de sécurité dans un réseau (ITSG-38)

Chaque zone possède les caractéristiques fondamentales suivantes :

- Chaque zone englobe un ou plusieurs réseaux routables distincts;
- Chaque réseau routable distinct est contenu dans une zone unique;
- Chaque zone est reliée à une autre zone au moyen d'un périmètre contenant des points d'interface de zone (PIZ);
- La seule zone autorisée à se connecter à la zone publique est la ZAP.

Les zones dont l'ensemble des composantes sont entièrement sous le contrôle du ministère sont désignées « zones contrôlées ». Dans la situation où le ministère ne contrôle pas l'ensemble des composantes d'une zone, cette zone est désignée « non contrôlée ».

Toutes les données entrant dans une zone et en sortant doivent se conformer aux exigences en matière de contrôle des données stipulées par la politique relative à cette zone.

2.1 Zone

Une zone est un concept servant à définir des exigences standard de sécurité de base qui, si elles sont adoptées par les ministères du GC, permettront d'assurer l'uniformité des mesures de sécurité mises en œuvre pour les réseaux de ces ministères. Une zone délimite dans un environnement réseauté une aire logique comportant un niveau de sécurité spécifique. Les zones définissent les frontières d'un réseau et les exigences connexes en matière de défense du périmètre. Comme il est expliqué dans le guide ITSG-22, les zones permettent de :

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

2.1.1 Zone publique

La zone publique (ZP) est entièrement ouverte; elle englobe les réseaux publics tels qu'Internet, le réseau téléphonique public 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. L'environnement de la zone publique est présumé être extrêmement hostile. [4]

2.1.2 Zone d'accès public

Le rôle de la zone d'accès public (ZAP) consiste à négocier les accès entre les systèmes opérationnels du GC et la zone publique. Les interfaces de tous les services du Gouvernement en direct devraient être mises en œuvre dans une ZAP. Les services de serveur mandataire qui permettent aux employés du gouvernement d'accéder aux applications Web devraient être mis en



Établissement des zones de sécurité dans un réseau (ITSG-38)

œuvre dans une ZAP, de même que les passerelles de courrier électronique externe, d'accès à distance et d'extranet. [4]

Une zone démilitarisée (ZD) est une composante de ZAP. Les ZD sont décrites dans le guide ITSG-22.

2.1.3 Zone de travail

La zone de travail (ZT) est l'environnement standard dans lequel sont exécutées les activités courantes du GC. C'est dans cette zone que sont installés la plupart des systèmes d'extrémité et des serveurs de groupe de travail. 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 sans l'ajout de contrôles de sécurité rigoureux et fiables qui débordent la portée des présentes lignes directrices.

À l'intérieur d'une ZT, le trafic n'est généralement pas restreint et peut provenir de sources internes, ou de sources externes autorisées par l'intermédiaire de la ZAP. Parmi les exemples de sources externes de trafic, on peut mentionner l'accès à distance, l'accès mobile et les extranets. Le trafic malveillant peut également provenir de sources hostiles internes, de programmes hostiles importés de la zone publique ou de nœuds malveillants non détectés sur le réseau (par exemple, un hôte compromis ou une connexion sans fil non autorisée à la zone). [4]

2.1.4 Zone d'accès restreint

Une zone d'accès restreint (ZAR) procure un environnement de réseau contrôlé habituellement adapté aux services de TI essentiels (ceux pour lesquels on a établi des exigences moyennes sur le plan de la fiabilité, mais où une compromission des services de TI entraînerait une interruption des activités) ou pour des dépôts volumineux d'informations sensibles (comme un centre de données). Elle permet l'accès depuis des systèmes situés dans la zone publique par l'intermédiaire d'une ZAP. [4]

2.2 Point d'interface de zone (PIZ)

Un point d'interface de zone (PIZ) établit une interface réseau entre deux zones distinctes. Les PIZ sont des concepts logiques servant à décrire les interfaces contrôlées reliant les zones. Les PIZ appliquent les politiques relatives aux transmissions de données au moyen de mesures de sécurité périmétrique. Les PIZ sont uniquement mentionnés dans le présent document afin d'explicitier le lien entre les PIZ décrits dans le document ITSG-22 et les périmètres.

Établissement des zones de sécurité dans un réseau (ITSG-38)

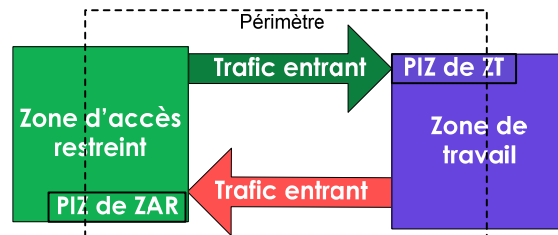


Figure 2 : Points d'interface de zone

Les PIZ possèdent les caractéristiques fondamentales suivantes :

- Tous les PIZ contrôlent les données entrantes;
- Chaque PIZ applique la politique de sécurité de sa zone respective;
- Toutes les données doivent être transmises par un PIZ¹.

La seule exception à ces caractéristiques est constituée par le PIZ installé entre la ZP et la ZAP. Le PIZ de la ZAP doit appliquer la politique de sécurité de sa zone à la fois pour le trafic entrant et le trafic sortant, puisque le GC n'exerce aucun contrôle direct sur la ZP et qu'il n'existe pas de PIZ de ZP. Cette importante distinction est illustrée à la **Figure 3** ci-dessous.

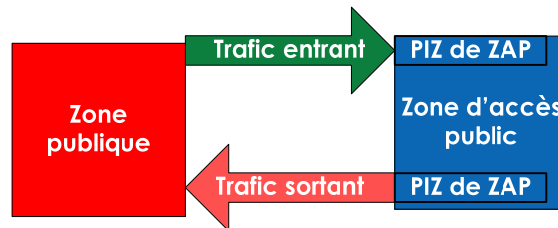


Figure 3 : Fonctionnement d'un PIZ de ZAP

Dans le contexte du présent document, les PIZ sont contenus dans un concept logique appelé « périmètre ».

Tel qu'il est illustré à la **Figure 4**, un périmètre contient les deux PIZ (le PIZ de ZT et le PIZ de ZAR) et contrôle le trafic dans les deux directions.

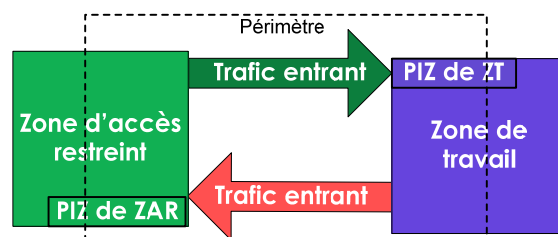


Figure 4 : Périmètre formé de deux PIZ

¹ Les données traversant une zone donnée sans aboutir à un point situé à l'intérieur de cette zone pourraient nécessiter des mesures de sécurité additionnelles.

Établissement des zones de sécurité dans un réseau (ITSG-38)

Un périmètre se compose de dispositifs de sécurité et de dispositifs de réseau et résulte de la combinaison des PIZ des deux zones adjacentes, tel qu'il est illustré à la **Figure 5**.

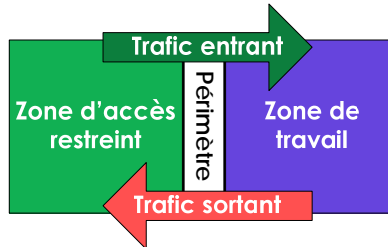


Figure 5 : Périmètre

Le recours au concept d'un périmètre contenant les deux PIZ permet de simplifier les diagrammes d'architecture, sans toutefois se soustraire à l'exigence du guide *ITSG-22* voulant que le trafic doit être contrôlé dans les deux directions (données entrantes et sortantes) pour chaque zone.

2.2.1 Mise en œuvre matérielle des périmètres (ou PIZ)

La mise en œuvre matérielle des périmètres (ou PIZ) peut se faire au moyen d'une seule composante ou d'une combinaison de composantes, tel qu'il est illustré à la **Figure 6**. La **Figure 6** illustre également comment le périmètre est équivalent aux deux PIZ (p. ex., la ZAR connectée à la ZT) et comment la mise en œuvre est réalisée sur le plan matériel (p. ex., coupe-feu, IPS, IDS et routeurs). Par exemple, un routeur (un dispositif de réseau) peut mettre en œuvre une partie du périmètre, mais il doit être utilisé en conjonction avec un système de prévention des intrusions (un dispositif de sécurité) et d'autres dispositifs de sécurité pour fournir les mesures de sécurité appropriées.

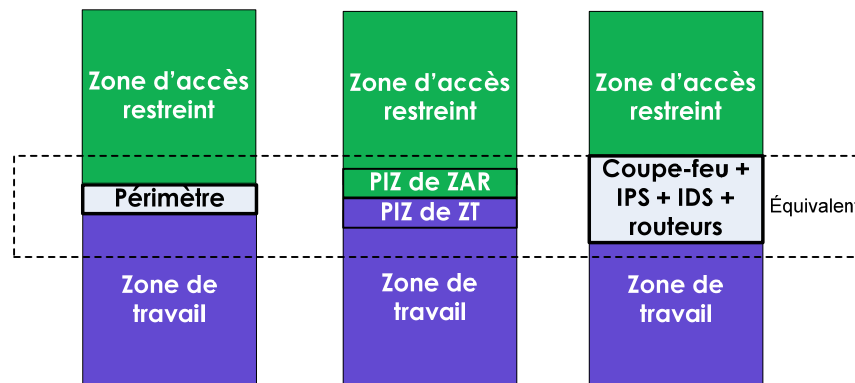


Figure 6 : Périmètres, PIZ et mise en œuvre équivalente sur le plan matériel

Les représentations matérielles telles que celles illustrées à la **Figure 6** sont des exemples uniquement qui ne reflètent aucune préférence spécifique en matière de conception ou d'approche.



Page intentionnellement laissée en blanc.



3 Services

Un service est un concept logique représentant une série d'exigences fonctionnelles au sein d'une architecture TI. Ces exigences fonctionnelles peuvent être simples, par exemple la résolution des noms de domaine, ou complexes, par exemple le traitement et la transmission des courriels. La mise en œuvre matérielle des services peut prendre plusieurs formes, par exemple un processus unique tournant sur un serveur, des processus multiples tournant sur une machine virtuelle, ou encore des processus distribués tournant sur une grappe de serveurs.

Un service peut être utilisé depuis les autres zones adjacentes, en plus de la zone dans laquelle il réside.

Le tableau ci-dessous décrit les services les plus couramment utilisés dans une infrastructure TI. Cette liste n'est pas exhaustive.

Tableau 1 : Liste des services

Nom du service	Description
Service d'accès à distance	Le service d'accès à distance fournit aux utilisateurs une connexion sécurisée avec le réseau. Ce service doit faire appel au service d'authentification pour authentifier les utilisateurs.
Service d'accès aux données	Le service d'accès aux données offre le stockage des fichiers et des services de bases de données pour les dépôts volumineux d'informations non sensibles.
Service d'accès aux données essentielles	Le service d'accès aux données essentielles offre le stockage des fichiers et des services de bases de données pour les dépôts volumineux d'informations sensibles. (Voir également Service Internet de la couche Accès aux données.)
Service d'administration de la sécurité	Ce service offre un point central pour l'administration des dispositifs de réseau et des dispositifs de sécurité.
Service d'administration TI	Le service d'administration TI assure l'administration de tous les services TI.
Service d'authentification	Le service d'authentification permet d'authentifier à la fois les applications et les utilisateurs.
Service d'horodatage	Le service d'horodatage permet l'affichage de l'heure exacte et la synchronisation horaire des plateformes informatiques au sein de l'infrastructure TI.
Service de bureautique	Le service de bureautique présente une interface utilisateur graphique ou une session de terminal aux utilisateurs pour qu'ils puissent accéder au réseau.



Établissement des zones de sécurité dans un réseau (ITSG-38)

Service de courrier électronique	Le service de courrier électronique fournit un service de courrier électronique interne et permet les communications externes par courrier électronique en communiquant avec le service de serveur mandataire de courrier électronique.
Service de noms de domaine externes	Le service de noms de domaine (DNS) externes fournit à Internet un ensemble limité d'adresses de domaine ministérielles aux fins de résolution et contrôle l'accès sécurisé des systèmes ministériels au DNS d'Internet.
Service de noms de domaine internes	Le service de noms de domaine (DNS) internes fournit les noms de domaine aux zones contrôlées (ZAP, ZT et ZAR). Les noms de domaine internes ne sont pas publiés dans le DNS externe.
Service de sauvegarde	Le service de sauvegarde assure la sauvegarde et la restauration ultérieure des données et des paramètres de configuration des plateformes informatiques. Les services de virtualisation et les services à haute disponibilité peuvent être considérés comme des services de sauvegarde.
Service de serveur mandataire d'entrée	Le service de serveur mandataire d'entrée achemine et filtre toutes les communications de données en provenance d'Internet vers les serveurs Web faisant face à la zone publique. Ce service peut assurer des fonctions d'équilibrage des charges, d'accélération du chiffrement et de filtrage de protocole.
Service de serveur mandataire de courrier électronique	Le service de serveur mandataire de courrier électronique fournit un serveur mandataire à Internet pour le service de courrier électronique et est utilisé pour toutes les communications externes par courrier électronique.
Service de serveur mandataire de sortie (serveur cache)	Le service de serveur mandataire de sortie prend en charge le filtrage des sites Web en fonction de leur contenu. Il peut permettre ou bloquer certains sites ou contenus Web selon les politiques ministérielles en vigueur.
Service de vérification	Le service de vérification reçoit les fichiers journaux créés par toutes les plateformes informatiques (p. ex., hôtes et serveurs) d'un réseau donné. Le service de vérification génère des alertes et des rapports aux fins d'un suivi ultérieur par un administrateur.
Service extranet	Le service extranet permet le partage de données et de ressources à des fins opérationnelles spécifiques avec des partenaires autorisés, par exemple d'autres niveaux de gouvernement (au pays et à l'étranger), des entités du secteur privé et des organismes non gouvernementaux.



Établissement des zones de sécurité dans un réseau (ITSG-38)

Service Internet de la couche Accès aux données	Ce service d'accès aux données stocke les données qui seront utilisées par le service Internet de la couche Application. Le service Internet de la couche Accès aux données offre le stockage des fichiers et des services de bases de données pour les dépôts volumineux d'informations sensibles. Il est jugé être équivalent au service d'accès aux données essentielles utilisé dans le réseau ministériel.
Service Internet de la couche Application	La couche Application (parfois désignée sous le nom de couche Métier) met en œuvre les fonctionnalités opérationnelles d'un réseau en exécutant les calculs et en prenant des décisions logiques. Elle est de plus responsable du traitement et du déplacement des données entre la couche Données et la couche Présentation ² .
Service Internet de la couche Présentation	Les services Internet de la couche Présentation fournit un portail aux clients externes (p. ex., les citoyens canadiens) pour qu'ils puissent demander des services gouvernementaux. La couche Présentation fournit l'information liée aux services tels que la navigation Web, les paiements par voie électronique et les échanges de données informatisés. Elle communique les demandes des utilisateurs ou des postes de travail à la couche Application.
Service intranet interne	Le service intranet interne assure l'accès aux intranets ministériels par les utilisateurs internes (p. ex., les fonctionnaires fédéraux).
Service Voix sur IP (VoIP)	Les dispositifs VoIP sont connectés à un réseau IP pour divers services tels la téléphonie.

² <http://msdn.microsoft.com/en-us/library/ms978689.aspx>



Page intentionnellement laissée en blanc.



4 Positionnement des services

La présente section décrit l'architecture des zones d'un réseau de services Internet et l'architecture des zones d'un réseau ministériel de manière à illustrer le positionnement des services.

Les exemples d'architecture décrivent la raison d'être du réseau, le positionnement des services pertinents, la situation contextuelle des zones au sein de l'architecture des zones de réseau ainsi que les politiques de sécurité mises en œuvre par les périmètres.

4.1 Exemple de réseau de services Internet

Le réseau de services Internet est principalement utilisé pour assurer la prestation d'applications opérationnelles non classifiées (de niveau Protégé B ou inférieur) auprès du grand public via Internet. Le réseau de services Internet, illustré à la **Figure 7**, se compose de quatre zones contrôlées :

- ZAR des services de la couche Accès aux données;
- ZAR des services de la couche Application;
- ZAR de gestion;
- ZAP connectée à la ZP (Internet, Réseau de la VCP).

Dans cette architecture, les applications opérationnelles sont hébergées dans les ministères du GC, et le grand public peut y accéder au moyen d'Internet et du Réseau de la Voie de communication protégée (Réseau de la VCP).



Établissement des zones de sécurité dans un réseau (ITSG-38)

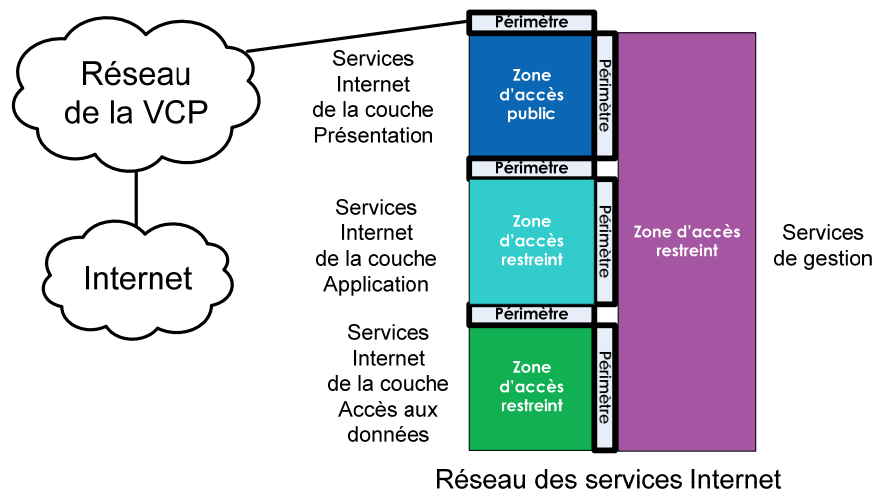


Figure 7 : Situation contextuelle d'une architecture de réseau de services Internet

Une liste générale de services était présentée à la **section 3**. Dans le cas d'une architecture de zones de réseau de services Internet, les services suivants sont normalement utilisés :

- Service de noms de domaine externes
- Service de serveur mandataire de courrier électronique
- Service de serveur mandataire d'entrée
- Service Internet de la couche Présentation
- Service de noms de domaine internes
- Service d'horodatage
- Service d'authentification
- Service de courrier électronique
- Service Internet de la couche Application
- Service Internet de la couche Accès aux données
- Service de vérification
- Service de sauvegarde
- Service d'administration TI
- Service d'administration de la sécurité

Le **Tableau 2** donne le positionnement des services dans les quatre zones d'un réseau de services Internet.



Établissement des zones de sécurité dans un réseau (ITSG-38)

Tableau 2 : Emplacement des services dans un réseau de services Internet

ZAP	ZAR des services Internet de la couche Application	ZAR de la couche Accès aux données	ZAR de gestion
Service de noms de domaine externes	Service de noms de domaine internes	Service Internet de la couche Accès aux données	Service de vérification
Service de serveur mandataire de courrier électronique	Service d'horodatage		Service de sauvegarde
Service de serveur mandataire d'entrée	Service d'authentification		Service d'administration TI
Service Internet de la couche Présentation	Service de courrier électronique		Service d'administration de la sécurité
	Service Internet de la couche Application		

4.2 Exemple d'architecture de zones de réseau ministériel

Le réseau ministériel est utilisé pour assurer la prestation des applications opérationnelles non classifiées (de niveau Protégé A ou Protégé B) auprès des fonctionnaires. Un réseau ministériel se compose de quatre zones :

- ZT;
- ZAR;
- ZAR de gestion;
- ZAP connectée à la zone publique.

L'architecture des zones pour un réseau ministériel est illustrée à la **Figure 8**. Dans cette architecture, les applications opérationnelles sont hébergées par les réseaux des ministères du GC et utilisées par les fonctionnaires. En règle générale, les fonctionnaires accèdent aux applications opérationnelles soit depuis leur propre réseau ministériel, soit par le réseau privé virtuel (RPV) du Réseau de la Voie de communication protégée (VCP).



Établissement des zones de sécurité dans un réseau (ITSG-38)

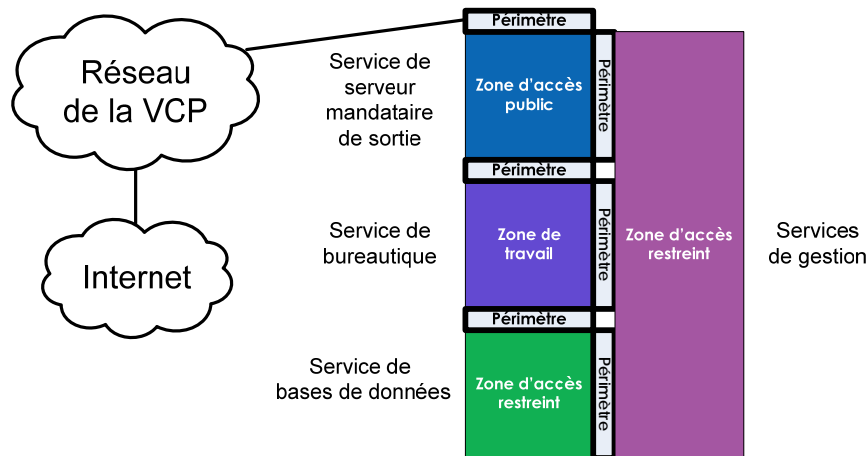


Figure 8 : Situation contextuelle d'une architecture de réseau ministériel

Une liste générale de services était présentée à la **section 3**. Dans le cas d'une architecture de zones de réseau ministériel, les services suivants sont utilisés :

- Service d'authentification d'application
- Service de vérification
- Service de sauvegarde
- Service d'accès aux données essentielles
- Service d'accès aux données
- Service de bureautique
- Service de serveur mandataire de courrier électronique
- Service de courrier électronique
- Service de noms de domaine externes
- Service extranet
- Service de serveur mandataire de sortie
- Service intranet interne
- Service d'administration TI
- Service de serveur mandataire d'entrée
- Service d'administration de la sécurité
- Service d'horodatage
- Service Voix sur IP



Établissement des zones de sécurité dans un réseau (ITSG-38)

Le Tableau 3 décrit le positionnement des services dans les quatre zones d'un réseau ministériel :

Tableau 3 : Emplacement des services dans un réseau ministériel

ZAP	ZT	ZAR	ZAR de gestion
Service de serveur mandataire de courrier électronique	Service d'authentification	Service d'accès aux données essentielles	Service de vérification
Service de noms de domaine externes	Services d'accès aux données		Service de sauvegarde
Service extranet	Service de bureautique		Service d'administration TI
Service de serveur mandataire de sortie	Service de courrier électronique		Service d'administration de la sécurité
Service Internet de la couche Présentation	Service de noms de domaine internes		
Service d'accès à distance	Service intranet interne		
Service de serveur mandataire d'entrée	Service d'horodatage		
	Service Voix sur IP		

4.3 Contextes spécifiques du réseau ministériel et du réseau de services Internet

Pour l'architecture des zones d'un réseau ministériel comme pour celle d'un réseau de services Internet, chaque zone a une raison d'être spécifique et un jeu bien défini de caractéristiques. Dans la présente section, les quatre types de zone sont décrits dans le contexte de l'architecture des zones d'un réseau ministériel et le contexte de l'architecture des zones d'un réseau de services Internet. Ces architectures sont illustrées à la **Figure 9** et à la **Figure 10** respectivement.



Établissement des zones de sécurité dans un réseau (ITSG-38)

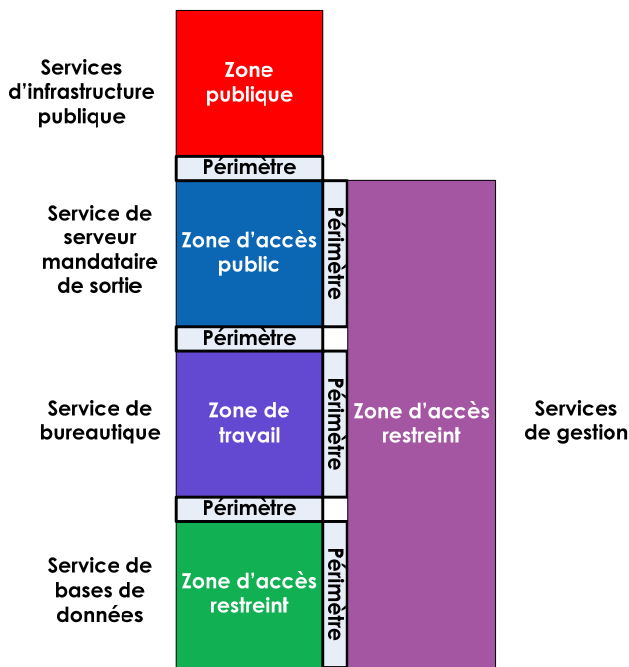


Figure 9 : Architecture des zones d'un réseau ministériel

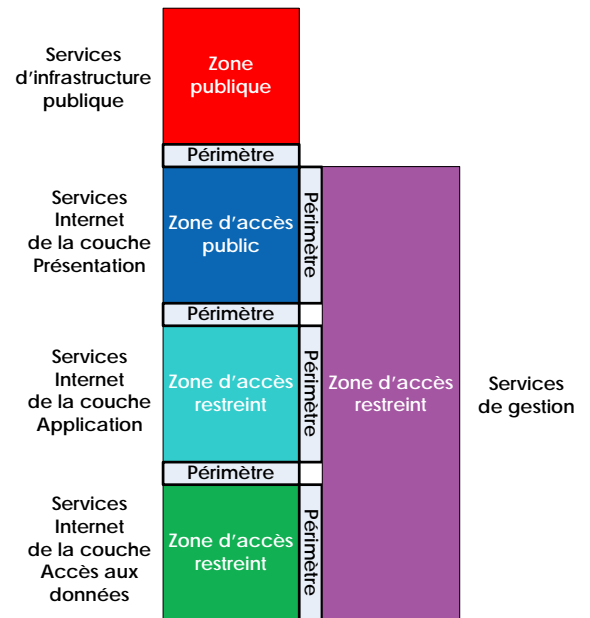


Figure 10 : Architecture des zones d'un réseau de services Internet

4.3.1 Zone publique

Les zones publiques font partie de l'infrastructure mondiale de l'information (Internet). Les réseaux fédérateurs exploités par des entreprises de télécommunications, tels que le Réseau de la Voie de communication protégée et les lignes privées, sont jugés être « non contrôlés » et sont donc traités en tant que zones publiques, puisqu'ils n'appartiennent pas au GC et qu'ils ne sont ni exploités ni matériellement contrôlés par ce dernier.

4.3.2 Zone d'accès public

4.3.2.1 Usage

La zone d'accès public (ZAP) regroupe les services de type Internet à l'intention des clients externes. Cette zone ne contient pas de données sensibles, mais permet leur passage à travers le réseau vers d'autres zones. Les données sensibles sont stockées dans des zones distinctes qui ne sont pas connectées directement à la zone publique. Le périmètre entre la ZAP et la zone publique met en œuvre différentes mesures de sécurité visant à protéger les services de la ZAP dans les zones contrôlées (ZAP, ZT et ZAR).



Établissement des zones de sécurité dans un réseau (ITSG-38)

4.3.2.2 Politique de sécurité régissant les communications avec la zone publique

Toutes les communications entrantes aboutissent à un service situé dans la ZAP, tel qu'un service de serveur mandataire ou un service de courrier électronique, après avoir été traitées au périmètre.

Toute autre communication entrante qui n'aboutit pas à un service TI situé dans la ZAP est bloquée.

Dans certaines circonstances, il est possible qu'aucun service de serveur mandataire ne soit disponible pour mettre fin à certains protocoles spécifiques dans la ZAP. Cette situation se produit habituellement, mais non exclusivement, avec les protocoles qui incorporent une fonctionnalité de chiffrement, tels que TLS (*Transport Layer Security*) et SFTP (*Secure File Transfer Protocol*). Dans cette situation, il importe de réaliser une évaluation des risques afin de déterminer les risques associés à la terminaison d'un tel trafic dans la ZT, et le besoin de faire appel à des mesures de sécurité additionnelles.

Toutes les communications qui entrent dans les zones publiques et qui en sortent devraient être circonscrites par le blocage des adresses réseau au moyen d'une liste noire, c'est-à-dire une liste des adresses réseau de la zone publique qui n'ont pas été attribuées ou qui sont des sources bien connues de données et/ou communications malveillantes. Les listes noires sont fournies par des entreprises privées, les entreprises de télécommunications et certains organismes gouvernementaux.

Toutes les communications sortantes doivent être filtrées de manière à ce que seules les adresses internes valides utilisées par le ministère soient autorisées à communiquer avec la ZP.

4.3.2.3 Politique de sécurité régissant les communications avec la zone de travail et la zone d'accès restreint

Toutes les communications entre la ZAP et les autres zones contrôlées (ZT et ZAR) devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. Dans le cas d'un réseau ministériel, le service de courrier électronique de la ZT peut uniquement communiquer avec le service de serveur mandataire de courrier électronique de la ZAP. Le service de bureautique de la ZT doit utiliser le service de serveur mandataire de sortie de la ZAP, qui à son tour communique avec les services Web de la ZP. La **Figure 11** illustre les voies de communication possibles entre la ZP et la ZAR.



Établissement des zones de sécurité dans un réseau (ITSG-38)

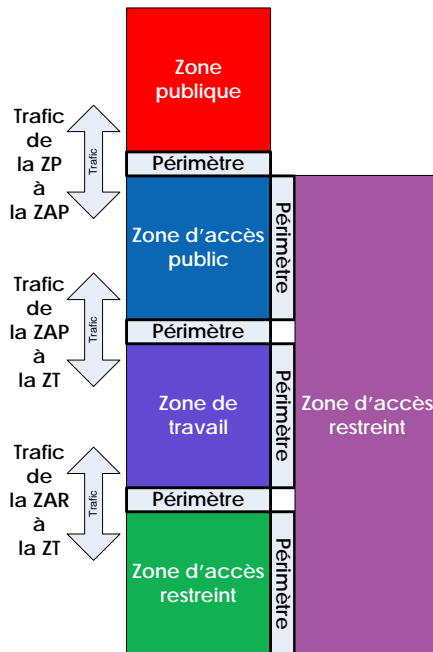


Figure 11 : Flux de communications au sein d'un réseau ministériel

4.3.2.4 Politique de sécurité régissant les communications entre la ZT, la ZAP, la ZAR et la ZAR de gestion

Toutes les communications entre la ZAR de gestion et les autres zones contrôlées (ZAP, ZT et ZAR) devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. La **Figure 11** illustre les voies de communication possibles entre la ZP et la ZAR.

4.3.3 Zone de travail

4.3.3.1 Usage

La grande majorité des activités ministérielles se déroulent dans la zone contrôlée. Les systèmes de la ZT ont accès (avec filtrage) à la ZP pour toute activité ministérielle légitime. Les communications des plateformes informatiques de la ZT qui accèdent à la ZP sont filtrées par les services de serveur mandataire et les périmètres de la ZAP.

Par exemple, les postes de travail, les imprimantes et les terminaux VoIP sont normalement hébergés dans la ZT.

4.3.3.2 Politiques de sécurité régissant les communications avec la zone publique

Les services de la ZT ne communiquent pas directement avec la zone publique. Certains protocoles qui incorporent une fonctionnalité de chiffrement, tels que SSH (*Secure Shell Protocol*) et HTTPS (*Hypertext Transfer Protocol over Secure Socket Layer*), ne peuvent pas



Établissement des zones de sécurité dans un réseau (ITSG-38)

être traités correctement par un serveur mandataire via la ZAP, et les connexions établies au moyen de ces protocoles devraient être soit refusées, soit filtrées au moyen d'une liste blanche.

Le filtrage au moyen d'une liste blanche consiste à laisser passer uniquement les adresses et protocoles autorisés. Il faudrait réaliser une évaluation des risques afin de déterminer les risques pour le réseau lorsqu'un protocole ne peut pas être interrompu dans la ZAP au moyen d'un serveur mandataire.

Si les résultats de l'évaluation des risques sont jugés acceptables par le ministère, alors les communications pourront traverser la ZAP et aboutir dans la ZT.

4.3.3.3 Politiques de sécurité régissant les communications entrantes depuis la zone d'accès public et la zone d'accès restreint

Toutes les communications entre la ZT et les autres zones contrôlées (ZAR et ZAP) devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. Les services de bureautique (la navigation Web, par exemple) devraient communiquer uniquement avec le service de serveur mandataire de la ZAP.

4.3.4 Zone d'accès restreint

4.3.4.1 Usage

Les zones d'accès restreint (ZAR) regroupent des services pour les activités des réseaux de services ministériels et de services Internet qui nécessitent des mesures de protection additionnelles contre les menaces en provenance des zones contrôlées.

Dans le cas d'un réseau ministériel, les services d'accès aux données essentielles qui doivent être protégés contre la ZT sont hébergés dans la zone d'accès restreint.

Les services Internet de la couche Accès aux données sont hébergés dans la zone d'accès restreint (3^e couche)³. Cette configuration est illustrée à la **Figure 10** à la page 18.

Dans le cas de certaines applications commerciales sur étagère, les services des couches Application et Accès aux données peuvent être regroupés dans un produit unique. Cette restriction nécessiterait que ces services soient déployés dans la ZAR (2^e couche) plutôt que dans une ZAR (3^e couche). L'approche à trois couches constitue l'architecture de sécurité de prédilection, parce qu'elle permet d'installer un périmètre entre l'application et les services de bases de données.

³ Il est possible de structurer une architecture classique à *trois couches* fondée sur une couche Présentation, une couche Application (logique) et une couche Accès aux données en utilisant une ZAP, une zone d'accès restreint pour la 2^e couche et une zone d'accès restreint pour la 3^e couche.



Établissement des zones de sécurité dans un réseau (ITSG-38)

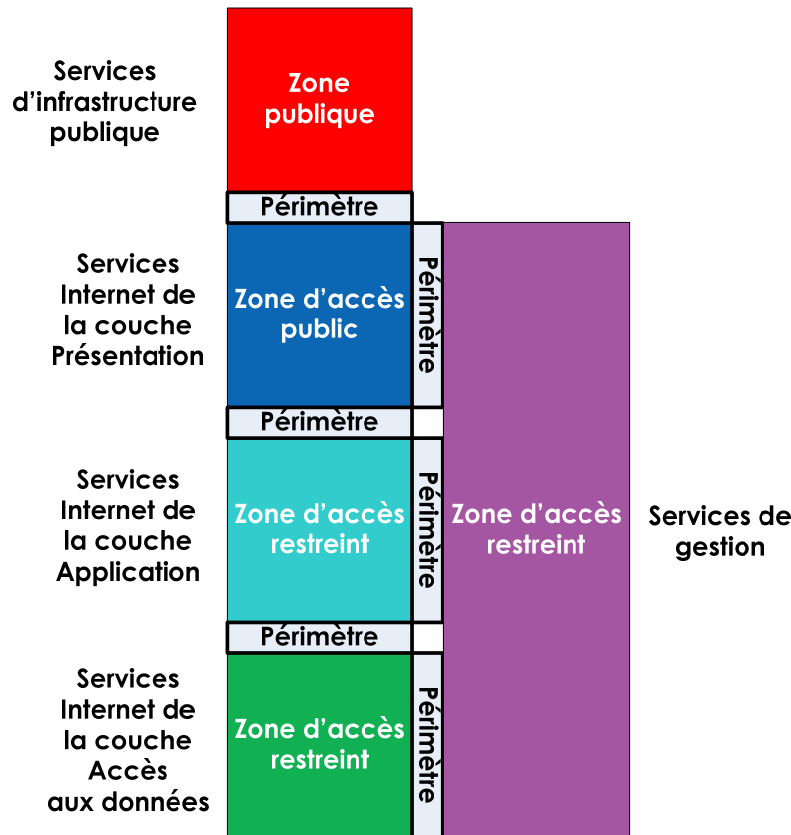


Figure 12 : Architecture du réseau de services Internet

4.3.4.2 Politiques de sécurité régissant les communications entrantes depuis la zone publique

Les services de ZAR ne communiquent pas directement avec la zone publique.

4.3.4.3 Politiques de sécurité régissant les communications entrantes depuis la zone de travail et la zone d'accès public

Toutes les communications entre la ZAR et les autres zones contrôlées devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. Les ZAR communiquent directement avec la ZT et les autres ZAR seulement. Seule exception : si la ZAR est également la ZAR de gestion, elle communiquera également avec la ZAP.

4.3.5 Zone d'accès restreint de gestion

4.3.5.1 Usage

Les architectures de réseau ministériel et de réseau de services Internet comportent une zone d'accès restreint conçue spécifiquement pour les activités de gestion, appelée « ZAR de



Établissement des zones de sécurité dans un réseau (ITSG-38)

gestion ». Cette zone regroupe les services liés à l'administration TI nécessaires pour l'exploitation du réseau ministériel ou du réseau de services Internet.

4.3.5.2 Politiques de sécurité régissant les communications avec la zone publique

Les services hébergés dans la ZAR de gestion communiquent uniquement avec la zone publique par l'intermédiaire de la ZAP pour obtenir des mises à jour sur les sites réseau d'un fournisseur en utilisant les mesures de sécurité appropriées afin de protéger l'intégrité et la confidentialité de la communication et d'authentifier l'adresse réseau du fournisseur.

4.3.5.3 Politiques de sécurité régissant les communications avec la ZT, la ZAP et la ZAR

Toutes les communications entre la ZAR et les autres zones contrôlées devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. La ZAR de gestion communique avec toutes les zones contrôlées (ZT, ZAR et ZAP).

4.3.6 Zone d'accès restreint du service Internet du palier Applications

4.3.6.1 Usage

Les architectures de réseau ministériel et de réseau de services Internet comportent une zone d'accès restreint conçue spécifiquement pour le service Internet de la couche Application, appelée ZAR du service Internet de la couche Application. Comme son nom l'indique, cette zone regroupe les services Internet de la couche Application.

4.3.6.2 Politiques de sécurité régissant les communications avec la zone publique

Les services hébergés dans la ZAR de gestion communiquent uniquement avec la zone publique par l'intermédiaire de la ZAP pour obtenir des mises à jour sur les sites réseau contrôlés d'un fournisseur en utilisant les mesures de sécurité appropriées afin de protéger l'intégrité et la confidentialité de la communication et d'authentifier l'adresse réseau contrôlée du fournisseur.

4.3.6.3 Politiques de sécurité régissant les communications avec la ZT, la ZAP et la ZAR

Toutes les communications entre la ZAR et les autres zones contrôlées devraient être traitées par le périmètre et filtrées au moyen d'une liste blanche. La ZAR de gestion communique avec toutes les zones contrôlées (les ZAR et la ZAP).



Page intentionnellement laissée en blanc.



Glossaire

Contrôles de sécurité	Mesures de sécurité conçues et mises en œuvre de manière à satisfaire aux exigences de sécurité. Il s'agit d'une abstraction logique des exigences de sécurité, spécifiée indépendamment du mécanisme matériel utilisé pour les réaliser.
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. [4]
Détection	Repérage et analyse des événements système en vue de repérer les tentatives non autorisées d'accès aux ressources d'un système.
Dispositif de réseau	Dispositif spécifiquement utilisé pour assurer une fonctionnalité propre à un réseau, par exemple un routeur ou un commutateur.
Dispositif de sécurité	Appareil dont l'objet principal est de fournir une fonctionnalité de sécurité.
Établissement de zones de sécurité d'un réseau	Approche logique permettant de contrôler les accès et les flux de données et de les restreindre aux seuls composants et utilisateurs autorisés en vertu des politiques de sécurité.
Hôte	Ordinateur en réseau qui ne retransmet pas les paquets IP qui ne sont pas adressés à cet ordinateur spécifique. [2]
Infrastructure TI	Tout ce qui est nécessaire : matériels, logiciels, réseaux, locaux, etc. pour développer, tester, fournir, surveiller, contrôler ou soutenir les services des TI. L'expression « infrastructure TI » concerne les technologies de l'information dans son ensemble, mais pas les personnes, ni les processus ou la documentation associés. [5]
Infrastructure TI du gouvernement du Canada	Tout ce qui est nécessaire : matériels, logiciels, réseaux, locaux, etc. pour développer, tester, fournir, surveiller, contrôler ou soutenir les services des TI du gouvernement du Canada. L'expression « infrastructure TI » concerne les technologies de l'information dans son ensemble, mais pas les personnes, ni les processus ou la documentation associés. [5]
Internet	Système mondial interconnecté de réseaux commerciaux, gouvernementaux, universitaires et autres qui utilisent tous la série de protocoles spécifiés par le Internet Architecture Board ainsi que les espaces de nommage et d'adressage gérés par la Internet Corporation for Assigned Names and Numbers. [2]
Liste blanche	Liste de contrôle d'accès visant à autoriser uniquement les connexions explicitement définies et à exclure toutes les autres connexions.
Liste noire	Liste de contrôle d'accès visant à exclure uniquement les connexions connues pour être malveillantes et à permettre toutes les autres connexions.
Passerelle	Système intermédiaire servant d'interface entre deux réseaux informatiques. [2]
Périmètre	Frontière entre deux zones de sécurité de réseau à travers laquelle le trafic peut être acheminé.
Plateforme informatique	Combinaison de matériel informatique et d'un système d'exploitation (lui-même composé de logiciels et/ou de micrologiciels). [2]



Établissement des zones de sécurité dans un réseau (ITSG-38)

Point d'interface de zone	Interface entre deux zones de sécurité de réseau à travers laquelle le trafic peut être acheminé. [4]
Protocole	Ensemble de règles (formats et procédures) permettant de mettre en œuvre et de contrôler certains types d'association (p. ex., les communications) entre des systèmes. Un exemple bien connu de protocole est le protocole Internet (IP). [2]
Réseau informatique	Ensemble de systèmes [de TI] et d'éléments de sous-réseau ou d'interréseau à travers lesquels les systèmes [de TI] peuvent échanger des données. [2]
Réseau privé virtuel	Réseau informatique partageant des liaisons de communication matérielles avec d'autres réseaux, mais dont les liaisons sont distinctes au plan logique.
Serveur	Plateforme informatique dont l'objet principal est d'offrir des services à d'autres plateformes informatiques. Dans le contexte du présent document, les serveurs et les postes de travail sont des plateformes informatiques.
Service	Concept logique représentant une série d'exigences fonctionnelles dans une architecture TI. Ces exigences fonctionnelles peuvent être simples, par exemple la résolution des noms de domaine, ou complexes, par exemple le traitement et la transmission des courriels. La mise en œuvre matérielle des services peut prendre plusieurs formes, par exemple, un processus unique tournant sur un serveur, des processus multiples tournant sur une machine virtuelle, ou encore des processus distribués tournant sur une grappe de serveurs.
Service de serveur 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'application ». [4]
Système d'extrémité	Système [plateforme informatique] qui, pour une instance de communication spécifique, constitue la source ou la destination ultime de la communication. [4]
Système d'utilisateur final	Système d'extrémité destiné aux activités humaines. Par exemple, un poste de travail composé d'un ordinateur personnel, d'un écran, d'un clavier, d'une souris et d'un système d'exploitation. Expression équivalente à « plateforme informatique ».
Système TI	Groupe d'éléments indépendants mais interreliés formant un élément unifié, qui collaborent en vue d'exécuter certaines tâches de traitement, de stockage ou de transmission d'information. La taille d'un système TI peut varier de petit (p. ex., système intégré, plateforme informatique, dispositif de réseau) à grand (p. ex., infrastructure TI, intranet).
Trafic malveillant	Toute donnée transmise sur un réseau qui peut compromettre la disponibilité, l'intégrité ou la confidentialité d'un système ou des données conservées sur un système.
Zone	Voir Zone de sécurité de réseau.
Zone de sécurité de réseau	Zone délimitant dans un environnement réseauté une aire logique comportant un niveau de sécurité spécifique. Les zones définissent les frontières d'un réseau et les exigences connexes en matière de défense du périmètre.



Bibliographie

- [1] National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Committee on National Security Systems, National Security Agency, juin 2006 [cité le 6 novembre 2006]. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
- [2] Internet Security Glossary, version 2 <http://tools.ietf.org/rfc/rfc4949.txt>
- [3] Baseline Security Architecture for GC IT Infrastructures, Centre de la sécurité des télécommunications Canada. 2009.
- [4] ITSG-22, Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada, Centre de la sécurité des télécommunications Canada. 2007.
- [5] ITIL® V3 Glossary v01, 30 mai 2007, http://www.best-management-practice.com/gempdf/ITILV3_Glossary_English_v1_2007.pdf
- [6] NIST SP 800-53 rev 3 - Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technologies. Février 2009.
- [7] SHIREY, Robert W. Request for Comments: 2828 – Internet Security Glossary [online]. The Internet Society, mai 2000 [cité le 25 janvier 2006]. <<http://www.ietf.org/rfc/rfc2828.txt>>.



Page intentionnellement laissée en blanc.