Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Conseils en matière de sécurité des technologies de l'information

Exigences de sécurité liées aux réseaux locaux sans fil

Aperçu

ITSG-41

Mars 2013

Canada

Avant-propos

Le document *Exigences de sécurité liées aux réseaux locaux sans fil (ITSG-41)* est un document NON CLASSIFIÉ publié avec l'autorisation du chef du *Centre de la sécurité des télécommunications Canada* (**CSTC**).

Les propositions de modifications devraient être envoyées au représentant des Services à la clientèle du CSTC par l'intermédiaire des responsables de la sécurité des TI du ministère.

Les demandes de copies supplémentaires ou de modification de la distribution devraient être soumises au représentant des Services à la clientèle du CSTC.

Pour en savoir plus, 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.

Date d'entrée en vigueur

Le présent document entre en vigueur le 2013-03-14.

Signé initialement par

Toni Moffa

Chef adjointe, Sécurité des TI

Résumé

L'information contenue dans le présent document vise à faciliter l'atténuation des menaces associées au déploiement des *réseaux locaux sans fil* (**WLAN**); elle inclut des conseils en matière de sécurité qui seront utiles durant la phase de conception de haut niveau. Les menaces types sont principalement le résultat de frontières physiques non sécurisées et incluent les suivantes :

- association non autorisée (accidentelle et malveillante);
- création de réseaux ad hoc;
- vol d'identité;
- déni de service;
- interception sans fil;
- vol de dispositif.

Les types de déploiement de WLAN, mentionnés dans le présent document, se fondent sur les besoins opérationnels actuels cernés dans les ministères du *gouvernement du Canada* (**GC**) pour les domaines classifiés et non classifiés. Les types de déploiement sont les suivants :

1) Points d'accès du gouvernement : les invités du ministère connectent leurs postes de travail sans fil à Internet par l'entremise des services WLAN du réseau ministériel; ils n'ont pas accès aux applications ministérielles;

2) Connexion utilisateur sans fil/réseau câblé : les employés situés à l'intérieur des frontières physiques du ministère connectent leurs postes de travail sans fil au réseau câblé du ministère par l'entremise des services WLAN;

3) Interconnexions de réseaux câblés par un pont sans fil : les employés situés à l'intérieur des frontières physiques du ministère connectent leurs postes de travail câblés à un sous-réseau câblé. La connectivité entre le sous-réseau et le réseau ministériel est assurée par un pont WLAN.

Des conceptions de haut niveau de référence accompagnent chaque scénario d'utilisation opérationnelle; quant aux aspects liés à la sécurité, ils sont pris en compte une fois les éléments de contrôle technique potentiels (c.-à-d. des éléments de contrôles de sécurité) déterminés et leur emplacement indiqué.

Les conseils formulés dans le présent document sont structurés de manière à faciliter leur utilisation dans le cadre des activités de gestion des risques liés à la sécurité des TI définies dans le document *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (**ITSG-33**) **[1]**[1].

1 Les numéros entre crochets ([9]) renvoient aux documents de référence qui figurent à la section ***Références*** de la dernière page du document.

Historique des révisions

Document n°	Titre	Date de publication
ITSG-41, Aperçu	Exigences de sécurité liées aux réseaux locaux sans fil – Aperçu	2013-03-14

Table des matières

AVANT-PROPOS II

DATE D'ENTRÉE EN VIGUEUR II

RÉSUMÉ III

HISTORIQUE DES RÉVISIONS IV

LISTE DES FIGURES 2

LISTE DES ANNEXES 2

LISTE DES ABRÉVIATIONS 3

1 INTRODUCTION 4

1.1 CONTEXTE 4
1.2 BUT 4
1.3 AUDITOIRE CIBLE 4
1.4 STRUCTURE DE LA PUBLICATION 4

2. VULNÉRABILITÉS COMMUNES DES WLAN 6

3. ÉLÉMENTS DE CONTRÔLE TECHNIQUES DES SERVICES WLAN 8

4. SCÉNARIOS D'UTILISATION OPÉRATIONNELLE 10

4.1 POINTS D'ACCÈS DU GOUVERNEMENT 10
4.2 CONNEXION UTILISATEUR SANS FIL/RÉSEAU CÂBLÉ 11
4.3 INTERCONNEXIONS DE RÉSEAUX CÂBLÉS PAR UN PONT SANS FIL 11

5. RÉSUMÉ 12

6. RÉFÉRENCES 13

Liste des figures

Figure 1 – Modes de transmission 6

Figure 2 – Contrôles de sécurité et éléments de contrôle 8

Figure 3 – Scénario d'utilisation opérationnelle des points d'accès du gouvernement ..10

Figure 4 – Scénario d'utilisation opérationnelle des connexions utilisateur sans fil/réseau câblé 11

Figure 5 – Interconnexions de réseaux câblés par un pont sans fil 11

Liste des annexes

Annexe 1 – Conception de haut niveau des points d'accès sans fil du gouvernement

Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé

Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil

Annexe 4 – Détermination des éléments de contrôle en fonction des contrôles de sécurité

Liste des abréviations

AES	Advanced Encryption Standard; norme AES
CDS	Cycle de développement des systèmes
Éléments de contrôle techniques	Éléments de contrôles de sécurité liés à l'application des technologies de système d'information (c.-à-d. matériel ou logiciel)
Ministère	Ministère ou organisme du GC
PASSI	Processus d'application de la sécurité dans les systèmes d'information
LAN	Réseau local
SDISF	Système de détection des intrusions sans fil
Services WLAN	Réseaux locaux sans fil déployés dans les réseaux ministériels
TI	Technologie de l'information
Wi-Fi	Technologie Wi-Fi (Wireless Fidelity), également appelée technologie « sans fil »
WLAN	Réseau local sans fil
WPA	Wi-Fi Protected Access; norme WPA

1 Introduction

1.1 Contexte

Les déploiements de réseaux locaux **(LAN**) sans fil influent sur la topologie du réseau ministériel de la même manière que l'ajout d'un LAN câblé. Les exigences de sécurité nécessaires à la protection d'un réseau local sans fil (**WLAN**) sont donc les mêmes que celles requises pour la protection d'un LAN câblé supplémentaire. Toutefois, comme la zone de couverture du WLAN ne peut être physiquement sécurisée aussi facilement que celle d'un LAN câblé, il faut tenir compte de certaines considérations supplémentaires au plan de la sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des communications du WLAN et pour protéger le réseau ministériel et ses services d'information contre les compromissions et les attaques.

Le présent document décrit le WLAN dans le contexte des dispositifs d'utilisateur sans fil reliés aux points d'accès de réseau au moyen de la technologie Wi-Fi, basée sur les normes de l'IEEE 802.11 **[2]**; il ne décrit pas les dispositifs d'utilisateur connectés au moyen de la technologie Bluetooth.

1.2 But

Le document s'appuie sur des scénarios d'utilisation opérationnelle définis pour décrire les exigences de sécurité techniques liées aux déploiements types de WLAN du ministère. Ces exigences sont ensuite associées à une architecture de référence axée sur des zones qui permet d'élaborer une conception WLAN de haut niveau.

Les conseils formulés dans le présent document sont structurés de manière à faciliter leur utilisation dans le cadre des activités de gestion des risques liés à la sécurité des *technologies de l'information* (**TI**) définies dans le guide ITSG-33**.**

1.3 Auditoire cible

Le document s'adresse aux praticiens des systèmes d'information et de la sécurité, aux décideurs au sein de la haute direction et aux responsables des activités de gestion des risques liés à la sécurité des TI qui interviennent dans la conception et la mise en œuvre des WLAN.

1.4 Structure de la publication

Ce document fait partie d'une série de documents qui constituent collectivement la suite de publications ITSG-41. Les autres documents de la série sont les suivants :

- *Annexe 1 – Conception de haut niveau des points d'accès sans fil du gouvernement;*
- *Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé;*
- *Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil;*

- *Annexe 4 – Détermination des éléments de contrôle en fonction des contrôles de sécurité.*

2. Vulnérabilités communes des WLAN

Les WLAN offrent de nombreux avantages supplémentaires par rapport aux LAN câblés, incluant une réduction des coûts de câblage, une plus grande facilité de déploiement dans les édifices existants (moins invasifs) et des capacités de prise en charge des communications en itinérance. C'est pourquoi les déploiements de ces réseaux deviennent de plus en plus populaires au sein du GC. Ce paradigme technologique soumet les ministères à des vulnérabilités supplémentaires susceptibles de compromettre la confidentialité, l'intégrité ou la disponibilité de leurs systèmes d'information et de leurs biens de TI.

Les frontières physiques de la zone de couverture des WLAN dépassent souvent le périmètre de sécurité physique du ministère. Ainsi, les attaquants ne sont pas obligés de se trouver à l'intérieur des frontières de sécurité physique du ministère pour lancer des attaques dans le réseau, tel qu'illustré à la *Figure 1 – Modes de transmission*. L'élargissement de l'environnement des communications associé à cette technologie fait en sorte que l'on doit tenir compte de menaces supplémentaires lors de la définition des exigences de sécurité inhérentes à cette solution.

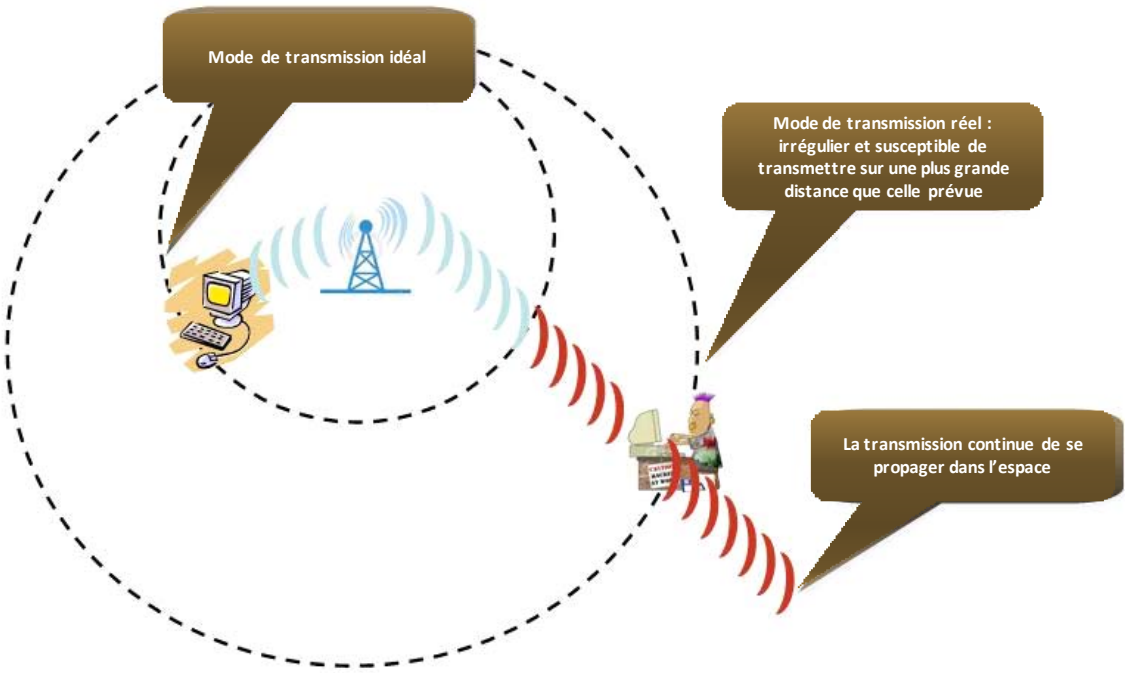

Figure 1 – Modes de transmission

Voici les vulnérabilités normalement associées aux déploiements de WLAN :

- **Association non autorisée :**
  - Accidentelle : Dispositifs ministériels qui se connectent automatiquement à un point d'accès situé dans le périmètre du réseau du ministère, mais qui ne fait pas partie du réseau. Inclut également les employés qui ajoutent par inadvertance des points d'accès au WLAN sans l'autorisation de la direction, créant ainsi des portes dérobées non sécurisées dans le réseau du ministère.
  - Malveillante : Dispositifs ministériels qui se connectent automatiquement à des points d'accès indésirables en se faisant passer pour des points d'accès valables (p. ex. les « attaques par interception » (*man-in-the-middle*) qui acheminent le trafic par un dispositif intermédiaire indésirable, permettant ainsi à l'utilisateur d'accéder aux ressources du ministère en interceptant tout le trafic).
- **Équipement non traditionnel :** Dispositifs secondaires (imprimantes Wi-Fi, dispositifs Bluetooth, etc.) ignorés par le ministère et dont les agents de menace se servent comme points d'entrée dans le réseau.
- **Réseaux ad hoc :** Connexions pair-à-pair activées dans les dispositifs ministériels (p. ex. les portables qui autorisent la connexion directe d'autres dispositifs) qui permettent à des dispositifs externes indésirables de se connecter au réseau.
- **Clonage d'identité :** Attaquant qui, en écoutant une connexion authentique, accède au réseau et clone une identité valable.
- **Déni de service :** Systèmes externes qui inondent les points d'accès du réseau de demandes d'accès falsifiées ou de données inutiles et qui empêchent ainsi les utilisateurs d'accéder au réseau, ce qui entraîne éventuellement une panne du WLAN.
- **Interception sans fil :** Trafic hertzien chiffré de manière inappropriée qui permet à des utilisateurs externes de faire de l'écoute clandestine.
- **Vol de dispositif :** Risque accru de vols de dispositifs sans fil en raison de leur portabilité; les dispositifs et/ou réseaux sont alors plus faciles à compromettre.

Étant donné l'augmentation des risques potentiels, il faut prévoir des contrôles de sécurité spécifiques et adapter les éléments de contrôle connexes à la solution déployée.

3. Éléments de contrôle techniques des services WLAN

Conformément au *Cycle de développement des systèmes* (**CDS**) du ministère, on a prévu la mise en place d'une phase d'analyse des besoins (définie dans le guide ITSG-33, Annexe 2 **[1]**) qui permet de sélectionner un ensemble approuvé de contrôles de sécurité adaptés au déploiement des services WLAN. La sélection des contrôles tient compte des aspects suivants :

a. besoins opérationnels des services de réseau local sans fil en matière de sécurité;

b. contrôles de sécurité ministériels obligatoires applicables au déploiement.

La *Figure 2 – Contrôles de sécurité et éléments de contrôle* montre l'ensemble approuvé de contrôles de sécurité prévus pour le déploiement des services WLAN et inclut les classes de contrôles de sécurité techniques, opérationnels, et de gestion. Le guide ITSG-33 définit ces classes comme suit :

a. Classe des contrôles de sécurité de gestion – comprend les contrôles de sécurité portant principalement sur les activités qui se rapportent à la gestion de la sécurité des TI et aux risques liés à la sécurité des TI;

b. Classe des contrôles de sécurité techniques – comprend les contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information principalement par l'intermédiaire de mécanismes de sécurité qu'on retrouve dans les composants matériels, logiciels et micrologiciels;

c. Classe des contrôles de sécurité opérationnels – comprend les contrôles de sécurité de système d'information qui sont mis en œuvre principalement par l'intermédiaire de processus exécutés par des personnes (c.-à-d. évaluation de la conformité aux politiques ou exécution de procédures).

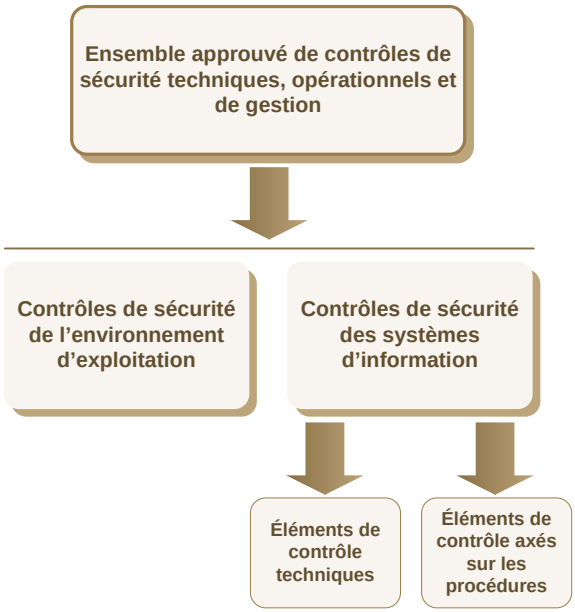

Figure 2 – Contrôles de sécurité et éléments de contrôle

Ces contrôles de sécurité sont ensuite regroupés en deux catégories :

- contrôles de sécurité liés à l'environnement d'exploitation;
- contrôles de sécurité liés aux systèmes d'information.

Les contrôles de sécurité liés à l'environnement d'exploitation ne sont pas décrits en détail dans le présent document puisqu'ils sont de nature essentiellement gestionnelle ou opérationnelle et appliqués au niveau du ministère par le biais de programmes, de politiques ou de procédures.

Les autres contrôles de sécurité liés aux systèmes d'information sont divisés comme suit :

- Éléments de contrôle techniques – éléments de contrôles de sécurité qui doivent être appliqués par des moyens techniques (p. ex. coupe-feu);
- Éléments de contrôle axés sur les procédures – éléments de contrôles de sécurité qui sont appliqués conformément à des politiques ou des procédures manuelles (p. ex. examen manuel des journaux de coupe-feu).

Puisque les éléments de contrôle axés sur les procédures sont intimement liés à la mise en œuvre d'exigences techniques (p. ex. la sélection de produits de TI, la politique ministérielle et la tolérance au risque), le présent document aborde uniquement les éléments de contrôle techniques. Les ministères doivent donc définir les éléments de contrôle correspondants axés sur les procédures pour appuyer la solution qu'ils ont retenue.

4. Scénarios d'utilisation opérationnelle

Les types de déploiements de WLAN et les éléments de contrôle techniques connexes abordés dans le présent document s'appuient essentiellement sur les besoins opérationnels des ministères. Les différents types de déploiements couvrent une gamme de scénarios allant d'une architecture rudimentaire de points d'accès à des applications plus complexes, telle l'interconnexion de réseaux ministériels par les services WLAN.

4.1 Points d'accès du gouvernement

Le scénario d'utilisation opérationnelle des points d'accès du gouvernement décrit le déploiement de services WLAN qui permet aux invités du ministère (c.-à-d. les non-employés) de connecter leurs dispositifs sans fil à Internet (Figure 3). Dans ce scénario, le rôle du réseau ministériel consiste essentiellement à traiter les communications des invités en provenance et à destination d'Internet. Les autres services ministériels offerts par le réseau ne sont pas accessibles aux invités, tels que décrits à l'*Annexe 1*.

Figure 3 – Scénario d'utilisation opérationnelle des points d'accès du gouvernement

Exemple : un ministère offre un accès Internet aux visiteurs dans une zone commune (p. ex. une salle d'attente ou une salle de réunion).

4.2 Connexion utilisateur sans fil/réseau câblé

Le scénario d'utilisation opérationnelle des connexions utilisateur sans fil/réseau câblé décrit le déploiement de services WLAN qui permet aux employés situés dans le périmètre physique du ministère de connecter leurs postes de travail sans fil (c.-à-d. les portables ou les ordinateurs de bureau) au réseau ministériel (Figure 4). Les employés peuvent se connecter aux services WLAN depuis leur bureau ou en itinérance (sans interruption de leur session) partout dans le ministère où les services sont disponibles, comme décrit à l'*Annexe 2*.

Figure 4 – Scénario d'utilisation opérationnelle des connexions utilisateur sans fil/réseau câblé

Exemple : un employé sur place utilise un portable sans fil pour se connecter aux ressources du ministère et s'acquitter de ses tâches courantes.

4.3 Interconnexions de réseaux câblés par un pont sans fil

Le scénario d'utilisation opérationnelle des interconnexions de réseaux câblés par un pont sans fil décrit le déploiement de services WLAN qui permet de relier un LAN câblé isolé à un réseau ministériel (Figure 5). Il n'y a aucune connexion physique entre le LAN câblé et le réseau ministériel. Le service WLAN étend l'accès du réseau et permet aux employés qui utilisent le LAN câblé isolé d'accéder aux services du réseau ministériel, tel que décrit à l'*Annexe 3*.

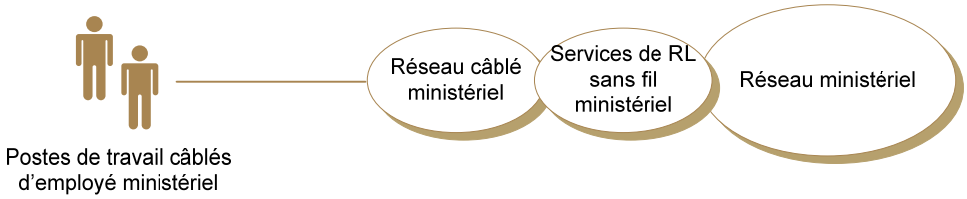

Figure 5 – Interconnexions de réseaux câblés par un pont sans fil

Exemple : deux infrastructures de réseau distinctes interconnectées au moyen de services sans fil (p. ex. d'un navire à un port).

5. Résumé

L'information contenue dans le présent document permettra, durant les phases d'analyse des besoins et de conception de haut niveau du CDS, de déterminer les contrôles de sécurité et les éléments de contrôle techniques appropriés pour aider à atténuer les menaces typiques auxquelles sont confrontés les WLAN. Les éléments de contrôle techniques présentés dans les annexes sont décrits dans le contexte d'une architecture de réseau axée sur les « zones » pour chaque scénario d'utilisation opérationnelle. Les praticiens de la sécurité doivent donc choisir l'annexe qui les concerne en se basant sur leur propre scénario d'utilisation et appliquer l'information qui s'y trouve pour les aider à mener à terme leur conception de haut niveau axée sur les zones.

6. Références

[1] *ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie – Aperçu* (**CSTC**) (nov. 2012)

[2] *IEEE Standards Association* (standards.iee.org)