Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Conseils en matière de sécurité des technologies de l'information

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

ITSG-41 – Annexe 1

Septembre 2012

Canada

Avant-propos

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

La présente publication entre en vigueur le (date à déterminer).

Toni Moffa

Chef adjointe, Sécurité des TI

Historique des révisions

Document nº	Titre	Date de publication
ITSG-41, Annexe 1	Conception de haut niveau des points d'accès sans fil du gouvernement	À déterminer

Table des matières

AVANT-PROPOS ..... **II**

DATE D'ENTRÉE EN VIGUEUR ..... **II**

HISTORIQUE DES RÉVISIONS ..... **III**

TABLE DES MATIÈRES ..... **IV**

LISTE DES FIGURES ..... **V**

LISTE DES TABLEAUX ..... **V**

LISTE DES ABRÉVIATIONS ..... **VI**

1. INTRODUCTION **1**

1.1 BUT 1
1.2 AUDITOIRE CIBLE 2
1.3 STRUCTURE DE LA PUBLICATION 2

2. CONCEPTION DE HAUT NIVEAU DES POINTS D'ACCÈS SANS FIL DU GOUVERNEMENT **3**

2.1 CONCEPTION DE HAUT NIVEAU DE RÉFÉRENCE DU RÉSEAU MINISTÉRIEL 3
2.1.1 Zones publiques *4*
2.1.2 Zones d'accès public *4*
2.1.3 Zones de travail *4*
2.1.4 Zones d'accès restreint *5*
2.1.5 Zones de gestion à accès restreint *7*
2.2 CONCEPTION DE HAUT NIVEAU DE RÉFÉRENCE DES SERVICES WLAN 7
2.2.1 Composants *8*
2.2.2 Communications *10*
2.2.3 Concept d'opération *12*
2.2.4 Restriction d'accès *13*
2.2.5 Surveillance *13*
2.3 POINTS DE MISE EN ŒUVRE DES ÉLÉMENTS DE CONTRÔLE TECHNIQUES 14
2.3.1 Résumés des éléments de contrôle techniques *15*
2.3.2 Recommandations concernant les points de mise en œuvre *24*

3. RÉFÉRENCES **75**

Liste des figures

Figure 1 – ITSG-33, Processus d'application de la sécurité dans les systèmes d'information 2

Figure 2 – Zones du réseau ministériel 3

Figure 3 – Services du réseau ministériel 6

Figure 4 – Point d'accès sans fil du gouvernement 9

Figure 5 – Types de communications des points d'accès sans fil du gouvernement 11

Figure 6 – Contrôles de sécurité et éléments de contrôle 14

Liste des tableaux

Tableau 1 – Points de mise en œuvre des points d'accès sans fil du gouvernement 25

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

1. Introduction

1.1 But

La présente annexe vise à faciliter la spécification de la conception de haut niveau pour assurer le déploiement sécurisé des services de *réseau local sans fil* (**WLAN**) en conformité avec la norme *802.11i* (**802.11**) [1][1] de l'*Institute of Electrical and Electronics Engineers (IEEE)*.

Le document inclut une conception de haut niveau de référence qui répond aux besoins du scénario d'utilisation opérationnelle des points d'accès sans fil du gouvernement suivant lequel des utilisateurs invités du ministère (c.-à-d. des non-employés) connectent leurs postes de travail sans fil (portables, assistants numériques, etc.) à Internet en utilisant les services WLAN du réseau ministériel. Ils ne peuvent accéder aux autres services du réseau ministériel offerts aux employés.

La structure des conseils en matière de sécurité respecte le cadre des activités de gestion des risques liés à la sécurité des technologies de l'information (**TI**) définies dans le document *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (**ITSG-33**) [2].

Le présent document doit être utilisé durant les activités de conception de haut niveau, tel qu'illustré dans la Figure 1 de l'ITSG-33, *Processus d'application de la sécurité dans les systèmes d'information*, définies dans le *Processus d'application de la sécurité dans les systèmes d'information* (**PASSI**) (voir le guide ITSG-33, Annexe 2 – Activités de gestion des risques liés à la sécurité des systèmes d'information, pour plus de détails). L'utilisation du document minimise les travaux de développement. Les ministères peuvent suivre les conseils qui s'y trouvent pour développer leur propre conception de haut niveau pour le déploiement des services WLAN et utiliser les conceptions de haut niveau de référence comme point de départ. Le document inclut des recommandations concernant les points de mise en œuvre des éléments de contrôle techniques dans les conceptions de référence.

Les éléments de contrôle techniques sont déterminés à partir de contrôles de sécurité sélectionnés dans le guide ITSG-33 (Annexe 3 – Catalogue des contrôles de sécurité). Les contrôles de sécurité sont sélectionnés pour :

1) répondre aux besoins opérationnels en matière de sécurité du déploiement des services WLAN;

2) se conformer aux contrôles de sécurité exigés par le ministère en matière de déploiement des services WLAN.

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

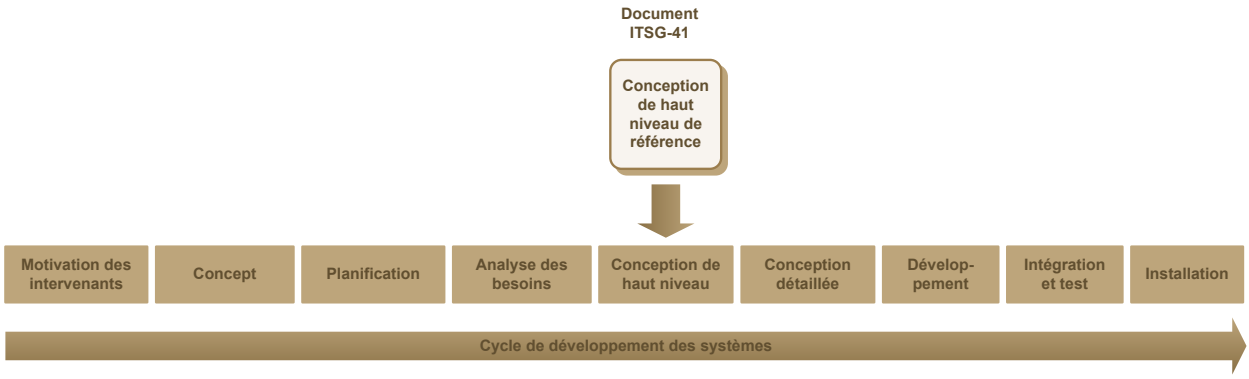

Figure 1 – ITSG-33, Processus d'application de la sécurité dans les systèmes d'information

1.2 Auditoire cible

Le présent document s'adresse aux praticiens de la sécurité et des systèmes d'information ainsi qu'aux responsables des activités de gestion des risques liés à la sécurité des TI liées à la conception et à la mise en œuvre de WLAN.

1.3 Structure de la publication

Le présent 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 :

- *ITSG-41, Exigences en matière de sécurité des réseaux locaux sans fil* [3]
- *ITSG-41, Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé* [4]
- *ITSG-41, Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil* [5]
- *ITSG-41, Annexe 4 – Détermination des éléments de contrôle en fonction des contrôles de sécurité* [6]

2. Conception de haut niveau des points d'accès sans fil du gouvernement

Cette section présente, dans un premier temps, la conception de haut niveau de référence d'un réseau ministériel type. La conception est ensuite complétée par les services WLAN du scénario d'utilisation opérationnelle de point d'accès sans fil du gouvernement. La section inclut également des recommandations concernant l'endroit où les éléments de contrôle techniques peuvent être appliqués dans la conception de haut niveau de référence. Le processus utilisé pour déterminer les éléments de contrôle techniques à partir d'un ensemble approuvé de contrôles de sécurité est décrit à l'Annexe 4**.**

2.1 Conception de haut niveau de référence du réseau ministériel

La conception de haut niveau de référence du réseau ministériel utilise le concept des zones, tel que décrit dans le guide *ITSG-38, Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* (**ITSG-38**) **[7].**

Le guide ITSG-38 décrit quatre types principaux de zone : zones publiques, zones d'accès public, zones de travail et zones d'accès restreint. Ces zones sont décrites dans les sous-sections suivantes et illustrées dans la Figure *2 – Zones du réseau ministériel* (**Figure 2**). Un ministère peut utiliser plusieurs zones d'un même type pour séparer des services d'information qui figurent dans un même type de zone, mais dont les exigences en matière de sécurité sont différentes. Par exemple, le ministère peut utiliser deux zones d'accès public distinctes, une pour offrir des services Web publics aux utilisateurs externes de la zone publique qui ne sont pas des employés du ministère, et une pour héberger des services d'accès à distance pour les utilisateurs externes qui sont des employés du ministère (c.-à-d. des utilisateurs d'accès à distance).

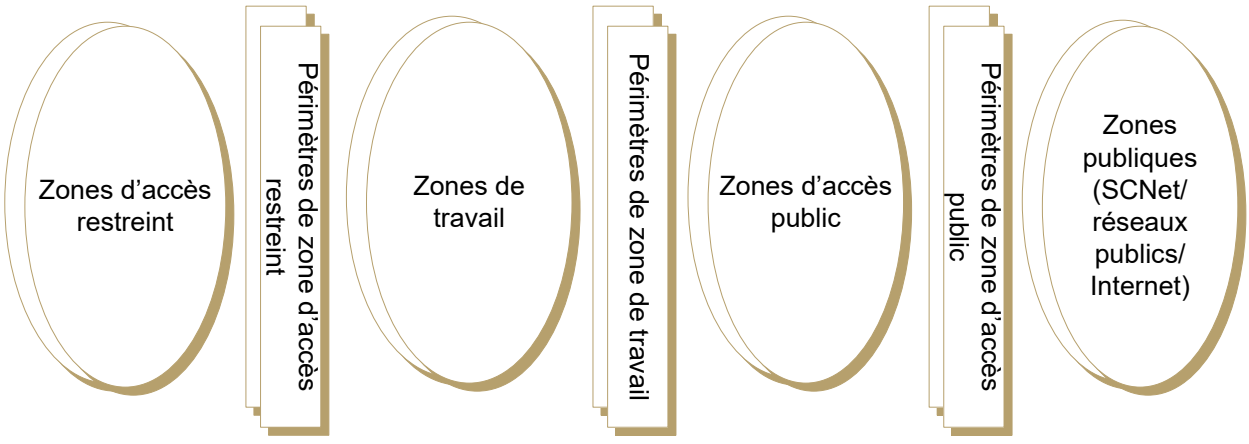

Figure 2 – Zones du réseau ministériel

2.1.1 Zones publiques

Les zones publiques sont des réseaux de communications non ministériels qui ne sont pas exploités par le ministère. Ils incluent le réseau *Réseau de la Voie de communication protégée* (**SCNetE**) et tout autre réseau public tel Internet. Les ministères ont normalement une interface directe avec le SCNet, qui utilise la dorsale axée sur la *commutation multiprotocole par étiquette* (**MPLS**) pour les interconnexions et offre une voie d'accès à Internet.

2.1.2 Zones d'accès public

Les attaquants qui tentent de compromettre l'hôte d'un réseau ministériel (p. ex. un serveur) ont plus de chance de réussir lorsque l'hôte est connecté directement au protocole *Transmission Control Protocol/Internet Protocol* (**TCP/IP**) plutôt que par l'intermédiaire d'un mandataire. Puisque le ministère ne contrôle pas les zones publiques, il n'est donc pas souhaitable de permettre une connectivité TCP/IP directe entre les zones publiques et les hôtes qui offrent les services d'information ministériels. Ainsi, les zones d'accès public illustrées dans la Figure 2 hébergent principalement des services de serveur mandataire et de relais qui permettent de négocier l'accès entre les services d'information du réseau ministériel accessibles de l'extérieur et les zones publiques. Les services d'information offerts dans les zones d'accès public peuvent inclure les services de serveur mandataire de courrier électronique, les services de serveur mandataire de sortie, les services de serveur mandataire d'entrée, les services d'annuaire externes, les services de *noms de domaine* (**DNS**) externes et les services d'accès à distance.

2.1.3 Zones de travail

Les zones de travail illustrées dans la Figure 2 hébergent principalement les services d'information auxquels accèdent les utilisateurs internes situés à l'intérieur des frontières de sécurité physique du ministère. Elles hébergent également les services d'information auxquels accèdent les utilisateurs externes situés à l'extérieur des frontières de sécurité physique du ministère dans les zones publiques. Ces services d'information accessibles de l'extérieur sont négociés par les services de serveur mandataire et de relais des zones d'accès public. Les services d'information offerts dans les zones de travail peuvent inclure les services de portail et Web, les services de bureautique, les services de courrier, les services DNS internes, les services de partage de fichiers, les services d'impression, etc. L'information d'utilisateur est traitée dans les zones de travail, mais n'y est pas conservée. Ces zones servent normalement au traitement des données plutôt qu'à leur stockage; les utilisateurs internes sont placés dans leur propre zone de travail. Les communications entre la zone de travail qui héberge les utilisateurs internes et celle qui héberge les services d'utilisateur sont contrôlées par un périmètre d'utilisateur interne.

2.1.4 Zones d'accès restreint

Les zones d'accès restreint illustrées dans la Figure 2 incluent les services de gestion de l'information nécessaires à la tenue à jour des données traitées par les services d'information dans les zones de travail et les zones d'accès elles-mêmes. Ces données peuvent être hébergées en recourant à des technologies de stockage d'entreprise telles les technologies de *stockage en réseau* (**NAS**) ou de *réseau de stockage* (**SAN**) et sont accessibles aux serveurs de bases de données, aux serveurs de courrier ou aux serveurs de fichiers. Ces zones incluent également les services réseau et de sécurité nécessaires au maintien des opérations et de la sécurité du réseau ministériel. Les différents services de base hébergés dans les zones d'accès restreint, décrits plus en détail ci-dessous, sont illustrés dans la Figure *3 – Services du réseau ministériel* :

1) Service de gestion de l'information : Ce service est responsable du stockage, de la protection et de l'archivage de l'information créée, traitée et stockée dans le réseau ministériel. L'information peut inclure l'information d'utilisateur (p. ex. fichiers, courriels, etc.) ou l'information système (p. ex. fichiers de configuration, fichiers de sauvegarde, images système, enregistrements de vérification, etc.);

2) Service de sauvegarde et de reprise : Ce service effectue les sauvegardes de l'information d'utilisateur (p. ex. fichiers, courriels, etc.) et de l'information système (p. ex. fichiers de configuration, fichiers de sauvegarde, images système, enregistrements de vérification, etc.) dans le réseau ministériel. Cette information est conservée et mise à la disposition des opérations de reprise (le cas échéant);

3) Service de réseautage (protocole **DHCP** (Dynamic Host Configuration Protocol), services de noms de domaine (**DNS**), horloge, routage, commutation, surveillance) : Ce service inclut les commutateurs, les routeurs, les coupe-feu et les serveurs de surveillance réseau nécessaires à l'établissement et au maintien de l'architecture en zones du réseau ministériel. Il inclut également les serveurs *DHCP* utilisés pour l'attribution des paramètres du protocole **IP** aux réseaux hôtes, les serveurs DNS utilisés pour les résolutions nom-adresse IP et les serveurs de temps réseau utilisés pour fournir des temps de référence aux réseaux hôtes aux fins de synchronisation des horloges système;

4) Service d'authentification et d'autorisation : Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les utilisateurs internes, les administrateurs internes et, éventuellement, les utilisateurs externes et appliquées dans la fonction de contrôle d'accès des services du réseau ministériel auxquels ils ont accès. Le service d'authentification et d'autorisation inclut un serveur **RADIUS** (*Remote Authentification Dial In User Service*) qui permet de prendre en charge les protocoles nécessaires pour assurer l'interface entre la fonction de contrôle d'accès et de connexion des services RADIUS du réseau ministériel et le service d'authentification et d'autorisation;

5) Service de vérification : Ce service inclut un dépôt central servant à la réception et au stockage des enregistrements de vérification produits par les services du réseau ministériel. Il analyse également les enregistrements contenus dans le dépôt et produit des rapports sur les événements d'intérêt et informe les individus, au besoin;

6) *Service de détection des intrusions* (**SDI**) : Ce service permet l'analyse en temps quasi réel du contenu non chiffré des communications des utilisateurs internes et externes et de l'administrateur interne afin de déceler tout comportement non autorisé;

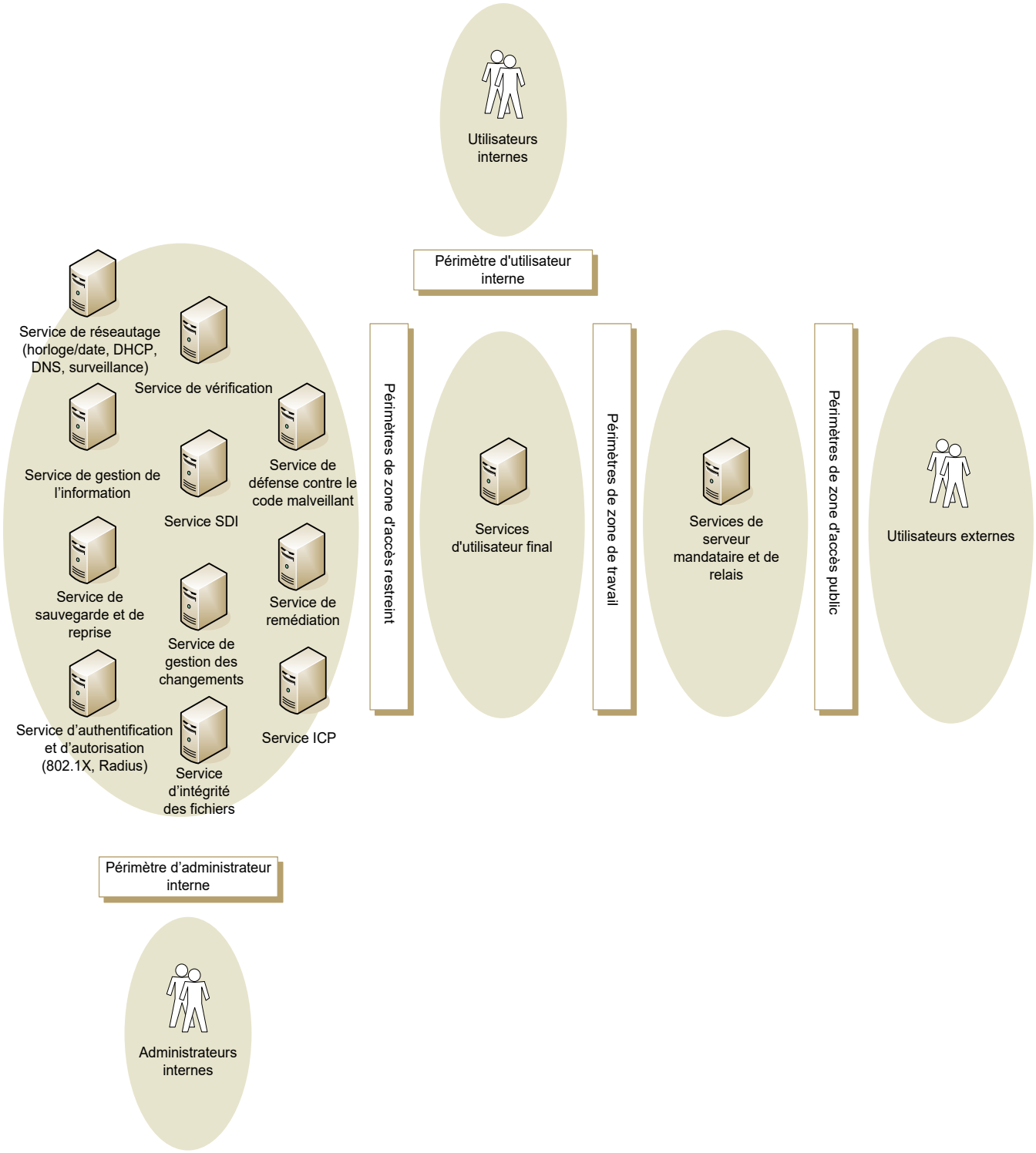

Figure 3 – Services du réseau ministériel

7) *Service de gestion des changements* (**SGC**) : Ce service permet de vérifier périodiquement les configurations de composant et de comparer ces configurations aux configurations approuvées dans le but de détecter tout changement non autorisé. Il permet également l'approvisionnement en configurations des services du réseau ministériel. Le service peut signaler tout changement non autorisé à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification;

8) *Service d'intégrité des fichiers* (**SIF**) : Ce service permet de détecter les modifications non autorisées apportées aux fichiers dans les services du réseau ministériel qui hébergent un agent SIF. Il peut signaler tout changement non autorisé à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification;

9) Service de défense contre le code malveillant (**SDCM**) : La configuration des services du réseau ministériel inclut des agents de défense contre le code malveillant qui relèvent des politiques, définies dans le SDCM, selon lesquelles on doit inspecter les données pour détecter tout code malveillant et prendre des mesures appropriées. Le SDCM centralise la gestion des mécanismes de protection contre le code malveillant mis en place dans les services du réseau ministériel. Il permet de mettre automatiquement à jour les composants de son logiciel de soutien ou les définitions des signatures;

10) Service de remédiation : Le service de remédiation automatise la collecte, l'analyse et l'approvisionnement de ses propres rustines logicielles de services de réseau ministériel;

11) Service d'*infrastructure à clé publique* (**ICP**) : Ce service permet la création, la révocation ou la récupération des clés cryptographiques, des identifiants et des certificats numériques utilisés au cours des opérations de chiffrement/déchiffrement de l'information ou d'authentification cryptographique.

2.1.5 Zones de gestion à accès restreint

Les administrateurs internes occupent leur propre zone de gestion à accès restreint. Les communications entre eux et les services des autres zones du réseau ministériel sont contrôlées par un périmètre d'administrateur interne ainsi que par tout autre périmètre franchi entre l'administrateur interne et le service concerné. Par exemple, un administrateur interne qui doit accéder à un service dans la zone d'accès public devra franchir le périmètre d'administrateur interne, les zones d'accès restreint et les périmètres de zone de travail. Les services du réseau ministériel doivent être mis en place en utilisant deux interfaces distinctes afin de séparer les communications de gestion utilisées pour l'administration ou la maintenance (p. ex. surveillance, journalisation, sauvegardes, mises à jour logicielles, etc.) des autres communications qui servent à appuyer les activités opérationnelles sollicitées par les utilisateurs.

2.2 Conception de haut niveau de référence des services WLAN

La conception de haut niveau de référence pour le scénario d'utilisation opérationnelle de point d'accès sans fil du gouvernement est illustrée dans la Figure *4 — Point d'accès sans fil du gouvernement*. Dans cette illustration, les dispositifs mobiles désignent des portables, des assistants numériques, etc. appartenant aux utilisateurs sans fil invités et configurés avec une interface réseau 802.11. Le ministère n'est aucunement responsable de la sécurité de ces dispositifs ou de l'information non classifiée qu'ils créent, consultent, traitent ou stockent.

2.2.1 Composants

Les composants suivants sont ajoutés au réseau ministériel pour soutenir l'offre de services sans fil aux utilisateurs sans fil invités :

1) Points d'accès : Points d'accès légers ou lourds déployés dans le but d'établir un secteur de service étendu pour les dispositifs mobiles. Les points d'accès lourds sont connectés à un commutateur de LAN câblé et gérés individuellement à partir des postes de travail d'administrateur de composants sans fil situés dans la zone de l'administrateur interne. Les points d'accès légers sont tous connectés à un commutateur sans fil et gérés centralement par l'entremise d'un commutateur ou d'une passerelle des postes de travail d'administrateur de composants sans fil situés dans la zone de l'administrateur interne;
2) Commutateur sans fil/câblé : Les points d'accès légers déployés sont connectés à un commutateur sans fil. Les points d'accès lourds utilisés sont connectés à un commutateur câblé;
3) Passerelle d'authentification : L'utilisateur sans fil invité s'authentifie auprès de la passerelle d'authentification avec un compte temporaire. Une fois que l'utilisateur invité a réussi à s'authentifier, la passerelle d'authentification autorise les communications entre le dispositif mobile de l'utilisateur sans fil invité et les réseaux SCNet/Internet;
4) Périmètre d'utilisateur sans fil invité : Ce périmètre permet de contrôler les communications entrantes et sortantes de la zone d'utilisateur sans fil invité;
5) Capteurs : Les capteurs du *Système de détection d'intrusions sans fil* (**SDISF**) peuvent être des capteurs spécialisés lorsque le SDISF est utilisé en mode recouvrement, ou des capteurs intégrés aux points d'accès lorsque le SDISF est utilisé en mode intégré;
6) Service SDISF : Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), permet l'analyse en temps quasi réel des événements dans la zone de l'utilisateur sans fil interne, vérifie si des composants sans fil non autorisés sont présents et surveille les attaques par déni de service.

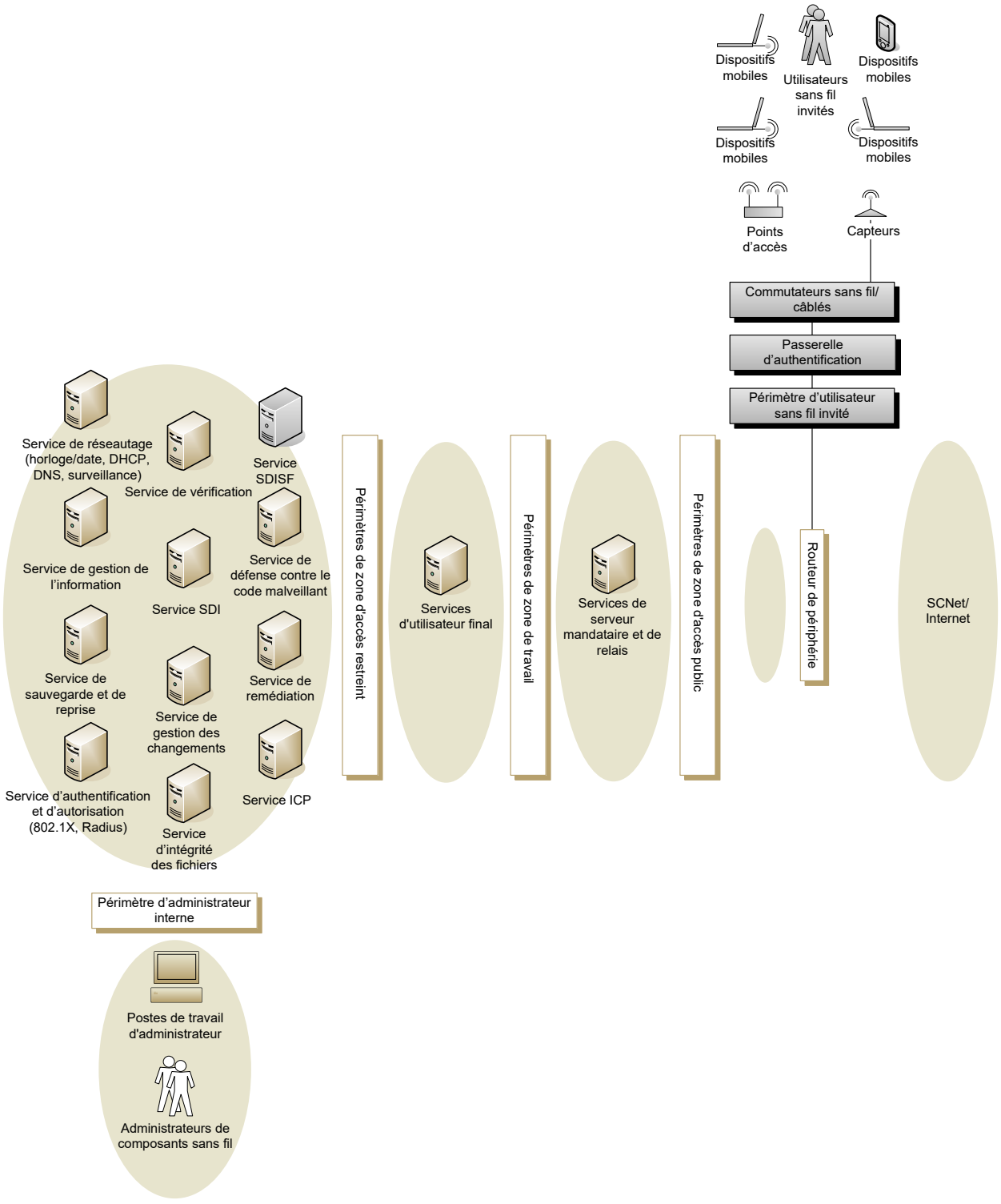

Figure 4 – Point d'accès sans fil du gouvernement

2.2.2 Communications

Les différentes catégories de communications du scénario d'utilisation opérationnelle des points d'accès sans fil du gouvernement sont illustrées dans la Figure *5 – Types de communications des points d'accès sans fil du gouvernement* (**Figure 5**) et incluent :

1) Les communications (étiquetées « 1 » dans la Figure 5) entre les composants sans fil et les services de base du réseau ministériel, abordées à la *Section 2.2.1 Composants*;
2) Les communications d'administrateur de composants sans fil (étiquetées « 2 » dans la Figure 5) utilisées pour administrer les composants sans fil entre les postes de travail d'administrateur et les composants sans fil;
3) Les communications d'utilisateur sans fil invité (étiquetées « 3 » dans la Figure 5) entre les postes de travail d'utilisateur sans fil invité et les réseaux SCNet/Internet.

Les dispositifs mobiles d'utilisateur sans fil invité occupent leur propre sous-zone à l'extérieur de la zone d'accès public du réseau ministériel. Cette sous-zone est désignée « zone d'utilisateur sans fil invité » et inclut son propre réseau routable. Une sous-zone permet de contrôler les communications entre la « zone d'utilisateur sans fil invité » et le réseau ministériel ou les réseaux SCNet/Internet. Ce contrôle est exercé au niveau du périmètre d'utilisateur sans fil invité.

Des contrôles de communication supplémentaires peuvent être appliqués dans le routeur de périphérie pour autant que l'on attribue à l'utilisateur sans fil invité sa propre interface réseau matérielle ou logique spécialisée dans le routeur de périphérie. Ces contrôles peuvent servir à restreindre les communications de la zone d'utilisateur sans fil invité avec les réseaux SCNet/Internet et à contrôler la largeur de bande appropriée (disponible pour le routeur de périphérie) attribuée à ces communications.

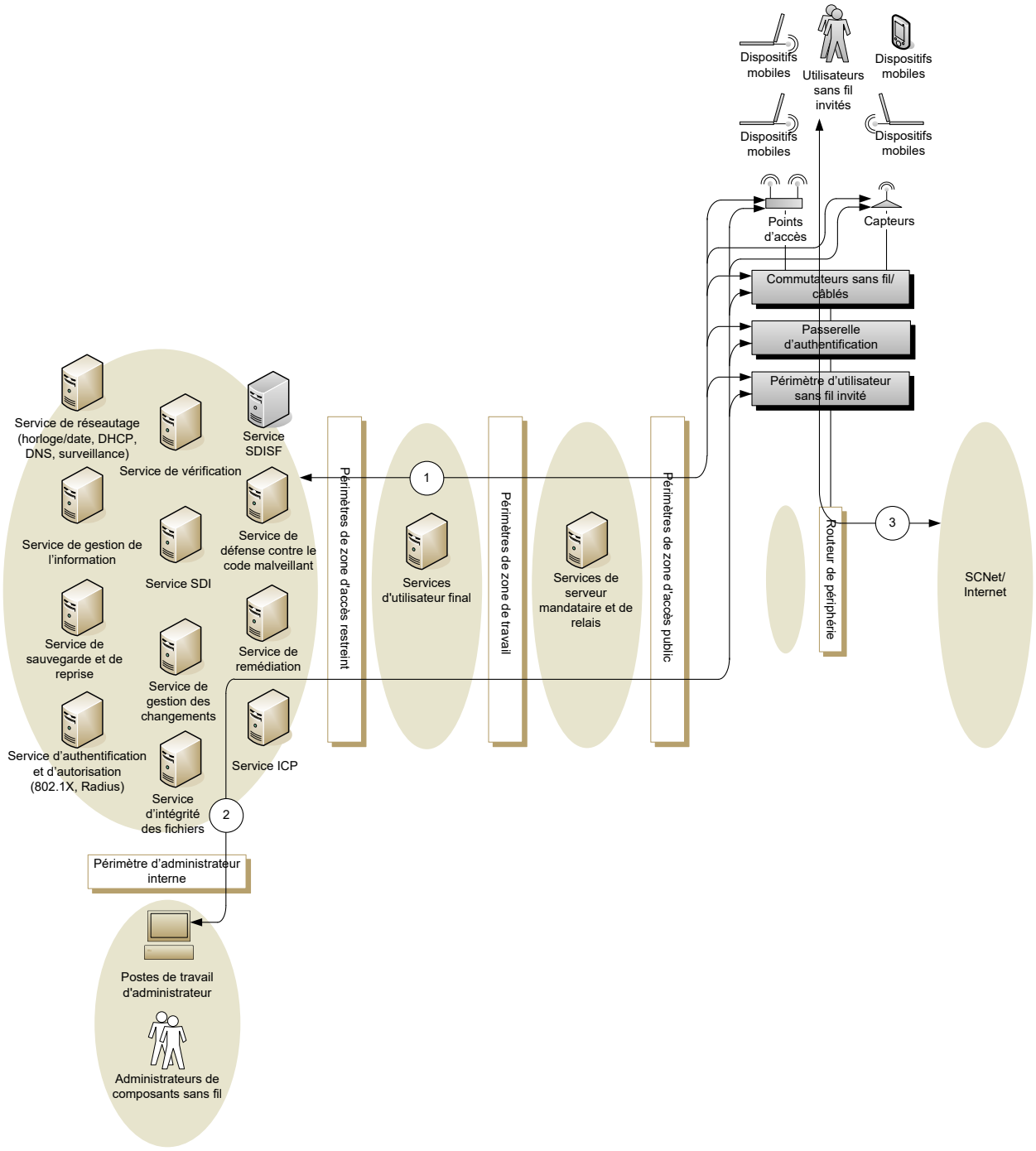

Figure 5 – Types de communications des points d'accès sans fil du gouvernement

2.2.3 Concept d'opération

Les utilisateurs sans fil invités n'ont accès à aucun des services d'utilisateur (services de bureautique, services de courrier électronique, services Web, etc.) dans le réseau ministériel. On leur accorde seulement une connectivité de réseau entre leurs dispositifs mobiles et les réseaux SCNet/Internet pour autant qu'ils se soient d'abord authentifiés à un point d'accès et qu'ils ont ensuite réussi à se connecter à la passerelle d'authentification avec un compte temporaire d'utilisateur invité. La passerelle d'authentification bloque toutes les communications de dispositif mobile des utilisateurs sans fil invités qui n'ont pas réussi à exécuter le processus de connexion. Une fois qu'ils ont réussi à se connecter et que leurs communications peuvent franchir la passerelle d'authentification, le périmètre d'utilisateur sans fil invité permet uniquement aux dispositifs mobiles de communiquer par les réseaux SCNet/Internet. Le périmètre contrôle également les communications entre les services de base du réseau ministériel et les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité. Les communications qui franchissent le périmètre sont contrôlées en tenant compte des ports TCP/IP et des adresses IP source et de destination. L'authentification des utilisateurs sans fil invités est effectuée seulement au niveau de l'utilisateur. L'authentification du dispositif mobile lui-même n'est pas requise puisque le ministère ne s'intéresse ni au type ni à la configuration des dispositifs mobiles utilisés.

Les comptes temporaires attribués aux utilisateurs sans fil invités peuvent être créés et gérés dans une base de données de comptes locale de la passerelle d'authentification ou dans le service d'authentification et d'autorisation. Dans ce dernier cas, la passerelle d'authentification doit être en mesure de transmettre les demandes d'authentification (produites par les connexions d'utilisateur sans fil invité) au service d'authentification et d'autorisation.

Les comptes d'administrateur de composants sans fil sont nécessaires à l'administration des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Ces comptes sont créés et tenus à jour dans le service d'authentification et d'autorisation. Puisque les utilisateurs sans fil invités ne peuvent accéder à aucun service d'utilisateur (service de courrier, services Web, services de bureautique, etc.), les exigences de sécurité en matière de contrôle d'accès des utilisateurs s'appliquent uniquement aux administrateurs de composants sans fil qui doivent administrer les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité.

Les utilisateurs sans fil invités sont responsables de la sécurité de leurs dispositifs mobiles sans fil ainsi que de l'information non classifiée qu'ils créent, consultent, traitent ou stockent et qui n'appartient pas au ministère. Lorsque les utilisateurs sans fil invités accèdent aux services sans fil, le système affiche un message d'information concernant les exigences en matière de responsabilité et d'utilisation acceptable qui leur incombent. Le scénario d'utilisation opérationnelle ne s'applique pas à la création, à l'accès, au traitement ou au stockage d'information protégée ou classifiée.

Des messages d'information sur l'utilisation du système sont affichés à l'intention des administrateurs de composants sans fil lors de la connexion aux composants sans fil. La notification d'utilisation système est affichée dans l'écran de connexion de l'utilisateur sans fil invité (p. ex. la page Web); elle est produite par la passerelle d'authentification, affichée sur le dispositif mobile et acceptée par l'utilisateur sans fil invité.

2.2.4 Restriction d'accès

Il est important de s'assurer que les postes de travail d'utilisateur sans fil interne conformes au protocole 802.11 ne puissent se connecter à la zone d'utilisateur sans fil invité, puis aux réseaux SCNet/Internet, puisque les contrôles de sécurité prévus pour ces postes dans le réseau ministériel pourraient être contournés.

Les fonctions 802.1X du protocole 802.11i peuvent être utilisées pour empêcher les postes de travail d'utilisateur interne de s'authentifier auprès des points d'accès de la zone d'utilisateur sans fil invité. Le serveur RADIUS du service d'authentification et d'autorisation et le serveur DHCP du service de réseautage peuvent être configurés avec des adresses **MAC** (*Media Access Control*) pour les postes de travail d'utilisateur interne configurés avec les fonctions 802.11. Les dispositifs mobiles qui s'authentifient auprès du point d'accès (lorsque des points d'accès lourds sont utilisés) ou du commutateur sans fil (lorsque des points d'accès légers sont utilisés) sont configurés de manière à utiliser une authentification ouverte. Toutefois, les demandes d'authentification sont transmises au serveur RADIUS avec le protocole 802.1X afin de vérifier que l'adresse MAC du dispositif mobile n'est pas une des adresses MAC du poste de travail d'utilisateur interne. Si le serveur RADIUS repère une adresse MAC de poste de travail d'utilisateur interne, il n'indique pas que l'authentification du poste de travail a réussi et le poste ne sera pas en mesure de communiquer au-delà des points d'accès de la zone d'utilisateur sans fil invité.

Les points d'accès ou le commutateur sans fil transmettent les demandes DHCP des dispositifs mobiles au serveur DHCP. Ce dernier est configuré de manière à attribuer une adresse IP incluse dans la gamme d'adresses assignée à la zone d'utilisateur sans fil invité pourvu :

1) Que la transmission provienne des points d'accès ou du commutateur sans fil dans la zone d'utilisateur sans fil invité;

2) Que l'adresse MAC du dispositif mobile n'est pas une des adresses MAC assignées aux postes de travail d'utilisateur interne.

L'adresse IP attribuée à la zone d'utilisateur sans fil invité doit appartenir à la gamme d'adresses spécialement assignée à la zone et ne doit chevaucher aucune des autres adresses IP assignées dans le réseau ministériel. Si ces adresses IP sont des adresses privées, le périmètre d'utilisateur sans fil invité doit les traduire en une ou plusieurs adresses IP publiques routables dans les réseaux SCNet ou Internet.

Bien que les communications d'utilisateur sans fil invité ne soient pas classifiées, on doit utiliser la fonction de chiffrement/déchiffrement **AES** (*Advanced Encryption Standard*) du protocole 802.11i si l'on détermine que la confidentialité des communications en question doit être maintenue.

2.2.5 Surveillance

Les capteurs SDISF surveillent les supports sans fil 802.11 et retransmettent l'information obtenue au service SDISF du LAN câblé aux fins de traitement. La seule fonction du SDISF est de surveiller les supports sans fil pour détecter toute attaque en provenance de la zone d'utilisateur sans fil invité qui cible le réseau ministériel ou les autres organisations; le contenu d'information des communications d'utilisateur sans fil invité elles-mêmes n'est pas surveillé.

Lorsque des points d'accès légers sont utilisés et que le commutateur sans fil qui les contrôle applique les fonctions du SDISF, ces fonctions peuvent être partagées par les communications

du poste de traitement et la surveillance de la zone de couverture des radiofréquences. Si le commutateur n'applique pas les fonctions du SDISF, on doit utiliser un serveur SDISF distinct et des capteurs spécialisés. Un serveur SDISF distinct et des capteurs spécialisés sont également nécessaires pour appliquer les fonctions du SDISF à tout déploiement de WLAN de point d'accès lourd.

2.3 Points de mise en œuvre des éléments de contrôle techniques

Cette section aborde dans un premier temps la conception de haut niveau de référence d'un réseau ministériel type. Cette conception de haut niveau est ensuite complétée par les services WLAN du scénario d'utilisation opérationnelle de point d'accès sans fil du gouvernement. Des recommandations sur l'endroit où les éléments de contrôle techniques peuvent être appliqués dans la conception de haut niveau de référence sont également incluses. Le processus qui permet de déterminer les éléments de contrôle techniques d'un ensemble approuvé de contrôles de sécurité est décrit à l'Annexe 4 (illustré dans la Figure *6 – Contrôles de sécurité et éléments de contrôle*).

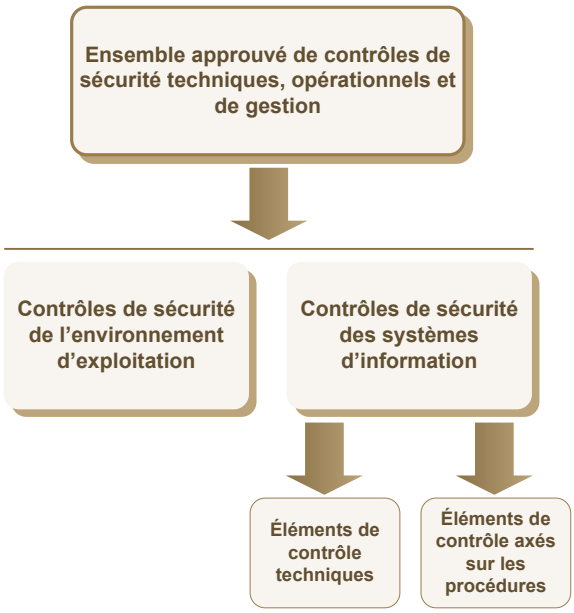

Figure 6 – Contrôles de sécurité et éléments de contrôle

2.3.1 Résumés des éléments de contrôle techniques

Cette section est une introduction aux recommandations présentées dans le Tableau 1.

AC-2 Gestion des comptes

La gestion des comptes s'applique aux comptes d'administrateur de composants sans fil nécessaires à l'administration des composants sans fil (c.-à-d. les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité) ainsi qu'aux comptes d'utilisateur sans fil invité nécessaires à l'utilisation des services sans fil.

Les comptes d'administrateur de composants sans fil sont requis pour les opérations de connexion et d'administration liées aux capteurs sans fil, aux points d'accès, aux commutateurs, à la passerelle d'authentification et aux composants de périmètre d'utilisateur sans fil invité. Le compte d'utilisateur sans fil invité est un compte temporaire qui sert uniquement à s'authentifier auprès de la passerelle d'authentification. Lorsqu'un dispositif mobile d'utilisateur sans fil invité tente de communiquer avec les réseaux SCNet/Internet, le système affiche à l'intention de l'utilisateur un écran de connexion (p. ex. une page Web) si la passerelle d'authentification détermine que ce dernier n'a pas déjà effectué d'authentification pour le dispositif en question. Une fois que l'utilisateur réussit le processus de connexion, la passerelle d'authentification autorise les communications en provenance des dispositifs mobiles d'utilisateur sans fil invité vers les réseaux SCNet/Internet. L'authentification est effectuée seulement au niveau de l'utilisateur. L'authentification du dispositif mobile lui-même n'est ni requise, ni effectuée puisque le ministère ne se préoccupe ni du type, ni de la configuration des dispositifs mobiles utilisés.

Les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité doivent inclure une fonction de contrôle d'accès administrative qui permet de s'assurer que l'on accorde l'accès uniquement aux administrateurs de composants sans fil qui ont réussi le processus de connexion. Chaque composant doit pouvoir consulter une base de données de comptes qui permet de vérifier les justificatifs d'identité des administrateurs de composants sans fil durant l'authentification. Cette base de données peut résider dans le composant ou le composant peut permettre de communiquer avec une base distincte hébergée dans un autre composant tel un serveur d'authentification. Si tous les composants permettent d'utiliser une base de données de comptes distincte, il suffit de tenir à jour un seul compte par administrateur de composants sans fil dans le serveur d'authentification. Sinon, on doit prévoir des comptes différents pour chaque composant.

Les utilisateurs sans fil invités s'authentifient auprès d'un seul composant, soit la passerelle d'authentification. Par conséquent, la tenue à jour des comptes d'utilisateur sans fil invité dans une base de données de comptes distincte (par opposition à l'utilisation d'une base locale résidant dans le serveur d'authentification) n'offre pas les mêmes avantages que la tenue à jour d'un seul compte pour les administrateurs de composants sans fil.

On présume que les comptes d'administrateur de composants sans fil sont tenus à jour dans une base de données de comptes distincte du service d'authentification et d'autorisation du réseau ministériel. On présume également que les comptes d'utilisateur sans fil invité sont soit gérés par le service d'authentification et d'autorisation du réseau ministériel, soit traités localement dans le serveur d'authentification. Selon le concept de droits d'accès minimaux, le dernier scénario peut être préférable lorsque les comptes d'utilisateur sans fil invité sont créés

par un individu situé dans la zone de réception du ministère (p. ex. un commissionnaire) et qui n'a pas besoin d'autres droits dans le réseau ministériel.

AC-3 Application de l'accès

L'application de l'accès est assurée par les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité afin de contrôler les mesures qu'un administrateur de composants sans fil est autorisé à prendre une fois qu'il a été effectivement authentifié. Ce contrôle ne s'applique pas aux utilisateurs sans fil invités puisqu'ils ne se connectent à aucun composant du réseau ministériel à de fins d'intervention. Ils s'authentifient plutôt auprès du serveur d'authentification pour assurer une connectivité de réseau entre leurs dispositifs mobiles et les réseaux SCNet/Internet.

Les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité doivent inclure une fonction de contrôle d'accès administrative pour contrôler les mesures que les administrateurs de composants sans fil peuvent prendre conformément aux politiques de sécurité définies pour chaque composant. Ces politiques peuvent être configurées dans une base de données de politiques locale incluse dans chaque composant, ou le composant peut permettre de communiquer avec une base de données hébergée dans un composant distinct tel un serveur d'autorisation. Si les composants permettent l'utilisation d'une base distincte, toutes les politiques de sécurité peuvent être tenues à jour dans un seul endroit pour l'ensemble des administrateurs. Sinon, il faut configurer des politiques différentes dans chaque composant.

On présume que les politiques qui définissent les mesures que les administrateurs de composants sans fil sont autorisés à prendre sont tenues à jour dans une base de données de politiques distincte du service d'authentification et d'autorisation du réseau ministériel et que ces politiques sont appliquées dans les composants sans fil.

AC-4 Application des contrôles du flux d'information

Le périmètre d'utilisateur sans fil invité est configuré avec des politiques qui définissent les communications entrantes et sortantes (en fonction du port TCP/IP, de l'adresse IP source et de destination, etc.) autorisées dans la zone d'utilisateur sans fil invité. Seules les communications autorisées peuvent franchir le périmètre d'utilisateur sans fil invité. Toutes les communications non autorisées sont bloquées. Les communications qui sont autorisées à franchir le périmètre d'utilisateur sans fil invité peuvent être de type composant-service, administrateur-composant, ou invité-SCNet/Internet.

Les communications composant-service comprennent les communications auxquelles ne participe pas l'utilisateur. Exemple : points d'accès qui communiquent avec un serveur d'authentification dans le service d'authentification et d'autorisation ministériel. Des communications administrateur-composant ont lieu lorsqu'un administrateur de composants sans fil se connecte à un composant sans fil à des fins administratives. Les communications invité-SCNet/Internet comprennent les communications entre les dispositifs mobiles et les réseaux SCNet/Internet. Le ministère ne surveille ni ne se préoccupe du contenu d'information réel des communications invité-SCNet/Internet.

AC-5 Séparation des tâches

La séparation des tâches est liée aux différents niveaux d'accès et est assurée par la configuration des politiques de sécurité relatives à l'application de l'accès de manière à refléter les différents groupes ou niveaux de privilèges. Chaque groupe ou niveau s'appuie sur un rôle distinct que doit jouer un administrateur de composants sans fil à l'égard des composants sans fil. On attribue à l'administrateur de composants sans fil uniquement les groupes ou niveaux de privilèges pour les rôles dont il est responsable. De plus, les groupes ou niveaux de privilèges sont définis de manière à empêcher tout administrateur individuel de composants sans fil d'obtenir le nombre de privilèges requis qui lui permettrait d'effectuer des activités frauduleuses sans collusion.

La séparation des tâches et les niveaux d'accès distincts ne s'appliquent pas aux utilisateurs sans fil invités puisqu'ils ne peuvent se connecter aux composants du réseau ministériel ni prendre de mesures à leur égard.

AC-6 Droit d'accès minimal

Le droit d'accès minimal est accordé en configurant les politiques de sécurité relatives à l'application de l'accès du service d'authentification et d'autorisation de manière à attribuer à chaque administrateur interne uniquement les groupes ou les niveaux de droit d'accès pour les rôles dont il est responsable.

AC-7 Tentatives d'ouverture de session infructueuses

Le verrouillage de compte est configuré dans le service d'authentification et d'autorisation et appliqué aux composants sans fil pour aider à prévenir tout accès non autorisé à des fins administratives en tentant de deviner le mot de passe. On présume que le préjudice causé sera minime advenant la divulgation non autorisée du nom et du mot de passe d'un utilisateur sans fil invité. Par conséquent, le verrouillage n'est pas appliqué dans la passerelle d'authentification pour ces utilisateurs.

AC-8 Notification d'utilisation système

Des messages d'information sur l'utilisation du système sont affichés à l'intention des administrateurs de composants sans fil lors de la connexion aux composants sans fil. Une notification d'utilisation système est affichée dans l'écran de connexion de l'utilisateur sans fil invité (p. ex. page Web); elle est produite par la passerelle d'authentification, affichée sur le dispositif mobile et acceptée par l'utilisateur sans fil invité.

AC-9 Notification d'ouverture de session précédente (accès)

Cette notification est configurée dans le service d'authentification et d'autorisation et appliquée aux composants sans fil pour aider à détecter tout accès non autorisé à des fins administratives en utilisant les justificatifs d'identité d'un compte valable d'administrateur de composants sans fil. On présume que le préjudice causé au ministère sera minime advenant une utilisation non autorisée des justificatifs d'identité d'utilisateur sans fil invité. Par conséquent, cette notification n'est pas appliquée dans la passerelle d'authentification pour ces utilisateurs.

AC-10 Contrôle de sessions simultanées

Les sessions d'utilisateur sans fil invité requièrent une seule session et sont limitées à ce nombre par la passerelle d'authentification. Le nombre limite de sessions simultanées est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et est contrôlé et appliqué par les composants sans fil.

AC-11 Verrouillage de session

On présume que le préjudice causé au ministère sera minime advenant l'utilisation non autorisée d'une session d'utilisateur sans fil invité. Par conséquent, le verrouillage n'est pas appliqué dans la passerelle d'authentification pour ces utilisateurs. Le verrouillage de session est configuré dans le service d'authentification et d'autorisation et appliqué aux composants sans fil aux fins d'accès par l'administrateur de composants sans fil.

AC-18 Accès sans fil

L'accès d'utilisateur sans fil invité est structuré et sécurisé conformément aux directives du présent document.

AU-3 Contenu des enregistrements de vérification

Le contenu d'information des enregistrements de vérification produits par les composants sans fil est lié à leur capacité de vérification.

AU-4 Capacité de stockage des vérifications

Le volume de stockage nécessaire à la tenue à jour des enregistrements de vérification des composants du réseau ministériel peut être important. Normalement, la capacité de stockage du serveur central de journalisation inclus dans le service de vérification de réseau ministériel n'est pas suffisante pour contenir les enregistrements de vérification; on présume donc que le serveur utilise la capacité de stockage offerte par le service de gestion de l'information.

Si un composant sans fil n'est pas en mesure de transmettre ses enregistrements de vérification au serveur central de journalisation, on doit donc prévoir une capacité de stockage suffisante dans le composant lui-même.

AU-5 Intervention en cas d'échecs de vérification

La fonction de vérification exige de chaque composant sans fil qu'il produise des enregistrements de vérification et réussisse à les transmettre au serveur central de journalisation. Tout échec du processus de vérification est dû soit à l'incapacité d'un composant sans fil de produire ou de stocker les nouveaux enregistrements de vérification ou de les transmettre au serveur central de journalisation, soit à l'incapacité de ce dernier de stocker les enregistrements reçus. Cette défaillance entraîne une perte d'information de vérification. Le ministère doit définir une politique sur les mesures à prendre dans une telle situation. L'arrêt du système d'information est la mesure la plus draconienne que l'on puisse prendre puisqu'elle affecte la disponibilité; toutefois, dans certains cas, elle peut s'imposer lorsqu'une perte d'information de vérification est jugée intolérable.

AU-6 Examen, analyse et rapports de vérification

Les enregistrements de vérification sont inutiles, sauf si l'information qu'ils contiennent peut être analysée de manière efficace pour détecter l'occurrence d'événements d'intérêt. De plus, l'analyse doit être holistique et inclure collectivement les enregistrements de plusieurs composants. Le service de vérification permet de traiter automatiquement les enregistrements de composants multiples selon des critères d'événement sélectionnables.

AU-7 Réduction des vérifications et génération de rapports

Le volume d'enregistrements de vérification peut être important (jusqu'à représenter le volume le plus important de données du réseau ministériel); la fonction de production de rapports doit donc être en mesure de regrouper l'information contenue dans les enregistrements individuels et, ainsi, de réduire la quantité de données ou le nombre d'enregistrements à conserver en permanence ou sur une longue période.

AU-8 Estampilles temporelles

Pour permettre à l'analyse des enregistrements de vérification de détecter les événements d'intérêt, on a besoin d'une méthode de synchronisation des enregistrements des nombreux composants. La méthode utilisée consiste à inclure dans chaque composant sans fil une estampille temporelle qui indique l'heure et la date exactes de création de chaque enregistrement et à faire en sorte que les composants sans fil synchronisent leur horloge système les uns avec les autres. Il est possible d'automatiser cette opération si chaque composant sans fil permet de mettre à jour son horloge système en communiquant avec un serveur de temps prévu dans le service réseau et en utilisant un protocole tel Network Time Protocol.

AU-9 Protection de l'information de vérification

Les enregistrements de vérification peuvent contenir de l'information qui doit être protégée sur le plan de la confidentialité (accès non autorisé), de l'intégrité (modification) ou de la disponibilité (suppression). La protection des enregistrements doit être prise en charge par les composants sans fil ainsi que par le service de vérification.

AU-12 Génération d'enregistrements de vérification

Les composants sans fil doivent assurer la vérification des événements, tels que définis dans le contrôle AU-2, et la génération des enregistrements de vérification appropriés qui peuvent être transmis au serveur central de journalisation aux fins d'analyse et de production de rapports.

AU-14 Vérification des sessions

Le réseau ministériel n'est pas tenu de surveiller et de saisir les communications d'utilisateur sans fil invité. La vérification des sessions peut s'appliquer aux sessions d'administrateur de composants sans fil si l'on est justifié de croire que des mesures administratives inappropriées ont été prises. Dans ce cas, le service SDI peut être utilisé pour accéder au contenu non chiffré des communications d'administrateur de composants sans fil et en journaliser ou saisir le contenu pour le service de vérification.

CM-5 Restrictions d'accès associées aux changements

L'application de l'accès est assurée par les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité pour contrôler les mesures que l'administrateur de composants sans fil est autorisé à prendre une fois qu'il a été effectivement authentifié. Cette exigence ne s'applique pas aux utilisateurs sans fil invités puisqu'ils ne se connectent à aucun composant du réseau ministériel à de fins d'intervention. Chaque composant sans fil doit être en mesure de vérifier l'application des restrictions d'accès et de produire les enregistrements de vérification concernés qui sont transmis au serveur central de journalisation.

CM-6 Paramètres de configuration

Chaque composant sans fil doit être configuré de manière à fonctionner suivant un mode qui offre uniquement la fonction requise. Toute autre fonction ou tout autre service doit être désactivé.

L'application de l'accès est assurée par les capteurs sans fil, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité pour contrôler les droits d'accès ou de modification que possède un administrateur de composants sans fil relativement à la configuration du composant sans fil. Toute modification de la configuration d'un composant sans fil doit être effectuée avec le SGC et signalée au service de vérification. Le service d'intégrité des fichiers peut servir à détecter les changements non autorisés apportés à la configuration du composant sans fil.

CM-7 Fonctionnalité minimale

Chaque composant sans fil doit être configuré de manière à offrir uniquement la fonction requise. Toute autre fonction ou tout autre service doit être désactivé.

CM-8 Inventaire des composants de système d'information

Le SGC conserve l'information sur la configuration autorisée des composants sans fil et vérifie périodiquement les composants pour s'assurer que leur configuration d'exploitation correspond à la configuration autorisée. Le service SDISF peut servir à surveiller toute connexion de composants et/ou de dispositifs non autorisés à la zone d'utilisateur sans fil invité.

CP-9 Sauvegarde du système d'information

Le volume de stockage nécessaire au maintien des sauvegardes de l'information système et d'utilisateur du réseau ministériel peut être important. Le service de sauvegarde et de reprise utilise donc l'espace de stockage offert par le service de gestion de l'information pour conserver ces sauvegardes.

Le service de sauvegarde et de reprise accède périodiquement aux composants sans fil en utilisant des privilèges d'administrateur pour créer des sauvegardes de leur information système.

CP-10 Reprise et reconstitution du système d'information

Le service de sauvegarde et de reprise accède, à de fins de reprise, aux sauvegardes de l'information système gérées par le service de gestion de l'information. L'information système

des composants sans fil permet de ramener un composant sans fil à un état connu après une défaillance ou une compromission.

IA-2 Identification et authentification (utilisateurs organisationnels)

La méthode d'authentification utilisée pour les administrateurs de composants sans fil est liée au niveau de protection requis et peut inclure les mots de passe/NIP, l'authentification multifactorielle, les mots de passe à usage unique, l'authentification axée sur les certificats ou les authentifiants de groupe.

IA-4 Gestion des identificateurs

L'utilisation de la gestion dynamique des identificateurs, des attributs et des autorisations d'accès connexes ne s'applique pas au scénario d'utilisation opérationnelle.

IA-5 Gestion des authentifiants

Les comptes d'utilisateur sans fil invité utilisent les mots de passe/NIP pour s'authentifier auprès du serveur d'authentification. La méthode d'authentification utilisée pour les administrateurs de composants sans fil est liée au niveau de protection requis et peut inclure les mots de passe/NIP, l'authentification multifactorielle, les mots de passe à usage unique, l'authentification axée sur les certificats ou les authentifiants de groupe. Si un mot de passe/NIP est utilisé pour les administrateurs de composants sans fil, il doit être conforme aux exigences de complexité des mots de passe. Si la méthode d'authentification utilisée pour les administrateurs de composants sans fil est axée sur les certificats et que ces derniers sont délivrés par le service d'ICP du réseau ministériel, le processus d'authentification :

1) Valide les certificats en établissant une voie de certification vers une autorité de certification fiable;
2) Remet à l'utilisateur le contrôle de la clé privée correspondante;
3) Associe l'identité authentifiée au compte de l'utilisateur.

IA-6 Rétroaction d'authentification

Le mécanisme d'authentification des composants sans fil occulte l'information sur la rétroaction d'authentification durant les connexions d'administrateur de composants sans fil.

On présume que le préjudice causé au ministère sera minime advenant une divulgation non autorisée des justificatifs d'identité d'authentification d'un utilisateur sans fil invité. Il n'est donc pas nécessaire d'occulter la rétroaction de l'information d'authentifiant dans la passerelle d'authentification pour les utilisateurs sans fil invités.

IA-7 Authentification des modules cryptographiques

Les comptes d'utilisateur sans fil invité utilisent des mots de passe/NIP pour s'authentifier auprès du serveur d'authentification. Si un module cryptographique est intégré à la méthode d'authentification utilisée pour les administrateurs de composants sans fil, il doit satisfaire aux exigences pertinentes des directives du GC en matière d'authentification auprès d'un module cryptographique.

IA-8 Identification et authentification (utilisateurs non organisationnels)

Les comptes d'utilisateur sans fil invité utilisent les mots de passe/NIP pour s'authentifier auprès du serveur d'authentification.

SC-2 Partitionnement des applications

Les administrateurs de composants sans fil se connectent aux capteurs sans fil, aux points d'accès, aux commutateurs, à la passerelle d'authentification et aux composants de périmètre d'utilisateur sans fil invité et en assurent l'administration. L'utilisateur sans fil invité s'authentifie auprès de la passerelle d'authentification pour communiquer avec les réseaux SCNet/Internet. Les fonctionnalités de l'administrateur de composants sans fil et de l'utilisateur sans fil invité sont distinctes à la fois sur le plan de leurs capacités et de leur méthode d'accès.

SC-3 Isolement des fonctions de sécurité

La fonctionnalité à laquelle les utilisateurs sans fil invités ont accès (c.-à-d. l'accès aux réseaux SCNet/Internet après une connexion réussie à la passerelle d'authentification) est séparée de la fonctionnalité de sécurité (utilisée par les administrateurs de composants sans fil) des composants sans fil.

SC-5 Protection contre les dénis de service

Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), surveille les attaques par déni de service émanant de la zone d'utilisateur sans fil interne contre le réseau ministériel ou d'autres réseaux.

SC-6 Priorité des ressources

Le routeur de périphérie du réseau ministériel est configuré de manière à limiter la largeur de bande disponible pour les communications des utilisateurs sans fil invités afin que ces communications n'aient aucune incidence négative sur la largeur de bande des communications entre le réseau ministériel et les réseaux SCNet/Internet.

SC-7 Protection des frontières

Le périmètre d'utilisateur sans fil invité est configuré à partir de politiques qui définissent (en fonction du port TCP/IP, de l'adresse IP source et de destination, etc.) les communications qui sont autorisées à entrer et sortir de la zone d'utilisateur sans fil invité.

SC-10 Déconnexion réseau

Le périmètre d'utilisateur sans fil invité peut être configuré de manière à interrompre les connexions réseau après une période d'inactivité spécifique.

SC-11 Chemin de confiance

Les administrateurs de composants sans fil accèdent aux composants depuis leurs postes de travail situés dans la sous-zone de gestion mise en place par le service réseau. Les politiques sur les flux d'information appliquées dans la zone d'accès restreint, la zone de travail et le périmètre d'utilisateur sans fil invité veillent à ce que l'administration des composants sans fil ne puisse s'effectuer qu'à partir des postes de cette sous-zone. Cela fait en sorte d'assurer la

fiabilité du chemin entre les administrateurs de composants sans fil et les composants eux-mêmes. Le chemin de communication fiable ne s'applique pas aux utilisateurs sans fil invités.

L'authentification et les autorisations relatives aux fonctions de sécurité sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction de contrôle d'accès et de connexion des composants sans fil.

SC-12 Établissement et gestion des clés cryptographiques

La gestion des clés cryptographiques utilisées par les administrateurs de composants sans fil (là où l'authentification axée sur l'ICP est utilisée) est assurée par le service d'ICP du réseau ministériel. Cette gestion n'est pas requise pour les utilisateurs sans fil invités.

SC-13 Utilisation de la cryptographie

Les mécanismes cryptographiques utilisés par les administrateurs de composants sans fil (là où l'authentification axée sur l'ICP est utilisée) sont assurés par le service d'ICP du réseau ministériel. Ces mécanismes ne sont pas requis pour les utilisateurs sans fil invités.

SC-24 Défaillance dans un état connu

La défaillance des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité s'effectue à un état connu pour tous les types de défaillance définis par le ministère.

SC-29 Hétérogénéité

La sélection des diverses technologies de l'information assure l'hétérogénéité des composants sans fil. (Nota : Cette approche peut être difficile dans le cas où les composants sont sélectionnés auprès d'un fournisseur unique à des fins d'intégration).

SC-32 Partitionnement des systèmes d'information

Le service réseau effectue le partitionnement du réseau ministériel en différentes zones et les composants qui résident dans chaque zone sont assujettis aux politiques de sécurité de la zone qui les concerne. Ces zones incluent la zone d'accès restreint, la zone de travail, la zone d'accès public, la sous-zone de gestion et la zone d'utilisateur sans fil invité.

SC-34 Programmes exécutables non modifiables

Les composants sans fil chargent et exécutent leur système d'exploitation et leurs applications à partir de supports matériels non inscriptibles.

SI-2 Correction des défauts

Le service de remédiation effectue automatiquement la collecte, l'analyse et l'approvisionnement du matériel et des mises à jour logicielles des composants sans fil qui lui sont compatibles.

SI-4 Surveillance des systèmes d'information

Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), détecte les attaques et indique toute utilisation non autorisée du système dans la zone d'utilisateur sans fil invité.

SI-6 Vérification de la fonctionnalité de sécurité

Les composants sans fil vérifient au démarrage, ou périodiquement après le démarrage, le bon fonctionnement de leurs propres fonctions de sécurité essentielles.

SI-7 Intégrité de l'information et des logiciels

Le SGC accède périodiquement aux composants sans fil avec les privilèges d'administrateur de composants sans fil pour obtenir la configuration d'exploitation actuelle et la comparer à la copie archivée de la configuration approuvée dans le but de détecter tout changement non autorisé.

SI-11 Traitement des erreurs

Les composants sans fil doivent assurer la vérification des événements, incluant les conditions d'erreur et le stockage des enregistrements de vérification dans le composant lui-même. Idéalement, les composants sans fil doivent également assurer la transmission des enregistrements de vérification dans un serveur central de journalisation afin de permettre la gestion et l'analyse collectives des enregistrements de tous les composants.

On présume que les composants sans fil peuvent transmettre leurs enregistrements de vérification dans le serveur central de journalisation du service de vérification de réseau ministériel.

2.3.2 Recommandations concernant les points de mise en œuvre

Cette section inclut un tableau de recommandations concernant l'endroit où les éléments de contrôle techniques peuvent être appliqués dans la conception de haut niveau de référence. On doit tenir compte uniquement des éléments de contrôle indiqués dans l'ensemble approuvé de contrôles de sécurité pour chaque scénario d'utilisation opérationnelle et non pas de tous les éléments indiqués dans le Tableau 1.

Le Tableau 1 recommande des points de mise en œuvre pour les éléments de contrôle techniques des scénarios d'utilisation opérationnelle de point d'accès sans fil du gouvernement. Il indique également les éléments de contrôle qui peuvent être mis en œuvre comme élément *système* (**S**), *commun* (**C**) ou *hybride* (**H**). Un élément système est traité soit individuellement par les composants ajoutés au réseau ministériel en vue du déploiement des services sans fil, soit comme une combinaison des composants et des mesures de protection et contremesures qui existent dans le réseau ministériel avant le déploiement des services sans fil. Un élément commun est appliqué en utilisant une ou plusieurs des mesures de protection et contremesures qui existent dans le réseau ministériel avant le déploiement des services sans fil et qui ne requièrent aucune modification. Un élément hybride est appliqué en utilisant une ou plusieurs des mesures de protection et contremesures qui existent dans le réseau ministériel avant le déploiement des services sans fil et qui doivent être modifiées.

Tableau 1 – Points de mise en œuvre des points d'accès sans fil du gouvernement

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-2 Gestion des comptes	AC-2-1 L'organisation fait appel à des mécanismes automatisés pour appuyer la gestion des comptes du système d'information.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation ou passerelle d'authentification. **Description :** Les mécanismes automatisés sont appliqués au service d'authentification et d'autorisation pour gérer les comptes d'utilisateur sans fil invité et les comptes d'administrateur de composants sans fil. Si l'authentification des utilisateurs sans fil invités est effectuée avec une base de données de comptes locale, les mécanismes sont appliqués à la passerelle d'authentification pour les comptes d'utilisateur sans fil invité. L'application des mécanismes automatisés au service d'authentification et d'autorisation constitue une exigence de sécurité commune de système d'information. Toute autre application constitue une exigence de sécurité système propre au système d'information.	C/S
AC-2 Gestion des comptes	AC-2-2 Le système d'information supprime automatiquement les comptes temporaires et d'urgence après [Affectation : délai défini par l'organisation pour chaque type de compte].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation ou passerelle d'authentification. **Description :** Les mécanismes automatisés sont appliqués au service d'authentification et d'autorisation pour supprimer les comptes temporaires et d'urgence créés pour les utilisateurs sans fil invités et les administrateurs de composants sans fil. Si l'authentification des utilisateurs sans fil invités est effectuée avec une base de données de comptes locale, les mécanismes sont appliqués à la passerelle d'authentification pour les comptes d'utilisateur sans fil invité. L'application des mécanismes automatisés au service d'authentification et d'autorisation constitue une exigence de sécurité commune de système d'information. Toute autre application constitue une exigence de sécurité système propre au système d'information.	C/S
AC-2 Gestion des comptes	AC-2-3 Le système d'information désactive automatiquement les comptes inactifs après [Affectation : délai défini par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation ou passerelle d'authentification**.** **Description :** Les mécanismes automatisés sont appliqués au service d'authentification et d'autorisation pour désactiver les comptes inactifs d'utilisateur sans fil invité et les comptes d'administrateur de composants sans fil après [Affectation : période définie par l'organisation]. Si l'authentification des utilisateurs sans fil invités est effectuée avec une base de données de comptes locale, les mécanismes sont appliqués à la passerelle d'authentification pour les comptes d'utilisateur sans fil invité. L'application des mécanismes automatisés au service d'authentification et d'autorisation constitue une exigence de sécurité commune de système d'information. Toute autre application constitue une exigence de sécurité système propre au système d'information.	C/S
AC-2 Gestion des comptes	AC-2-4 Le système d'information vérifie automatiquement les activités de création, de	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de vérification et passerelle d'authentification.	C/S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	modification, de désactivation et de suppression de compte, et en informe les personnes concernées, le cas échéant.	**Description :** Les mécanismes automatisés sont appliqués au service d'authentification et d'autorisation pour signaler au service de vérification les activités de gestion des comptes des utilisateurs sans fil invités et des administrateurs de composants sans fil. Au besoin, le service de vérification informe les individus concernés. Si l'authentification des utilisateurs sans fil invités est effectuée avec une base de données de comptes locale, une vérification automatisée des activités de gestion des comptes d'utilisateur sans fil invité est effectuée par la passerelle d'authentification et signalée au service de vérification. L'application des mécanismes automatisés au service d'authentification et d'autorisation constitue une exigence de sécurité commune de système d'information. Toute autre application constitue une exigence de sécurité système propre au système d'information.	
AC-2 Gestion des comptes	AC-2-5 L'organisation : (a) exige des utilisateurs qu'ils ferment leur session après [Affectation : délai d'inactivité prévu ou description du moment de la fermeture de session défini par l'organisation]; (b) détermine la période du jour et la durée d'utilisation normales pour les comptes du système d'information; (c) surveille toute utilisation irrégulière des comptes du système d'information; (d) signale toute utilisation irrégulière aux responsables désignés de l'organisation.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation et service de vérification. **Description :** Les mécanismes automatisés sont appliqués au service d'authentification et d'autorisation pour signaler au service de vérification l'heure et la durée de toute utilisation atypique des comptes d'administrateur de composants sans fil. Au besoin, le service de vérification informe les individus concernés de l'utilisation atypique. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	C
AC-2 Gestion des comptes	AC-2-6 Le système d'information gère de manière dynamique les droits d'accès utilisateur et les autorisations d'accès connexes.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service d'authentification et d'autorisation gère de manière dynamique les droits et autorisations d'accès des administrateurs de composants sans fil. Ces droits et autorisations sont appliqués à la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S
AC-2 Gestion des comptes	AC-2-7 L'organisation : (a) établit et administre les comptes utilisateur privilégiés	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	conformément à un plan de contrôle d'accès basé sur les rôles qui regroupe les droits d'accès au réseau et au système d'information dans des rôles; (b) suit et surveille les attributions de rôles privilégiés.	**Description :** Les comptes d'administrateur de composants sans fil sont classés dans le service d'authentification et d'autorisation selon des rôles axés sur les droits. Ces droits sont appliqués à la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	
AC-3 Application de l'accès	AC-3-A Le système d'information applique les autorisations approuvées pour l'accès logique au système conformément à la politique pertinente.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S
AC-3 Application de l'accès	AC-3-2 Le système d'information applique une double autorisation basée sur les politiques et procédures organisationnelles concernant [Affectation : commandes privilégiées définies par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Des autorisations doubles pour les [Affectation : commandes privilégiées définies par l'organisation] sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités à qui on attribue seulement une connectivité aux réseaux SCNet/Internet et qui n'exécutent aucune commande privilégiée.	S
AC-3 Application de l'accès	AC-3-3 Le système d'information applique [Affectation : politiques de contrôle d'accès non discrétionnaire définies par l'organisation] aux [Affectation : ensembles d'utilisateurs et de ressources définis par l'organisation] lorsque l'ensemble de règles de chaque politique précise : (a) l'information sur le contrôle d'accès (c.-à-d. les	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les [Affectation : politiques de contrôle d'accès non discrétionnaires définies par l'organisation] concernant [Affectation : ensemble d'utilisateurs et de ressources défini par l'organisation] sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	attributs) qu'il utilise (p. ex. poste, nationalité, âge, projet, période du jour); (b) les relations obligatoires entre les éléments d'information sur le contrôle d'accès pour autoriser l'accès.	de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	
AC-3 Application de l'accès	AC-3-4 Le système d'information applique une politique de contrôle d'accès discrétionnaire (DAC pour Discretionary Access Control) qui : (a) permet aux utilisateurs de préciser et de contrôler le partage de l'information soit avec des individus ou des groupes d'individus identifiés, ou les deux; (b) limite la propagation des droits d'accès; (c) inclut ou exclut l'accès à la granularité d'un seul utilisateur.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de gestion de l'information, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les politiques de contrôle d'accès discrétionnaires sont configurées dans le service d'authentification et d'autorisation et appliquées dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Elles sont configurées de manière à (**a**) permettre aux utilisateurs de préciser et de contrôler le partage d'information avec des individus ou des groupes d'individus particuliers, ou les deux, (**b**) à limiter la propagation des droits d'accès et (**c**) à inclure ou exclure l'accès à la granularité d'un seul utilisateur. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S
AC-3 Application de l'accès	AC-3-5 Le système d'information empêche l'accès à [Affectation : information pertinente en matière de sécurité définie par l'organisation] sauf lorsqu'il est en état de non-fonctionnement sécurisé.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'accès à [Affectation : information sur la sécurité définie par l'organisation] est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqué dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S
AC-3 Application de l'accès	AC-3-6 L'organisation chiffre ou conserve hors ligne dans un endroit sécurisé [Affectation : information sur l'utilisateur ou le système définie par l'organisation].	**Point(s) de mise en œuvre :** Service de gestion de l'information **Description :** Le service de gestion de l'information protège l'information précisée dans [Affectation : information système et/ou d'utilisateur définie par l'organisation] en recourant au chiffrement.	C

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-4 Application des contrôles du flux d'information	AC-4-A Le système d'information applique des autorisations approuvées pour contrôler le flux de l'information dans le système et entre les systèmes interconnectés conformément à la politique pertinente.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet.	S
AC-4 Application des contrôles du flux d'information	AC-4-1 Le système d'information applique le contrôle de flux d'information en utilisant des attributs de sécurité explicites, sur l'information et les objets source et de destination, comme base pour les décisions concernant le contrôle de flux.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Les communications sont contrôlées en tenant compte des ports TCP/IP et des adresses IP source et de destination.	S
AC-4 Application des contrôles du flux d'information	AC-4-2 Le système d'information applique le contrôle de flux d'information à l'aide de domaines de traitement protégés (p. ex. application de type domaine) comme base pour les décisions concernant le contrôle de flux.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Le scénario d'utilisation opérationnelle ne requiert pas l'application du type de domaine du contrôle de flux d'information.	S
AC-4 Application des contrôles du flux d'information	AC-4-3 Le système d'information applique le contrôle dynamique de flux d'information en s'appuyant sur une politique qui permet ou interdit les flux d'information en fonction de conditions changeantes ou de motifs opérationnels.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. L'application des politiques de contrôle dynamique du flux d'information, qui permettent ou interdisent les flux d'information selon les conditions changeantes ou les considérations opérationnelles, est assurée par le périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-4 Application des contrôles du flux d'information	AC-4-4 Le système d'information empêche les données chiffrées de contourner les mécanismes de vérification de contenu.	**Point(s) de mise en œuvre :** S.O. **Description :** Le périmètre d'utilisateur sans fil invité ne contrôle pas les communications des dispositifs mobiles en fonction du contenu d'information des communications, qui peut être chiffré.	-
AC-4 Application des contrôles du flux d'information	AC-4-5 Le système d'information applique [Affectation : restrictions définies par l'organisation concernant l'intégration de types de données dans d'autres types de données].	**Point(s) de mise en œuvre :** S.O. **Description :** Le périmètre d'utilisateur sans fil invité ne contrôle pas les communications des dispositifs mobiles en fonction du contenu d'information des communications.	-
AC-4 Application des contrôles du flux d'information	AC-4-6 Le système d'information applique le contrôle de flux d'information aux métadonnées.	**Point(s) de mise en œuvre :** S.O. **Description :** Le périmètre d'utilisateur sans fil invité ne contrôle pas les communications des dispositifs mobiles en fonction du contenu d'information des communications.	-
AC-4 Application des contrôles du flux d'information	AC-4-7 Le système d'information applique [Affectation : flux unidirectionnels définis par l'organisation] en utilisant des mécanismes matériels.	**Point(s) de mise en œuvre :** S.O. **Description :** L'application de flux unidirectionnels basés sur des mécanismes matériels est normalement exigée pour le transfert d'information entre des systèmes d'information dont les niveaux de sécurité sont différents; cette exigence ne s'applique pas au scénario d'utilisation opérationnelle.	-
AC-4 Application des contrôles du flux d'information	AC-4-8 Le système d'information applique le contrôle de flux d'information en utilisant [Affectation : filtres de la politique de sécurité définis par l'organisation] comme base pour les décisions concernant le contrôle de flux.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Le périmètre d'utilisateur sans fil invité utilise des [Affectation : filtres de la politique de sécurité définis par l'organisation] comme base pour les décisions concernant le contrôle de flux.	S
AC-4 Application des contrôles du flux d'information	AC-4-9 Le système d'information impose une vérification manuelle de [Affectation : filtres de la politique de sécurité définis par l'organisation] lorsqu'il n'est pas en mesure de prendre de	**Point(s) de mise en œuvre :** S.O. **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. La vérification manuelle des	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	décision en matière de contrôle de flux d'information.	[Affectation : filtres de la politique de sécurité définis par l'organisation] n'est pas une exigence applicable au scénario d'utilisation opérationnelle.	
AC-4 Application des contrôles du flux d'information	AC-4-10 Le système d'information permet à un administrateur privilégié d'activer ou de désactiver [Affectation : filtres de la politique de sécurité définis par l'organisation].	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Le contrôle du flux d'information utilise [Affectation : filtres de la politique de sécurité définis par l'organisation] comme base pour les décisions concernant le contrôle de flux. Ces filtres peuvent être configurés, activés ou désactivés par un administrateur de composants sans fil.	S
AC-4 Application des contrôles du flux d'information	AC-4-11 Le système d'information permet à un administrateur privilégié de configurer [Affectation : filtres de la politique de sécurité définis par l'organisation] pour appuyer les différentes politiques de sécurité.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entre les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et les services du réseau ministériel (p. ex. service d'authentification et d'autorisation, service de vérification, etc.). Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Le contrôle du flux d'information utilise [Affectation : filtres de la politique de sécurité définis par l'organisation] comme base pour les décisions concernant le contrôle de flux. Ces filtres peuvent être configurés, activés ou désactivés par un administrateur de composants sans fil.	S
AC-4 Application des contrôles du flux d'information	AC-4-12 Le système d'information, lors du transfert d'information entre différents domaines de sécurité, identifie les flux d'information selon la spécification du type de données et l'utilisation des données.	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne contrôle pas les communications de dispositif mobile de l'utilisateur sans fil invité vers les réseaux SCNet/Internet en se basant sur le contenu d'information des communications.	-
AC-4 Application des contrôles du flux d'information	AC-4-13 Le système d'information, lors du transfert d'information entre différents domaines de sécurité, décompose l'information en sous-composantes pertinentes pour la présenter aux mécanismes d'application de la politique.	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne contrôle pas les communications de dispositif mobile de l'utilisateur sans fil invité vers les réseaux SCNet/Internet en se basant sur le contenu d'information des communications.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-4 Application des contrôles du flux d'information	AC-4-14 Le système d'information, lors du transfert d'information entre différents domaines de sécurité, applique les filtres de la politique qui limitent la structure et le contenu des données selon [Affectation : exigences de la politique de sécurité de l'information définies par l'organisation].	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne contrôle pas les communications de dispositif mobile de l'utilisateur sans fil invité vers les réseaux SCNet/Internet en se basant sur le contenu d'information des communications.	-
AC-4 Application des contrôles du flux d'information	AC-4-15 Le système d'information, lors du transfert d'information entre différents domaines de sécurité, détecte l'information non autorisée et en interdit le transfert, conformément à la politique de sécurité.	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne contrôle pas les communications de dispositif mobile de l'utilisateur sans fil invité vers les réseaux SCNet/Internet en se basant sur le contenu d'information des communications.	-
AC-4 Application des contrôles du flux d'information	AC-4-17 Le système d'information : (a) identifie de façon unique et authentifie les domaines source et destination pour le transfert de l'information; (b) lie les attributs de sécurité à l'information pour faciliter l'application de la politique sur le flux d'information; (c) suit les problèmes associés à la liaison des attributs de sécurité et au transfert de l'information.	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne contrôle pas les communications de dispositif mobile de l'utilisateur sans fil invité vers les réseaux SCNet/Internet en se basant sur le contenu d'information des communications.	-
AC-5 Séparation des tâches	AC-5-C L'organisation met en œuvre la séparation des tâches en attribuant des autorisations d'accès aux systèmes d'information.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction administrative de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-6 Droit d'accès minimal	AC-6-4 Le système d'information fournit des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès utilisateur.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité héberge les postes de travail des utilisateurs dans son propre sous-réseau (c.-à-d. le domaine de traitement) et limite les communications de leur dispositif mobile aux seuls réseaux SCNet/Internet.	S
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-A Le système d'information applique une limite de [Affectation : nombre défini par l'organisation] tentatives d'ouverture de session invalides consécutives par l'utilisateur sur une période de [Affectation : durée définie par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La limite de [Affectation : nombre défini par l'organisation] tentatives consécutives d'accès non réussies par un utilisateur au cours d'une période de [Affectation : période définie par l'organisation] est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquée dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-B Le système d'information [Sélection : verrouille le compte ou le nœud pendant (Affectation : durée définie par l'organisation); verrouille le compte ou le nœud jusqu'à ce qu'un administrateur le libère; reporte l'invite d'ouverture de session suivante selon (Affectation : algorithme de temporisation défini par l'organisation)] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé. Le contrôle s'applique à une tentative d'ouverture de session effectuée tant à l'aide d'une connexion locale que d'une connexion réseau.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le verrouillage de compte est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqué dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-1 Le système d'information verrouille automatiquement le compte ou le nœud jusqu'à ce qu'il soit libéré par un administrateur lorsque le nombre maximal de tentatives infructueuses est dépassé.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le verrouillage de compte est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqué dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Seul un administrateur peut libérer les comptes verrouillés. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
AC-7 Tentatives d'ouverture de session infructueuses	AC-7-2 Le système d'information fournit une protection supplémentaire pour les accès aux dispositifs mobiles au moyen d'une ouverture de session en éliminant l'information du dispositif après [Affectation : nombre défini par l'organisation] tentatives infructueuses d'ouverture de session sur le dispositif.	**Point(s) de mise en œuvre :** S.O. **Description :** Le ministère n'est pas responsable de la configuration et de la sécurité des dispositifs mobiles des utilisateurs sans fil invités, ni de la protection de l'information transmise, traitée ou stockée.	-
AC-8 Notification d'utilisation système	AC-8-A Le système d'information, avant d'accorder l'accès, affiche un message ou une bannière de notification d'utilisation approuvée du système, qui comprend des énoncés de confidentialité et de sécurité conformément à la Politique d'utilisation des réseaux électroniques du SCT.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les bannières d'ouverture de session sont configurées dans la passerelle d'authentification et affichées par les utilisateurs sans fil invités. Elles sont également configurées dans les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et affichées par les administrateurs de composants sans fil. La bannière inclut des énoncés de confidentialité et de sécurité conformément à la *Politique d'utilisation des réseaux électroniques du SCT.*	S
AC-8 Notification d'utilisation système	AC-8-B Le système d'information continue d'afficher le message ou la bannière de notification jusqu'à ce que l'utilisateur opte d'ouvrir une session ou d'accéder au système.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les bannières d'ouverture de session sont configurées dans la passerelle d'authentification et affichées par les utilisateurs sans fil invités. Elles sont également configurées dans les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité et affichées par les administrateurs de composants sans fil. Elles continuent de s'afficher jusqu'à la fin du	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		processus de connexion ou jusqu'à ce que les utilisateurs décident d'ouvrir une session ou d'accéder au système d'information.	
AC-8 Notification d'utilisation système	AC-8-C Le système d'information, dans le cas d'un système accessible au public : (a) affiche, le cas échéant, l'information d'utilisation du système avant d'accorder l'accès; (b) affiche, au besoin, des mises en garde concernant la surveillance, l'enregistrement et la vérification conformes aux dispositions sur la protection des renseignements personnels pour de tels systèmes qui interdisent généralement ces activités; et (c) inclut dans le message de notification aux utilisateurs publics du système une description des utilisations autorisées du système.	**Point(s) de mise en œuvre :** S.O. **Description :** La sécurité des systèmes offerts au public par le réseau ministériel ne s'applique pas au scénario d'utilisation opérationnelle.	-
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-A Le système d'information indique à l'utilisateur qui vient d'ouvrir une session la date et l'heure de sa dernière ouverture de session (dernier accès).	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service d'authentification et d'autorisation produit, à l'intention des administrateurs de composants sans fil, une notification de la date et de l'heure de la dernière connexion qui s'affiche durant le processus de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-1 Le système d'information indique à l'utilisateur qui vient d'ouvrir une session la date et l'heure de sa dernière ouverture de session (dernier accès).	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La notification de connexion non réussie est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et s'affiche durant le processus de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-2 Le système d'information indique à l'utilisateur le nombre de [Sélection : ouvertures de session/accès réussis; ouvertures de session/accès infructueux; les deux] pendant [Affectation : durée définie par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La notification de connexion réussie et non réussie des [Sélection : connexions/accès réussis; tentatives de connexion/accès non réussies; les deux] durant la [Affectation : période définie par l'organisation] est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et affichée durant le processus de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
AC-9 Notification d'ouverture de session précédente (accès)	AC-9-3 Le système d'information indique à l'utilisateur de [Affectation : ensemble, défini par l'organisation, des modifications liées à la sécurité apportées au compte de l'utilisateur] pendant [Affectation : durée définie par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les paramètres de compte d'utilisateur sont configurés dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil. La fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité communique aux administrateurs de composants sans fil les [Affectation : ensemble des changements liés à la sécurité apportés au compte de l'utilisateur] durant [Affectation : période définie par l'organisation]. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
AC-10 Contrôle des sessions simultanées	AC-10-A Le système d'information limite le nombre de sessions simultanées pour chaque compte système à [Affectation : nombre défini par l'organisation].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La limite du nombre de sessions simultanées est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et fixée à [Affectation : nombre défini par l'organisation; elle s'affiche durant le processus de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Elle est configurée dans la passerelle d'authentification pour les utilisateurs sans fil invités.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AC-11 Verrouillage de session	AC-11-A Le système d'information empêche tout autre accès au système en verrouillant la session après [Affectation : délai défini par l'organisation] d'inactivité ou à la réception d'une demande d'un utilisateur.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le verrouillage de session est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et s'affiche durant le processus de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence ne s'applique pas aux utilisateurs sans fil invités puisque le ministère n'est pas responsable de sécuriser leurs sessions.	S
AC-11 Verrouillage de session	AC-11-B Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur réinitialise l'accès en exécutant les procédures établies d'identification et d'authentification.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le verrouillage de session est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqué dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Le verrouillage est annulé lorsque le processus de reconnexion est réussi. Cette exigence ne s'applique pas aux utilisateurs sans fil invités puisque le ministère n'est pas responsable de sécuriser leurs sessions.	S
AC-11 Verrouillage de session	AC-11-1 Le mécanisme de verrouillage de session du système d'information, lorsqu'il est activé dans un dispositif doté d'un écran, affiche des motifs visibles qui permettent de masquer ce qui figurait précédemment à l'écran.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le verrouillage de session est configuré dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqué dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Durant le verrouillage, les postes de travail d'administrateur de composants sans fil affichent des motifs visibles qui permettent de masquer ce qui figurait précédemment à l'écran. Cette exigence ne s'applique pas aux utilisateurs sans fil invités puisque le ministère n'est pas responsable de sécuriser leurs sessions.	S
AC-16 Attributs de sécurité	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle. Le ministère n'est pas responsable de la sécurité de l'information non classifiée transmise, traitée ou stockée par les utilisateurs sans fil invités.	-
AC-18 Accès sans fil	AC-18-B L'organisation surveille le système d'information pour	**Point(s) de mise en œuvre :** Service SDISF, points d'accès sans fil et capteurs.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	détecter les accès sans fil non autorisés à ce dernier.	**Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), assure la surveillance et le signalement des composants sans fil non autorisés.	
AC-18 Accès sans fil	AC-18-C L'organisation autorise l'accès sans fil au système d'information avant la connexion.	**Point(s) de mise en œuvre :** Passerelle d'authentification **Description :** On doit d'abord attribuer un compte temporaire aux utilisateurs sans fil invités, qui doivent ensuite réussir à s'authentifier auprès de la passerelle d'authentification avant que leur dispositif mobile soit autorisé à se connecter aux réseaux SCNet/Internet.	S
AC-18 Accès sans fil	AC-18-D L'organisation applique les exigences concernant les connexions sans fil au système d'information.	**Point(s) de mise en œuvre :** Passerelle d'authentification **Description :** On doit d'abord attribuer un compte temporaire aux utilisateurs sans fil invités, qui doivent ensuite réussir à s'authentifier auprès de la passerelle d'authentification avant que leur dispositif mobile soit autorisé à se connecter aux réseaux SCNet/Internet.	S
AC-18 Accès sans fil	AC-18-1 Le système d'information protège l'accès sans fil au moyen de l'authentification et du chiffrement.	**Point(s) de mise en œuvre :** Passerelle d'authentification **Description :** On doit d'abord attribuer un compte temporaire aux utilisateurs sans fil invités, qui doivent ensuite réussir à s'authentifier auprès de la passerelle d'authentification avant que leur dispositif mobile soit autorisé à se connecter aux réseaux SCNet/Internet. L'utilisation du chiffrement n'est pas requise puisque le ministère n'est pas responsable de la sécurité des communications de ces utilisateurs.	S
AC-18 Accès sans fil	AC-18-2 L'organisation surveille le système d'information pour détecter les connexions sans fil non autorisées, y compris le balayage des points d'accès sans fil non autorisés [Affectation : fréquence définie par l'organisation], et prend les mesures appropriées si une telle connexion est découverte.	**Point(s) de mise en œuvre :** Service SDISF, points d'accès sans fil et capteurs. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), assure la surveillance et le signalement des composants sans fil non autorisés, y compris le balayage [Affectation : fréquence définie par l'organisation] des points d'accès sans fil non autorisés.	S
AC-18 Accès sans fil	AC-18-4 L'organisation ne permet pas aux utilisateurs de configurer eux-mêmes les capacités de réseautage sans fil.	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle n'impose aucune restriction aux dispositifs mobiles utilisés par les utilisateurs sans fil invités.	-
AC-18 Accès sans fil	AC-18-5 L'organisation restreint les communications sans fil aux frontières qu'elle contrôle.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		Description : La zone d'utilisateur sans fil invité est délimitée par des frontières contrôlées par l'organisation.	
AC-19 Contrôle d'accès pour les dispositifs mobiles	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle. Le ministère n'est pas responsable de la configuration des dispositifs mobiles ou de leur sécurité.	-
AC-21 Collaboration et échange d'information entre utilisateurs	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle dont le seul but est d'appuyer la connectivité entre le réseau des utilisateurs sans fil invités et les réseaux SCNet/Internet plutôt que d'assurer la sécurité du partage d'information entre les utilisateurs.	-
AU-3 Contenu des enregistrements de vérification	AU-3-A Le système d'information produit des enregistrements de vérification qui contiennent suffisamment d'information pour permettre, au minimum, d'établir le type d'événement qui s'est produit, la date et l'heure de l'événement, l'endroit où il s'est produit, sa source, son résultat (réussite ou échec) et l'identité de tous les utilisateurs ou sujets qui lui sont associés.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre au service de vérification des enregistrements qui contiennent suffisamment d'information sur l'événement pour permettre d'établir ses caractéristiques (son type, moment où il s'est produit (date et heure), endroit où il s'est produit, sa source, son résultat (réussite ou échec) et l'identité de tout utilisateur et/ou sujet qui lui est associé).	S
AU-3 Contenu des enregistrements de vérification	AU-3-1 Le système d'information inclut [Affectation : information supplémentaire et plus détaillée définie par l'organisation] dans les enregistrements de vérification pour les événements répartis par type, emplacement ou sujet.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de configurer [Affectation : information supplémentaire et plus détaillée définie par l'organisation] des événements signalés au service de vérification.	S
AU-3 Contenu des enregistrements de vérification	AU-3-2 L'organisation centralise la gestion du contenu des enregistrements de vérification générés par [Affectation : composants de système définis par l'organisation].	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		service de vérification. Le service tient à jour un dépôt central de tous les enregistrements de vérification.	
AU-4 Capacité de stockage des vérifications	AU-4-A L'organisation attribue la capacité de stockage des enregistrements de vérification et configure les vérifications de manière à réduire la probabilité de dépassement de cette capacité.	**Point(s) de mise en œuvre :** Service de vérification et service de gestion de l'information. **Description :** Le service de vérification dispose de suffisamment de capacité de stockage, gérée par le service de gestion de l'information, pour éviter la perte d'enregistrements.	C
AU-5 Intervention en cas d'échecs de vérification	AU-5-A Le système d'information avertit les responsables désignés de l'organisation dans l'éventualité d'un échec de traitement de vérification.	**Point(s) de mise en œuvre :** Service de vérification **Description :** Le service de vérification avertit les responsables désignés de l'organisation dans l'éventualité d'une défaillance du processus de vérification.	C
AU-5 Intervention en cas d'échecs de vérification	AU-5-B Le système d'information prend les mesures supplémentaires suivantes : [Affectation : mesures à prendre définies par l'organisation (p. ex. arrêt du système, écrasement des enregistrements de vérification les plus anciens, arrêt de la génération des enregistrements de vérification)].	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet d'effectuer [Affectation : mesures à prendre définies par l'organisation (p. ex. arrêt du système, écrasement des enregistrements de vérification les plus anciens, arrêt de la génération des enregistrements de vérification)] dans l'éventualité d'une défaillance du processus de vérification du composant.	S
AU-5 Intervention en cas d'échecs de vérification	AU-5-1 Le système d'information génère un avertissement lorsque le volume de stockage attribué aux enregistrements de vérification atteint [Affectation : pourcentage défini par l'organisation] de sa capacité maximale.	**Point(s) de mise en œuvre :** Service de vérification et service de gestion de l'information. **Description :** Le service de vérification produit un avertissement lorsque le volume de stockage attribué aux enregistrements de vérification dans le service de gestion de l'information atteint [Affectation : pourcentage défini par l'organisation] sa capacité maximale.	C
AU-5 Intervention en cas d'échecs de vérification	AU-5-2 Le système d'information génère une alerte en temps réel lorsque les événements d'échec de vérification suivants se produisent : [Affectation :	**Point(s) de mise en œuvre :** Service de vérification **Description :** Le service de vérification produit une alerte en temps réel lorsque [Affectation : événements d'échec de vérification définis par l'organisation qui nécessitent une alerte en temps réel] des événements d'échec de vérification se produisent.	C

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	événements d'échec de vérification définis par l'organisation qui nécessitent une alerte en temps réel].		
AU-5 Intervention en cas d'échecs de vérification	AU-5-3 Le système d'information applique des seuils de volume de trafic configurables représentant la capacité de vérification du trafic réseau et [Sélection : rejette ou retarde] le trafic au-dessus de ces seuils.	**Point(s) de mise en œuvre :** Service réseau **Description :** Les routeurs du service réseau permettent d'attribuer des seuils de volume de trafic réseau lié à la vérification et [Sélection : rejettent ou retardent] le trafic au-dessus de ces seuils.	C
AU-5 Intervention en cas d'échecs de vérification	AU-5-4 Le système d'information effectue un arrêt système à la suite d'un échec de vérification, sauf lorsqu'il existe une capacité de vérification de secours.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet d'arrêter le composant dans l'éventualité d'un échec de vérification.	S
AU-6 Examen, analyse et rapports de vérification	AU-6-3 L'organisation analyse et met en corrélation les enregistrements de vérification des différents dépôts afin d'acquérir une connaissance de sa situation globale.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au service de vérification. Le service de vérification gère un dépôt central et un centre de gestion de tous les enregistrements de vérification pour être au fait de la situation à l'échelle de l'organisation.	S
AU-6 Examen, analyse et rapports de vérification	AU-6-4 Le système d'information centralise l'examen et l'analyse des enregistrements de vérification provenant de plusieurs composants du système.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au service de vérification. Le service de vérification tient à jour un dépôt central de tous les enregistrements de vérification aux fins d'examen et d'analyse.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AU-6 Examen, analyse et rapports de vérification	AU-6-5 L'organisation intègre l'analyse des enregistrements de vérification à l'analyse de l'information liée au balayage des vulnérabilités, des données de rendement et de l'information sur la surveillance réseau pour accroître sa capacité d'identification les activités inappropriées ou inhabituelles.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au service de vérification. Le service de vérification tient à jour un dépôt central de tous les enregistrements de vérification aux fins d'examen et d'analyse.	S
AU-7 Réduction des vérifications et génération de rapports	AU-7-A Le système d'information offre une capacité de réduction des vérifications et de génération de rapports.	**Point(s) de mise en œuvre :** Service de vérification **Description :** Le service de vérification offre une capacité de réduction des vérifications et de génération de rapports.	C
AU-7 Réduction des vérifications et génération de rapports	AU-7-1 Le système d'information permet de traiter automatiquement les enregistrements de vérification des événements d'intérêt en fonction de critères d'événement sélectionnables.	**Point(s) de mise en œuvre :** Service de vérification **Description :** Le service de vérification offre une fonction qui permet de traiter automatiquement les enregistrements de vérification des événements d'intérêt en fonction de critères d'événement sélectionnables.	C
AU-8 Estampilles temporelles	AU-8-A Le système d'information utilise des horloges de système internes pour générer des estampilles temporelles pour les enregistrements de vérification.	**Point(s) de mise en œuvre :** Service réseau, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de générer des estampilles temporelles pour les enregistrements de vérification transmis au service de vérification. Chaque composant peut également synchroniser son horloge en utilisant la fonction de serveur de temps centralisée du service réseau.	S
AU-8 Estampilles temporelles	AU-8-1 Le système d'information synchronise ses horloges internes [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : source de temps faisant autorité définie par l'organisation].	**Point(s) de mise en œuvre :** Service réseau, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité permettent de synchroniser leurs horloges [Affectation : fréquence définie par l'organisation] en utilisant la fonction de serveur de temps centralisée du service réseau.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
AU-9 Protection de l'information de vérification	AU-9-A Le système d'information protège l'information de vérification et les outils de vérification contre l'accès, la modification et la suppression non autorisés.	**Point(s) de mise en œuvre :** Service de vérification, service d'authentification et d'autorisation. **Description :** Les autorisations d'accès aux données et aux outils de vérification du service de vérification sont configurées dans le service d'authentification et d'autorisation et appliquées par le service de vérification.	C
AU-9 Protection de l'information de vérification	AU-9-1 Le système d'information produit les enregistrements de vérification sur des supports matériels non réinscriptibles.	**Point(s) de mise en œuvre :** Service de vérification **Description :** Le service de vérification offre la capacité de produire des enregistrements de vérification sur des supports matériels non inscriptibles.	C
AU-9 Protection de l'information de vérification	AU-9-2 Le système d'information sauvegarde les enregistrements de vérification [Affectation : fréquence définie par l'organisation] dans un système ou un support différent du système faisant l'objet de la vérification.	**Point(s) de mise en œuvre :** Service de sauvegarde et de reprise **Description :** Le service de sauvegarde et de reprise sauvegarde les enregistrements de vérification [Affectation : fréquence définie par l'organisation] dans un système ou un support distinct de celui qui fait l'objet de la vérification.	C
AU-9 Protection de l'information de vérification	AU-9-3 Le système d'information utilise des mécanismes cryptographiques pour protéger l'intégrité de l'information de vérification et des outils de vérification.	**Point(s) de mise en œuvre :** Service de vérification et service de gestion de l'information. **Description :** Le service de vérification utilise des mécanismes cryptographiques pour protéger l'intégrité des données de vérification stockées et gérées par le service de gestion de l'information.	C
AU-9 Protection de l'information de vérification	AU-9-4 L'organisation autorise l'exécution des commandes privilégiées et l'accès à l'information liée à la sécurité par la méthode d'accès à distance uniquement dans le cas de besoins opérationnels probants et documente le motif de cet accès dans le plan de sécurité du système d'information.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de vérification et service de gestion de l'information. **Description :** Les autorisations d'accès aux données de vérification stockées par le service de vérification dans le service de gestion de l'information, et la fonction de vérification des composants sans fil, sont configurées dans le service d'authentification et d'autorisation pour s'assurer que l'accès à la fonction de gestion de la vérification soit réservé à un sous-ensemble restreint d'utilisateurs privilégiés et (b) pour protéger les enregistrements de vérification contre tout accès extérieur aux comptes privilégiés et contre l'exécution de toute fonction privilégiée.	C
AU-10 Non-répudiation	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle. Le ministère n'est pas responsable de sécuriser	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		l'information transmise, traitée ou stockée par les utilisateurs sans fil invités, incluant la non-répudiation des opérations effectuées.	
AU-12 Génération d'enregistrements de vérification	AU-12-A Le système d'information comprend une capacité de génération d'enregistrements de vérification pour la liste d'événements vérifiables définie au contrôle AU-2 au [Affectation : composants du système d'information définis par l'organisation].	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de produire des enregistrements de vérification et de les transmettre au service de vérification pour les événements définis en AU-2 dans [Affectation : composants de système d'information définis par l'organisation].	S
AU-12 Génération d'enregistrements de vérification	AU-12-B Le système d'information permet au personnel désigné de l'organisation de sélectionner les événements vérifiables qui doivent être vérifiés par composant de système particulier.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité peut être configurée par les administrateurs de composants sans fil pour les événements à vérifier et à transmettre au service de vérification.	S
AU-12 Génération d'enregistrements de vérification	AU-12-C Le système d'information génère des enregistrements de vérification pour la liste des événements vérifiés définie au contrôle AU-2 et dont le contenu est défini au contrôle AU-3.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de produire des enregistrements de vérification et de les transmettre au service de vérification pour les événements définis en AU-2 avec le contenu défini en AU-3.	S
AU-12 Génération d'enregistrements de vérification	AU-12-1 Le système d'information compile les enregistrements de vérification provenant de [Affectation : composants du système d'information définis par l'organisation] en une piste de vérification (logique ou physique) globale qui est corrélée dans le temps, en-dedans de [Affectation : niveau de tolérance défini par l'organisation pour les	**Point(s) de mise en œuvre :** Service de vérification, service réseau, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au service de vérification. Chaque composant synchronise son horloge système en utilisant la fonction de serveur de temps du service réseau pour s'assurer que les enregistrements de vérification sont corrélés dans le temps en dedans de [Affectation : niveau de tolérance	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	relations entre les estampilles temporelles des enregistrements individuels de la piste de vérification].	défini par l'organisation pour les relations entre les estampilles temporelles des enregistrements individuels de la piste de vérification].	
AU-12 Génération d'enregistrements de vérification	AU-12-2 Le système d'information produit une piste de vérification (logique ou physique) globale composée d'enregistrements de vérification dans un format normalisé.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de transmettre des enregistrements de vérification au service de vérification. Les enregistrements de vérification produits par les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité sont en format normalisé ou convertis dans ce format par le service de vérification.	S
AU-14 Vérification des sessions	AU-14-A Le système d'information permet de saisir ou d'enregistrer et de journaliser tout le contenu d'une session utilisateur.	**Point(s) de mise en œuvre :** Service SDI **Description :** Le service SDI peut permettre d'accéder au contenu non chiffré des communications d'administrateur de composants sans fil et de journaliser ou saisir le contenu pour le service de vérification. Le ministère n'est pas tenu de saisir/enregistrer et journaliser tout le contenu relatif à une session d'utilisateur sans fil invité.	C
AU-14 Vérification des sessions	AU-14-B Le système d'information permet de visualiser ou d'écouter à distance et en temps réel tout le contenu d'une session utilisateur établie.	**Point(s) de mise en œuvre :** Service SDI **Description :** Le service SDI peut permettre d'accéder au contenu non chiffré des communications d'administrateur de composants sans fil et de visualiser ou d'écouter en temps réel tout le contenu relatif à une session établie d'utilisateur. Le ministère n'est pas tenu de visualiser ou d'écouter en temps réel tout le contenu relatif à une session établie d'utilisateur sans fil invité	C
AU-14 Vérification des sessions	AU-14-1 Le système d'information lance les vérifications de session au démarrage du système.	**Point(s) de mise en œuvre :** Service SDI **Description :** Le service SDI peut permettre d'accéder au contenu non chiffré des communications d'administrateur de composants sans fil et de journaliser ou saisir le contenu pour le service de vérification. Cette exigence de contrôle de sécurité ne s'applique pas aux communications d'utilisateur sans fil invité. Le service SDI est en mesure de lancer le processus de vérification dès le démarrage du système.	C
CM-5 Restrictions d'accès associées aux changements	CM-5-A L'organisation définit, documente, approuve et applique les restrictions d'accès logique et physique associées aux	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	changements au système d'information.	**Description :** Les autorisations de changements apportés à la configuration des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité par les administrateurs de composants sans fil sont attribuées dans le service d'authentification et d'autorisation et appliquées dans les composants sans fil. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	
CM-5 Restrictions d'accès associées aux changements	CM-5-1 L'organisation utilise des mécanismes automatisés pour appliquer les restrictions d'accès et faciliter la vérification des mesures d'application.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité. La vérification de l'application de ces autorisations est également effectuée par les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	S
CM-5 Restrictions d'accès associées aux changements	CM-5-3 Le système d'information empêche l'installation de [Affectation : programmes logiciels essentiels définis par l'organisation] qui ne sont pas signés à l'aide d'un certificat reconnu et approuvé par l'organisation.	**Point(s) de mise en œuvre :** S.O. **Description :** Le ministère n'est pas responsable de la sécurité ou de la configuration des dispositifs mobiles des utilisateurs sans fil invités.	-
CM-5 Restrictions d'accès associées aux changements	CM-5-6 L'organisation restreint les privilèges de changement des logiciels résidents dans les bibliothèques de logiciels (y compris les programmes privilégiés).	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et permettent de définir les restrictions d'accès logique associées aux changements des logiciels résidents dans les bibliothèques de logiciels (y compris les programmes privilégiés). Les autorisations sont appliquées dans la fonction administrative locale de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Cette exigence de contrôle de sécurité ne s'applique	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		pas aux utilisateurs sans fil invités qui n'ont aucun droit d'accès au réseau ministériel ou qui n'en consultent pas les données.	
CM-5 Restrictions d'accès associées aux changements	CM-5-7 Le système d'information met en œuvre automatiquement [Affectation : mesures de protection et contremesures définies par l'organisation] lorsque les fonctions (ou mécanismes) de sécurité sont modifiées de manière inappropriée.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et permettent de définir les restrictions d'accès logique associées aux changements des logiciels résidents dans les bibliothèques de logiciels (y compris les programmes privilégiés). Les autorisations sont appliquées dans la fonction administrative locale de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Le système d'information met en œuvre automatiquement [Affectation : mesures de protection et contremesures définies par l'organisation] lorsque les fonctions (ou mécanismes) de sécurité sont modifiées de manière inappropriée.	S
CM-6 Paramètres de configuration	CM-6-B L'organisation met en œuvre les paramètres de configuration.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité sont configurés avec des paramètres de configuration obligatoires les plus rigoureux.	S
CM-6 Paramètres de configuration	CM-6-1 L'organisation utilise des mécanismes automatisés pour centraliser la gestion, l'application et la vérification des paramètres de configuration.	**Point(s) de mise en œuvre :** SGC, SIF, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le SGC permet d'acquérir et de vérifier les configurations de composant des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Il est en mesure de vérifier périodiquement ces configurations et de les comparer aux configurations approuvées. Le SIF offre la possibilité de vérifier les paramètres de configuration dans les fichiers des composants dans lesquels on peut installer un agent SIF. Le SGC et le SIF peuvent signaler tout changement non autorisé détecté à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification.	S
CM-6 Paramètres de configuration	CM-6-2 L'organisation utilise des mécanismes automatisés pour intervenir dans les cas où des changements non autorisés sont apportés aux [Affectation :	**Point(s) de mise en œuvre :** SGC, SIF, service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations d'accès aux paramètres de configuration sont configurées dans le service d'autorisation et appliquées dans la fonction de contrôle d'accès des	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	paramètres définis par l'organisation de configuration].	capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. La fonction de contrôle d'accès signale toute tentative d'accès non autorisé au service de vérification. Elle est en mesure de vérifier périodiquement les configurations de composant et de les comparer aux configurations approuvées dans le but de détecter tout changement non autorisé. Le SIF offre la possibilité de détecter les modifications non autorisées aux fichiers des composants dans lesquels on peut installer un agent SIF. Et le SGC et le SIF signalent tout changement non autorisé détecté. Ils peuvent signaler ce type de changement apporté aux [Affectation : paramètres de configuration définis par l'organisation] à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification.	
CM-6 Paramètres de configuration	CM-6-3 L'organisation intègre un mécanisme de détection des changements de configuration non autorisés liés à la sécurité à sa capacité d'intervention en cas d'incident pour s'assurer que de tels événements sont suivis, surveillés, corrigés et conservés à des fins historiques.	**Point(s) de mise en œuvre :** SGC, SIF, service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations d'accès aux paramètres de configuration sont configurées dans le service d'autorisation et appliquées dans la fonction de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. La fonction de contrôle d'accès signale toute tentative d'accès non autorisé au service de vérification. Elle est en mesure de vérifier périodiquement les configurations de composant et de les comparer aux configurations approuvées dans le but de détecter tout changement non autorisé. Le SIF offre la possibilité de détecter les modifications non autorisées aux fichiers des composants dans lesquels on peut installer un agent SIF. Et le SGC et le SIF signalent tout changement non autorisé détecté. Ils peuvent signaler ce type de changement à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification. Les événements peuvent ensuite être acheminés vers le processus d'intervention en cas d'incident du ministère aux fins de suivi, de surveillance, de correction et de disponibilité à des fins historiques.	S
CM-7 Fonctionnalité minimale	CM-7-A L'organisation configure le système d'information de manière à offrir uniquement les capacités jugées essentielles et interdit ou restreint spécifiquement l'utilisation des fonctions, ports, protocoles ou services suivants : [Affectation : liste définie par l'organisation des fonctions, ports, protocoles ou services interdits ou restreints].	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité sont configurés de manière à offrir uniquement les capacités jugées essentielles et interdit ou restreint spécifiquement l'utilisation des fonctions, ports, protocoles ou services suivants : [Affectation : liste définie par l'organisation des fonctions, ports, protocoles ou services interdits ou restreints].	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
CM-7 Fonctionnalité minimale	CM-7-2 L'organisation utilise des mécanismes automatisés pour empêcher l'exécution des programmes conformément à [Sélection (une ou plusieurs) : liste des programmes autorisés; liste des programmes non autorisés; règles d'autorisation des modalités d'utilisation d'un programme].	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle n'inclut aucune configuration de sécurité des dispositifs mobiles.	-
CM-8 Inventaire des composants de système d'information	CM-8-2 L'organisation utilise des mécanismes automatisés pour faciliter la tenue d'un inventaire des composants du système d'information qui soit à jour, complet, exact et facilement accessible.	**Point(s) de mise en œuvre :** SGC **Description :** Le SGC offre la capacité de vérifier les configurations de composant aux fins d'automatisation de l'inventaire.	C
CM-8 Inventaire des composants de système d'information	CM-8-3 L'organisation : (a) utilise des mécanismes automatisés [Affectation : fréquence définie par l'organisation] pour détecter l'ajout de tout composant ou dispositif non autorisé au système d'information; et (b) désactive l'accès réseau de ces composants ou dispositifs ou informe les autorités responsables de l'organisation.	**Point(s) de mise en œuvre :** Service SDISF, points d'accès sans fil et capteurs. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), effectue une surveillance à chaque [Affectation : fréquence définie par l'organisation] pour détecter l'ajout de tout composant ou dispositif non autorisé au système d'information et (**b**) désactive l'accès réseau de ces composants ou dispositifs ou informe les autorités responsables de l'organisation.	S
CP-9 Sauvegarde du système d'information	CP-9-A L'organisation effectue des sauvegardes des données utilisateur contenues dans le système d'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise].	**Point(s) de mise en œuvre :** S.O. **Description :** Le scénario d'utilisation opérationnelle ne prévoit aucun stockage ni sauvegarde d'information des utilisateurs sans fil invités.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
CP-9 Sauvegarde du système d'information	CP-9-B L'organisation effectue des sauvegardes des données système contenues dans le système d'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise].	**Point(s) de mise en œuvre :** Service de sauvegarde et de reprise, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service de sauvegarde et de reprise accède aux capteurs, aux points d'accès, aux commutateurs, à la passerelle d'authentification et aux composants de périmètre d'utilisateur sans fil invité pour sauvegarder l'information système contenue dans le système d'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise].	S
CP-9 Sauvegarde du système d'information	CP-9-C L'organisation effectue des sauvegardes de la documentation liée au système d'information, y compris la documentation sur la sécurité, [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise].	**Point(s) de mise en œuvre :** Service de sauvegarde et de reprise et service de gestion de l'information. **Description :** Le service de sauvegarde et de reprise effectue des sauvegardes de la documentation liée au système d'information qui sont gérées par le service de gestion de l'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise].	C
CP-9 Sauvegarde du système d'information	CP-9-6 L'organisation effectue la sauvegarde du système d'information en recourant à un système secondaire redondant, situé hors de l'emplacement du système opérationnel, qui peut être activé sans perte d'information ou perturbation des opérations.	**Point(s) de mise en œuvre :** Tous **Description :** Un système secondaire redondant est prévu pour assurer la disponibilité permanente de la fonction dans l'éventualité d'une défaillance du système principal.	S
CP-10 Reprise et reconstitution du système d'information	CP-10-2 Le système d'information applique un processus de reprise des transactions pour les systèmes de traitement transactionnel.	**Point(s) de mise en œuvre :** S.O. **Description :** Les utilisateurs sans fil invités ne peuvent accéder aux applications axées sur les transactions utilisées par le ministère.	-
CP-10 Reprise et reconstitution du système d'information	CP-10-5 L'organisation offre [Affectation : capacité de basculement définie par l'organisation pour le système d'information] en [Sélection : temps réel; temps quasi réel].	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité sont mis en œuvre de manière à appuyer [Affectation : capacité de basculement définie par l'organisation pour le système d'information] en [Sélection : temps réel; temps quasi réel].	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-A Le système d'information identifie de façon unique et authentifie les utilisateurs organisationnels (ou les processus exécutés en leur nom).	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les justificatifs d'identité de compte sont configurés dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliqués dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité.	S
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-1 Le système d'information utilise l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'authentification multifactorielle est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquée dans la fonction de connexion d'accès au réseau des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Les utilisateurs sans fil invités ne bénéficient d'aucun droit.	-
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-2 Le système d'information utilise l'authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.	**Point(s) de mise en œuvre :** S.O. **Description :** L'utilisation de l'authentification multifactorielle ne s'applique pas aux utilisateurs sans fil invités (qui n'ont aucun droit) aux fins d'accès local puisqu'on leur attribue uniquement des comptes d'utilisateur temporaires basés sur des justificatifs d'identité liés à des mots de passe.	-
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-3 Le système d'information utilise l'authentification multifactorielle pour l'accès local aux comptes privilégiés.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'authentification multifactorielle est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquée dans la fonction de connexion d'accès locale des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Les utilisateurs sans fil invités ne bénéficient d'aucun droit.	S
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-4 Le système d'information utilise l'authentification multifactorielle pour l'accès local aux comptes non privilégiés.	**Point(s) de mise en œuvre :** S.O. **Description :** L'utilisation de l'authentification multifactorielle ne s'applique pas aux utilisateurs sans fil invités (qui n'ont aucun droit) aux fins d'accès local puisqu'on leur attribue uniquement des comptes d'utilisateur temporaires basés sur des justificatifs d'identité liés à des mots de passe.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-5 L'organisation : (a) permet l'utilisation d'authentifiants de groupe seulement s'ils sont utilisés de pair avec un authentifiant individuel ou unique; et (b) exige des utilisateurs qu'ils soient authentifiés par un authentifiant individuel avant d'utiliser un authentifiant de groupe.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Si des authentifiants de groupe sont utilisés pour des comptes d'administrateur de composants sans fil, ils le sont uniquement de pair avec un authentifiant individuel/unique; les individus sont d'abord authentifiés avec un authentifiant individuel avant l'utilisation d'un authentifiant de groupe. La fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité offre ce processus d'authentification. Les authentifiants de groupe ne s'appliquent pas aux utilisateurs sans fil invités puisqu'on leur attribue uniquement des comptes d'utilisateur temporaires basés sur des justificatifs d'identité liés à des mots de passe.	S
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-6 Le système d'information utilise, pour l'accès réseau aux comptes privilégiés, une authentification multifactorielle où l'un des facteurs est fourni par un dispositif distinct du système d'information auquel l'utilisateur accède.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'authentification multifactorielle est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquée dans la fonction de connexion d'accès au réseau des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Un des facteurs est fourni par un dispositif distinct du système d'information qui fait l'objet de l'accès. Les utilisateurs sans fil invités ne bénéficient d'aucun droit.	-
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-7 Le système d'information utilise, pour l'accès réseau aux comptes non privilégiés, une authentification multifactorielle où l'un des facteurs est fourni par un dispositif distinct du système d'information auquel l'utilisateur accède.	**Point(s) de mise en œuvre :** S.O. **Description :** L'utilisation de l'authentification multifactorielle ne s'applique pas aux utilisateurs sans fil invités (qui n'ont aucun droit) aux fins d'accès local puisqu'on leur attribue uniquement des comptes d'utilisateur temporaires basés sur des justificatifs d'identité liés à des mots de passe.	-
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-8 Le système d'information utilise [Affectation : mécanismes d'authentification résistant aux réinsertions définis par l'organisation] pour l'accès réseau aux comptes privilégiés.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La méthode d'authentification est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquée dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité utilise	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		[Affectation : mécanismes d'authentification résistant aux réinsertions définis par l'organisation]. Les utilisateurs sans fil invités ne bénéficient d'aucun droit.	
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-9 Le système d'information utilise [Affectation : mécanismes d'authentification résistant aux réinsertions définis par l'organisation] pour l'accès réseau aux comptes non privilégiés.	**Point(s) de mise en œuvre :** S.O. **Description :** L'utilisation de l'authentification multifactorielle ne s'applique pas aux utilisateurs sans fil invités (qui n'ont aucun droit) aux fins d'accès local puisqu'on leur attribue uniquement des comptes d'utilisateur temporaires basés sur des justificatifs d'identité liés à des mots de passe.	-
IA-2 Identification et authentification (utilisateurs organisationnels)	IA-2-100 Le système d'information utilise l'authentification multifactorielle pour l'accès à distance aux comptes privilégiés.	**Point(s) de mise en œuvre :** S.O. **Description :** Les administrateurs de composants sans fil n'utilisent pas de connexions d'accès à distance pour administrer leurs composants.	-
IA-3 Identification et authentification des dispositifs	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisqu'il n'exige pas l'authentification des postes de travail d'utilisateur sans fil invité.	-
IA-4 Gestion des identificateurs	IA-4-5 Le système d'information gère de manière dynamique les identificateurs, les attributs et les autorisations d'accès connexes.	**Point(s) de mise en œuvre :** S.O. **Description :** L'utilisation de la gestion dynamique des identificateurs, attributs et autorisations d'accès connexes ne s'applique pas au scénario d'utilisation opérationnelle.	-
IA-5 Gestion des authentifiants	IA-5-1 Authentification axée sur les mots de passe – Le système d'information : (a) applique un mot de passe de complexité minimale [Affectation : exigences définies par l'organisation concernant la sensibilité à la casse, le nombre de caractères, la combinaison minuscules-majuscules, les lettres minuscules, les chiffres et les caractères spéciaux, y compris les exigences minimales pour chaque type]; (b) applique au minimum [Affectation : nombre de caractères modifiés défini par l'organisation] lors de la création	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les comptes d'administrateur de composants sans fil sont configurés dans le service d'authentification et d'autorisation pour appuyer l'authentification axée sur les mots de passe qui (**a**) applique un mot de passe de complexité minimale [Affectation : exigences définies par l'organisation concernant la sensibilité à la casse, le nombre de caractères, la combinaison minuscules-majuscules, les lettres minuscules, les chiffres et les caractères spéciaux, y compris les exigences minimales pour chaque type]; (**b**) applique au minimum [Affectation : nombre de caractères modifiés défini par l'organisation] lors de la création de nouveaux mots de passe; (**c**) chiffre les mots de passe stockés et en transit; (**d**) applique les restrictions minimales et maximales de durée des mots de passe, soit [Affectation : nombre défini par l'organisation pour la durée minimale ou maximale]; et (**e**) interdit la réutilisation des mots de passe pendant [Affectation : nombre défini par l'organisation] générations. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	de nouveaux mots de passe; (c) chiffre les mots de passe stockés et en transit; (d) applique les restrictions minimales et maximales de durée des mots de passe, soit [Affectation : nombre défini par l'organisation pour la durée minimale ou maximale]; et (e) interdit la réutilisation des mots de passe pendant [Affectation : nombre défini par l'organisation] générations.	leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	
IA-5 Gestion des authentifiants	IA-5-2 Authentification axée sur l'ICP – Le système : (a) valide les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé; (b) applique la procédure d'accès autorisé à la clé privée correspondante; et (c) associe l'identité authentifiée au compte de l'utilisateur.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, service ICP, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'authentification basée sur l'ICP est configurée dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et prise en charge par le service ICP pour (**a**) valider les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé; (**b**) appliquer la procédure d'accès autorisé à la clé privée correspondante; et (**c**) associer l'identité authentifiée au compte de l'utilisateur. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
IA-6 Rétroaction d'authentification	IA-6-A Le système d'information obscure les rétroactions d'information durant le processus d'authentification afin de protéger l'information contre de possibles exploitations ou utilisations par des personnes non autorisées.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** L'authentification appliquée dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité occulte l'information sur la rétroaction d'authentification durant le processus d'authentification. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	S
IA-7 Authentification des modules cryptographiques	IA-7-A Le système d'information utilise des mécanismes d'authentification auprès d'un module cryptographique qui satisfont à l'orientation du CSTC en matière d'authentification.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les méthodes d'authentification sont configurées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		appliquées dans la fonction de connexion des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Ces méthodes répondent aux exigences des conseils concernés du CSTC en matière d'authentification auprès d'un module cryptographique. Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités puisque leurs comptes exigent un niveau de sécurité inférieur à ceux des administrateurs de composants sans fil.	
IA-8 Identification et authentification (utilisateurs non organisationnels)	IA-8-A Le système d'information identifie de façon unique et authentifie les utilisateurs non organisationnels (ou les processus exécutés en leur nom).	**Point(s) de mise en œuvre :** Passerelle d'authentification **Description :** Les utilisateurs sans fil invités doivent réussir à s'authentifier auprès de la passerelle d'authentification avec des justificatifs d'identité de compte temporaire avant que leurs dispositifs mobiles soient autorisés à se connecter aux réseaux SCNet/Internet.	S
MA-4 Télémaintenance	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle qui n'offre pas de soutien pour les activités de télémaintenance et de télédiagnostic.	-
SC-2 Partitionnement des applications	SC-2-A Le système d'information sépare la fonctionnalité utilisateur (y compris les services d'interface utilisateur) de la fonctionnalité de gestion du système d'information.	**Point(s) de mise en œuvre :** Service réseau **Description :** Le réseau ministériel inclut une sous-zone de gestion mise en place par le service réseau pour séparer les services d'utilisateurs et de gestion.	C
SC-2 Partitionnement des applications	SC-2-1 Le système d'information empêche la présentation de la fonctionnalité liée à la gestion du système d'information à une interface pour les utilisateurs généraux (c.-à-d. non privilégiés).	**Point(s) de mise en œuvre :** Points d'accès, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les points d'accès, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité empêchent l'affichage d'information sur la fonction de gestion des systèmes d'information à tout point d'interface auquel ont accès les utilisateurs sans fil invités.	S
SC-3 Isolement des fonctions de sécurité	SC-3-A Le système d'information isole les fonctions de sécurité des autres fonctions.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité isolent les fonctions de sécurité des autres fonctions.	S
SC-3 Isolement des fonctions de sécurité	SC-3-1 Le système d'information recoure à des mécanismes sous-jacents de séparation matérielle	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité recourent à des	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	pour faciliter l'isolement des fonctions de sécurité.	mécanismes sous-jacents de séparation matérielle pour faciliter l'isolement des fonctions de sécurité.	
SC-3 Isolement des fonctions de sécurité	SC-3-2 Le système isole, à la fois des autres fonctions de sécurité et des fonctions non liées à la sécurité, les fonctions de sécurité appliquant le contrôle de l'accès et du flux d'information.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité isolent, à la fois des autres fonctions de sécurité et des fonctions non liées à la sécurité, les fonctions de sécurité qui appliquent le contrôle de l'accès et du flux d'information.	S
SC-3 Isolement des fonctions de sécurité	SC-3-3 L'organisation recoure à un périmètre d'isolation du système d'information pour réduire le nombre de fonctions non liées à la sécurité partageant le même périmètre que les fonctions de sécurité.	**Point(s) de mise en œuvre :** Service réseau et périmètre d'utilisateur sans fil invité **Description :** Les dispositifs mobiles d'utilisateur sans fil invité sont limités à la zone d'utilisateur sans fil invité établie par le service réseau et au périmètre d'utilisateur sans fil invité. La zone d'utilisateur sans fil invité isole les utilisateurs sans fil invités des fonctions de sécurité du réseau ministériel.	S
SC-3 Isolement des fonctions de sécurité	SC-3-4 L'organisation applique les fonctions de sécurité sous forme de modules essentiellement indépendants qui évitent toute interaction inutile entre eux.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité appliquent les fonctions de sécurité sous forme de modules essentiellement indépendants qui évitent toute interaction inutile entre eux.	S
SC-3 Isolement des fonctions de sécurité	SC-3-5 L'organisation applique les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient assujetties au bon fonctionnement des couches supérieures ou de leurs fonctions.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité appliquent les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient assujetties au bon fonctionnement des couches supérieures ou de leurs fonctions.	S
SC-4 Information contenue dans les ressources partagées	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisqu'il ne fait pas appel à l'utilisation de ressources système partagées.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SC-5 Protection contre les dénis de service	SC-5-A Le système d'information protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Affectation : liste définie par l'organisation des types d'attaques par déni de service ou renvoi à la source de la liste actuelle].	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), surveille les attaques par déni de service [Affectation : liste définie par l'organisation des types d'attaques par déni de service ou renvoi à la source de la liste actuelle] dans la zone d'utilisateur sans fil invité tandis que le service SDI surveille ce même type d'attaque [Affectation : liste définie par l'organisation des types d'attaques par déni de service ou renvoi à la source de la liste actuelle] dans le reste du réseau ministériel.	S
SC-5 Protection contre les dénis de service	SC-5-1 Le système d'information limite la capacité des utilisateurs de lancer des attaques par déni de service contre d'autres systèmes d'information ou réseaux.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), surveille les attaques par déni de service provenant de la zone d'utilisateur sans fil invité tandis que le service SDI surveille ce même type d'attaque en provenance du reste du réseau ministériel.	S
SC-5 Protection contre les dénis de service	SC-5-2 Le système d'information gère l'excédent de capacité et de largeur de bande, ou toute autre redondance, afin de limiter les effets d'attaques par déni de service de types inondation d'information.	**Point(s) de mise en œuvre :** Service réseau **Description :** Les routeurs du service réseau permettent l'attribution de seuils de volume de trafic par types de trafic réseau pour limiter les effets des attaques par déni de service de types inondation d'information.	C
SC-6 Priorité des ressources	SC-6-A Le système d'information limite l'utilisation des ressources selon leur priorité.	**Point(s) de mise en œuvre :** Service réseau **Description :** Les routeurs du service réseau permettent l'attribution de seuils de volume de trafic par types de trafic réseau pour limiter l'utilisation des ressources selon la priorité associée aux types de trafic.	C
SC-7 Protection des frontières	SC-7-A Le système d'information surveille et contrôle les communications à sa frontière externe et à ses principales frontières internes.	**Point(s) de mise en œuvre :** Service réseau et périmètre d'utilisateur sans fil invité. **Description :** Les périmètres utilisés pour mettre en œuvre les zones du réseau ministériel (incluant le périmètre d'utilisateur sans fil invité) surveillent et contrôlent les communications à sa frontière externe et à ses principales frontières internes.	S
SC-7 Protection des frontières	SC-7-B Le système d'information se connecte aux réseaux ou aux systèmes d'information externes uniquement par des interfaces gérées qui sont dotées de	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité négocie les accès entre les réseaux publics et la zone des utilisateurs sans fil invités.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	mécanismes de protection des frontières répartis conformément à l'architecture de sécurité de l'organisation.		
SC-7 Protection des frontières	SC-7-1 L'organisation attribue physiquement les composants de système d'information accessibles au public pour séparer les sous-réseaux par des interfaces réseau physiques distinctes.	**Point(s) de mise en œuvre :** Service réseau **Description :** Les composants de système d'information accessibles au public se trouvent dans la zone d'accès public créée par le service réseau.	C
SC-7 Protection des frontières	SC-7-2 Le système d'information empêche tout accès public aux réseaux internes de l'organisation sauf dans le cas où l'accès est négocié de manière appropriée par des interfaces gérées dotées de dispositifs de protection des frontières.	**Point(s) de mise en œuvre :** Service réseau et périmètre d'utilisateur sans fil invité. **Description :** Les périmètres utilisés pour mettre en œuvre les zones du réseau ministériel (incluant le périmètre d'utilisateur sans fil invité) surveillent et contrôlent les communications à sa frontière externe et à ses principales frontières internes. Ces périmètres empêchent l'accès public aux réseaux internes du ministère.	S
SC-7 Protection des frontières	SC-7-3 L'organisation limite le nombre de points d'accès au système d'information afin d'exercer une meilleure surveillance des communications entrantes et sortantes et du trafic réseau.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Les points d'accès des utilisateurs sans fil invités sont limités à la zone d'utilisateur sans fil invité.	S
SC-7 Protection des frontières	SC-7-4 L'organisation : (a) applique une interface gérée à chaque service de télécommunications externe; (b) établit une politique de flux de trafic pour chaque interface gérée; (c) utilise des contrôles de sécurité selon les besoins pour protéger la confidentialité et l'intégrité de l'information transmise; (d) documente chaque exception à la politique de flux de	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'accèdent pas à de l'information dans le réseau ministériel.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	trafic en précisant le besoin de la mission ou de l'activité opérationnelle donnant lieu à l'exception et la durée de ce besoin; (e) examine les exceptions à la politique de flux de trafic [Affectation : fréquence définie par l'organisation]; et (f) supprime les exceptions à la politique de flux de trafic qui ne sont plus justifiées par un besoin explicite de la mission ou d'une activité opérationnelle.		
SC-7 Protection des frontières	SC-7-5 Le système d'information, au niveau des interfaces gérées, interdit tout trafic réseau par défaut et ne l'autorise qu'exceptionnellement (c.-à-d. interdit tout trafic, permet le trafic par exception).	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité interdit tout trafic réseau par défaut et ne l'autorise qu'exceptionnellement.	S
SC-7 Protection des frontières	SC-7-6 L'organisation empêche toute diffusion d'information non autorisée hors des frontières du système d'information ou toute communication non autorisée à travers les frontières du système d'information en cas de défaillance opérationnelle des mécanismes de protection des frontières.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité tombe à l'état ouvert (c.-à-d. interdit toute communication) pour empêcher toute diffusion non autorisée d'information.	S
SC-7 Protection des frontières	SC-7-7 Le système d'information empêche les dispositifs distants, qui ont établi une connexion non distante avec le système, de communiquer à l'extérieur de cette voie de communication avec des ressources de réseaux externes.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SC-7 Protection des frontières	SC-7-8 Le système d'information achemine [Affectation : trafic de communications interne défini par l'organisation] vers [Affectation : réseaux externes définis par l'organisation] à travers des serveurs mandataires authentifiés dans les interfaces gérées des dispositifs de protection des frontières.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet. Les communications d'utilisateur sans fil invité ne sont pas des communications internes du réseau ministériel.	S
SC-7 Protection des frontières	SC-7-9 Le système d'information, au niveau des interfaces gérées, interdit le trafic réseau et vérifie les utilisateurs internes (ou le code malveillant) qui représentent une menace pour les systèmes d'information externes.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications de dispositif mobile de manière à ce qu'elles accèdent uniquement aux réseaux SCNet/Internet.	S
SC-7 Protection des frontières	SC-7-10 L'organisation empêche l'exfiltration d'information non autorisée à travers les interfaces gérées.	**Point(s) de mise en œuvre :** S.O. **Description :** Cette exigence de contrôle de sécurité ne s'applique pas aux utilisateurs sans fil invités qui n'accèdent pas à de l'information dans le réseau ministériel.	-
SC-7 Protection des frontières	SC-7-11 Le système d'information vérifie les communications entrantes pour s'assurer qu'elles proviennent d'une source autorisée et qu'elles sont acheminées vers une destination autorisée.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité contrôle les communications entrantes et sortantes de la zone d'utilisateur sans fil invité en tenant compte des ports TCP/IP et des adresses IP source et de destination.	S
SC-7 Protection des frontières	SC-7-12 Le système d'information applique des mécanismes de protection des frontières intégrés à l'hôte pour les serveurs, les postes de travail et les dispositifs mobiles.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Des mécanismes de protection des frontières intégrés à l'hôte sont appliqués aux capteurs, aux points d'accès, aux commutateurs, à la passerelle d'authentification et aux composants de périmètre d'utilisateur sans fil invité.	S
SC-7 Protection des frontières	SC-7-13 L'organisation isole les [Affectation : outils, mécanismes et composants de soutien clés de	**Point(s) de mise en œuvre :** Service réseau et périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	sécurité de l'information définis par l'organisation] des autres composants internes du système d'information au moyen de sous-réseaux physiques distincts dotés d'interfaces gérées tournées vers les autres parties du système.	**Description :** Les périmètres utilisés pour mettre en œuvre les zones du réseau ministériel (incluant le périmètre d'utilisateur sans fil invité) isolent les [Affectation : outils, mécanismes et composants de soutien clés de sécurité de l'information définis par l'organisation] des autres composants internes du système d'information.	
SC-7 Protection des frontières	SC-7-15 Le système d'information achemine tous les accès réseau privilégiés à travers une interface gérée spécialisée aux fins de contrôle des accès et de vérification.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité incluent une interface réseau de gestion distincte reliée à la sous-zone de gestion. Cette interface est utilisée pour permettre à l'administrateur interne d'accéder aux composants et pour appuyer le contrôle d'accès et la vérification à des fins administratives.	S
SC-7 Protection des frontières	SC-7-16 Le système d'information empêche la découverte des composants de système particuliers (ou dispositifs) d'une interface gérée.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité incluent une interface réseau de gestion distincte reliée à la sous-zone de gestion. Cette interface ignore les outils ou techniques de détection de réseau non autorisés.	S
SC-7 Protection des frontières	SC-7-17 L'organisation utilise des mécanismes automatisés pour imposer le respect rigoureux des formats de protocole.	**Point(s) de mise en œuvre :** Service réseau **Description :** Le service réseau prévoit des zones et des sous-zones qui permettent de séparer les composants dans le réseau ministériel selon les politiques de sécurité concernées. Les composants de périmètre qui séparent les zones et les sous-zones imposent un respect rigoureux du format du protocole et interdisent toute communication qui ne s'y conforme pas.	C
SC-7 Protection des frontières	SC-7-18 Le système d'information passe en mode de fonctionnement à sécurité intégrée (fail secure) dans l'éventualité d'une défaillance opérationnelle d'un dispositif de protection des frontières.	**Point(s) de mise en œuvre :** Service réseau et périmètre d'utilisateur sans fil invité. **Description :** Le service réseau et le périmètre d'utilisateur sans fil invité offrent des zones et des sous-zones qui permettent de séparer les composants dans le réseau ministériel selon les politiques de sécurité concernées. Les composants de périmètre qui séparent les zones et les sous-zones cessent de fonctionner de manière sécuritaire et interdisent toute communication durant leur état d'échec.	C

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SC-8 Intégrité des transmissions	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité des communications d'utilisateur sans fil invité.	-
SC-9 Confidentialité des transmissions	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité des communications d'utilisateur sans fil invité.	-
SC-10 Déconnexion réseau	SC-10-A Le système d'information met un terme à toute connexion réseau associée à une session de communications à la fin de la session ou après [Affectation : durée définie par l'organisation] d'inactivité.	**Point(s) de mise en œuvre :** Périmètre d'utilisateur sans fil invité **Description :** Le périmètre d'utilisateur sans fil invité est configuré de manière à interrompre les connexions réseau à la fin d'une session ou après [Affectation : période définie par l'organisation] d'inactivité.	S
SC-11 Chemin de confiance	SC-11-A Le système d'information établit une voie de communication de confiance entre l'utilisateur et les fonctions de sécurité de système suivantes : [Affectation : fonctions de sécurité définies par l'organisation et incluant, au minimum, l'authentification et la réauthentification du système d'information].	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les administrateurs de composants sans fil accèdent aux capteurs, aux points d'accès, aux commutateurs, à la passerelle d'authentification et aux composants de périmètre d'utilisateur sans fil invité depuis leurs postes de travail situés dans la sous-zone de gestion créée par le service réseau. Les politiques sur les flux d'information appliquées dans la zone d'accès restreint et la zone de travail font en sorte que les [Affectation : fonctions de sécurité définies par l'organisation et incluant, au minimum, l'authentification et la réauthentification du système d'information] peuvent seulement être exécutées depuis les postes de travail d'administrateur interne situés dans la sous-zone de gestion. Le chemin entre les administrateurs internes et les composants sans fil est par conséquent fiable.	S
SC-12 Établissement et gestion des clés cryptographiques	SC-12-A L'organisation établit et gère les clés cryptographiques utilisées pour les opérations de cryptographie requises dans le système d'information.	**Point(s) de mise en œuvre :** Service ICP **Description :** Le service ICP établit et gère les clés cryptographiques utilisées pour les opérations de cryptographie requises dans le système d'information.	C
SC-12 Établissement et gestion des clés cryptographiques	SC-12-2 L'organisation produit, contrôle et distribue des clés cryptographiques symétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC.	**Point(s) de mise en œuvre :** Service ICP **Description :** Le service ICP produit, contrôle et distribue des clés cryptographiques symétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC.	C

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SC-12 Établissement et gestion des clés cryptographiques	SC-12-3 L'organisation produit, contrôle et distribue des clés cryptographiques symétriques et asymétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC.	**Point(s) de mise en œuvre :** Service ICP **Description :** Le service ICP produit, contrôle et distribue des clés cryptographiques symétriques et asymétriques à l'aide d'une technologie et de processus de gestion des clés approuvés par le CSTC.	C
SC-12 Établissement et gestion des clés cryptographiques	SC-12-4 L'organisation produit, contrôle et distribue des clés cryptographiques asymétriques à l'aide de certificats approuvés d'assurance de niveau moyen ou de matériel de chiffrement préplacé.	**Point(s) de mise en œuvre :** Service ICP **Description :** Le service ICP produit, contrôle et distribue des clés cryptographiques asymétriques à l'aide de certificats ICP approuvés de classe 3 ou de matériel de chiffrement préplacé.	C
SC-12 Établissement et gestion des clés cryptographiques	SC-12-5 L'organisation produit, contrôle et distribue des clés cryptographiques asymétriques à l'aide de certificats approuvés d'assurance de niveau moyen ou élevé et des jetons de sécurité matériels qui protègent la clé privée de l'utilisateur.	**Point(s) de mise en œuvre :** Service ICP **Description :** Le service ICP produit, contrôle et distribue des clés cryptographiques asymétriques à l'aide de certificats ICP approuvés de classe 3 ou 4 et des jetons de sécurité matériels qui protègent la clé privée de l'utilisateur.	C
SC-13 Utilisation de la cryptographie	S.O.	Ce contrôle de sécurité ne s'applique pas au scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de sécuriser l'information transmise par les utilisateurs sans fil invités.	-
SC-14 Protection de l'accès public	S.O.	Ce contrôle de sécurité ne s'applique pas au scénario d'utilisation opérationnelle, qui ne couvre pas la protection de l'intégrité et de la disponibilité de l'information et des applications offertes au public.	-
SC-16 Transmission des attributs de sécurité	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle. L'échange d'information et les attributs de sécurité qui lui sont associés entre les différents systèmes d'information (c.-à-d. le réseau ministériel et certains autres systèmes d'information) ne sont pas pris en charge par le scénario d'utilisation opérationnelle.	-
SC-18 Code mobile	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		des communications d'utilisateur sans fil invité ou de l'information qu'elles traitent ou stockent.	
SC-20 Service sécurisé de résolution de nom ou d'adresse (source autorisée)	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'offre pas de services DNS pour les utilisateurs sans fil invités. Les dispositifs mobiles sont plutôt configurés à l'aide du protocole DHCP par le service réseau avec des adresses IP pour les serveurs DNS publics principal et secondaire.	-
SC-21 Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache)	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'offre pas de services DNS pour les utilisateurs sans fil invités. Les dispositifs mobiles sont plutôt configurés à l'aide du protocole DHCP par le service réseau avec des adresses IP pour les serveurs DNS publics principal et secondaire.	-
SC-22 Architecture et fourniture de service de résolution de nom ou d'adresse	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'offre pas de services DNS pour les utilisateurs sans fil invités. Les dispositifs mobiles sont plutôt configurés à l'aide du protocole DHCP par le service réseau avec des adresses IP pour les serveurs DNS publics principal et secondaire.	-
SC-23 Authenticité des sessions	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas à ce scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité des communications d'utilisateur sans fil invité.	-
SC-24 Défaillance dans un état connu	SC-24-A Le système d'information tombe à l'état [Affectation : état connu défini par l'organisation] pour [Affectation : types de défaillance définis par l'organisation] et conserve [Affectation : information sur l'état du système définie par l'organisation] durant la défaillance.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateur sans fil et périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, le commutateur sans fil et le périmètre d'utilisateur sans fil invité tombent à l'état [Affectation : état connu défini par l'organisation] pour [Affectation : types de défaillance définis par l'organisation] et conserve [Affectation : information sur l'état du système définie par l'organisation] durant la défaillance.	S
SC-25 Noeuds légers	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas puisque l'utilisation de nœuds légers n'est pas prise en charge par le scénario d'utilisation opérationnelle.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SC-26 Pièges à pirates	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas puisque l'utilisation de pièges à pirates n'est pas prise en charge par le scénario d'utilisation opérationnelle.	-
SC-27 Applications indépendantes des systèmes d'exploitation	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas au scénario d'utilisation opérationnelle puisque les utilisateurs sans fil invités n'accèdent à aucune application ministérielle.	-
SC-28 Protection de l'information inactive		Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas au scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité de l'information inactive des utilisateurs sans fil invités.	-
SC-29 Hétérogénéité	SC-29-A L'organisation utilise diverses technologies de l'information pour la mise en œuvre du système d'information.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateur sans fil et périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs sans fil et le périmètre d'utilisateur sans fil invité sont mis en œuvre en utilisant différentes technologies de l'information. Cette approche peut ne pas convenir lorsque les composants sans fil sont achetés d'un même fournisseur pour faciliter leur intégration mutuelle.	S
SC-30 Techniques de virtualisation	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle puisque les utilisateurs sans fil invités n'accèdent à aucun service ministériel qui doit être protégé par des techniques de virtualisation.	-
SC-32 Partitionnement des systèmes d'information	SC-32-A L'organisation partitionne au besoin le système d'information en composants hébergés dans des domaines (ou environnements) physiques distincts.	**Point(s) de mise en œuvre :** Service réseau **Description :** Le service réseau et le périmètre d'utilisateur sans fil invité créent des zones et des sous-zones qui servent à séparer les composants dans le réseau ministériel en fonction de leurs politiques de sécurité.	C
SC-33 Intégrité de la préparation des transmissions	S.O.	Ce contrôle de sécurité, et ses éléments de contrôle techniques, ne s'appliquent pas au scénario d'utilisation opérationnelle puisque le ministère n'est pas responsable de la sécurité des communications d'utilisateur sans fil invité.	-
SC-34 Programmes exécutables non modifiables	SC-34-A Le système d'information, au niveau de [Affectation : composants de système d'information définies par l'organisation], charge et exécute l'environnement	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité identifiés dans	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	d'exploitation à partir de supports non inscriptibles mis en œuvre par matériel.	[Affectation : composants de système d'information définis par l'organisation] chargent et exécutent leur environnement d'exploitation à partir de supports matériels non inscriptibles.	
SC-34 Programmes exécutables non modifiables	SC-34-B Le système d'information, au niveau de [Affectation : composants de système d'information définis par l'organisation], charge et exécute [Affectation : applications définies par l'organisation] à partir de supports non inscriptibles mis en œuvre par matériel.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité identifiés dans [Affectation : composants de système d'information définis par l'organisation] chargent et exécutent [Affectation : applications définies par l'organisation] à partir de supports matériels non inscriptibles.	S
SC-34 Programmes exécutables non modifiables	(1) L'organisation utilise [Affectation : composants de système d'information définis par l'organisation] avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage du composant ou lors des mises sous tension et hors tension.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité identifiés dans [Affectation : composants de système d'information définis par l'organisation] sont configurés avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage du composant ou lors des mises sous tension et hors tension.	S
SC-100 Authentification de la source	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle, puisque le ministère n'est pas responsable de protéger l'information transmise, traitée ou stockée par les utilisateurs sans fil invités, incluant l'authentification de la source des messages.	-
SC-101 Systèmes de télécommunications non classifiés dans les installations sécurisées	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas, puisque l'utilisation de systèmes de télécommunications n'est pas prise en charge par le scénario d'utilisation opérationnelle.	-
SI-2 Correction des défauts	SI-2-1 L'organisation centralise la gestion du processus de correction des défauts et installe les mises à jour logicielles automatiquement.	**Point(s) de mise en œuvre :** Service de remédiation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service de remédiation automatise la collecte, l'analyse et l'approvisionnement des rustines logicielles des capteurs, des points d'accès, des	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité qui lui sont compatibles.	
SI-2 Correction des défauts	SI-2-2 L'organisation utilise des mécanismes automatisés [Affectation : fréquence définie par l'organisation] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des défauts.	**Point(s) de mise en œuvre :** Service de remédiation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service de remédiation automatise la collecte, l'analyse et l'approvisionnement des rustines logicielles des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité qui lui sont compatibles.	S
SI-2 Correction des défauts	SI-2-4 L'organisation utilise des outils automatisés de gestion des correctifs pour faciliter la correction des défauts des [Affectation : composants du système d'information définis par l'organisation].	**Point(s) de mise en œuvre :** Service de remédiation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Le service de remédiation automatise la collecte, l'analyse et l'approvisionnement des rustines logicielles des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité qui lui sont compatibles.	S
SI-3 Protection contre les codes malveillants		Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle, puisque le ministère n'est pas responsable de la sécurité de l'information des utilisateurs sans fil invités.	-
SI-4 Surveillance des systèmes d'information	SI-4-A L'organisation surveille les événements liés au système d'information conformément à [Affectation : objectifs de surveillance définis par l'organisation] et détecte les attaques contre le système.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), surveille les événements conformément à [Affectation : objectifs de surveillance définis par l'organisation] et détecte les attaques contre le système.	S
SI-4 Surveillance des systèmes d'information	SI-4-C L'organisation déploie dans le système d'information des dispositifs de surveillance à la fois (a) stratégiquement pour collecter l'information qu'elle juge essentielle et (b) de manière aléatoire pour faire le suivi des types de transaction qui l'intéressent particulièrement.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), assure une capacité de surveillance dans la zone d'utilisateur sans fil invité tandis que le service SDI offre la même capacité dans le reste du réseau ministériel.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SI-4 Surveillance des systèmes d'information	SI-4-1 L'organisation utilise des protocoles communs pour interconnecter et configurer les outils individuels de détection d'intrusion en un système unique.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), s'intègre au service SDI pour offrir un système global de détection d'intrusions.	S
SI-4 Surveillance des systèmes d'information	SI-4-2 L'organisation utilise des outils automatisés pour prendre en charge l'analyse des événements en temps quasi réel.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), assure une analyse en temps quasi réel des événements dans la zone d'utilisateur sans fil invité tandis que le service SDI offre le même service dans le reste du réseau ministériel.	S
SI-4 Surveillance des systèmes d'information	SI-4-3 L'organisation utilise des outils automatisés pour intégrer les outils de détection d'intrusion aux mécanismes de contrôle d'accès et de flux afin de permettre la reconfiguration de ces mécanismes en vue d'isoler et d'éliminer rapidement les attaques.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et périmètre d'utilisateur sans fil invité. **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), s'intègre au périmètre d'utilisateur sans fil invité pour assurer le contrôle du flux d'information en vue d'isoler et d'éliminer les attaques.	S
SI-4 Surveillance des systèmes d'information	SI-4-4 Le système d'information surveille les communications entrantes et sortantes pour détecter toute activité ou condition inhabituelle ou non autorisée.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et périmètre d'utilisateur sans fil invité. **Description :** Le service SDISF, incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), et le périmètre d'utilisateur sans fil invité surveillent les communications entrantes et sortantes pour détecter toute activité ou condition inhabituelle ou non autorisée.	S
SI-4 Surveillance des systèmes d'information	SI-4-5 Le système d'information produit des alertes en temps quasi réel lorsque les indications de compromission réelle ou potentielle suivantes se présentent : [Affectation : liste des indicateurs de compromission définie par l'organisation].	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI **Description :** Le service SDISF, de pair avec ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), détectent les événements dans la zone d'utilisateur sans fil invité et produisent des alertes en temps réel lorsque les indications de compromission réelle ou potentielle suivantes se présentent : [Affectation : liste des indicateurs de compromission définie par l'organisation].	S
SI-4 Surveillance des systèmes d'information	SI-4-6 Le système d'information empêche les utilisateurs non privilégiés de contourner les	**Point(s) de mise en œuvre :** S.O.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	capacités de détection et de prévention des intrusions.	**Description :** Les utilisateurs sans fil invités n'ont pas accès au réseau ministériel et ne peuvent donc contourner les capacités de détection et de prévention d'intrusions.	
SI-4 Surveillance des systèmes d'information	SI-4-7 Le système d'information informe [Affectation : liste définie par l'organisation des employés (identifiés par nom ou rôle) chargés d'intervenir en cas d'incident] des événements suspects et prend les [Affectation : liste définie par l'organisation des mesures les moins perturbatrices visant à mettre fin aux événements suspects].	**Point(s) de mise en œuvre :** Service SDISF, points d'accès sans fil, capteurs, service SDI et service de vérification. **Description :** Le service SDISF (incluant les capteurs (SDISF en mode recouvrement) ou les points d'accès (SDISF en mode intégré)), le service SDI et le service de vérification informent [Affectation : liste définie par l'organisation des employés (identifiés par nom ou rôle) chargés d'intervenir en cas d'incident] des événements suspects et prend les [Affectation : liste définie par l'organisation des mesures les moins perturbatrices visant à mettre fin aux événements suspects].	S
SI-4 Surveillance des systèmes d'information	SI-4-8 L'organisation protège l'information obtenue des outils de surveillance des intrusions contre tout accès non autorisé et toute modification et suppression.	**Point(s) de mise en œuvre :** Service d'authentification et d'autorisation, Service SDISF et service SDI. **Description :** Les autorisations sont attribuées dans le service d'authentification et d'autorisation pour les administrateurs de composants sans fil et appliquées dans la fonction de contrôle d'accès des services SDISF et SDI. Elles font en sorte que l'information obtenue des outils de surveillance des intrusions est protégée contre les accès, les modifications et les suppressions non autorisés.	S
SI-4 Surveillance des systèmes d'information	SI-4-10 L'organisation prend les mesures nécessaires pour rendre le trafic chiffré visible aux outils de surveillance du système d'information.	**Point(s) de mise en œuvre :** S.O. **Description :** Le ministère n'a aucun contrôle sur les communications d'utilisateur sans fil invité et ne peut faire en sorte que le service SDISF puisse prendre connaissance du trafic chiffré.	-
SI-4 Surveillance des systèmes d'information	SI-4-11 L'organisation analyse le trafic des communications sortantes à la frontière externe du système (c.-à-d. à son périmètre) et, le cas échéant, à certains de ses points intérieurs (p. ex. sous-réseaux, sous-systèmes) pour découvrir des anomalies.	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et périmètre d'utilisateur sans fil invité. **Description :** Le service SDISF, incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), et le périmètre d'utilisateur sans fil invité surveillent les communications entrantes et sortantes pour détecter toute activité ou condition inhabituelle ou non autorisée.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SI-4 Surveillance des systèmes d'information	SI-4-12 L'organisation utilise des mécanismes automatisés pour alerter le personnel de sécurité des répercussions potentielles des activités inhabituelles ou inappropriées suivantes : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes].	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès, service SDI et service de vérification. **Description :** Le service SDISF, incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), le service SDI et le service de vérification alertent le personnel de sécurité des répercussions potentielles des activités inhabituelles ou inappropriées suivantes : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes].	S
SI-4 Surveillance des systèmes d'information	SI-4-13 L'organisation : (a) analyse le trafic des communications ou la tendance des événements pour le système d'information; (b) développe des profils représentant les modèles de trafic ou les événements communs; et (c) Utilise les profils pour calibrer les dispositifs de surveillance afin de réduire le nombre de faux positifs à [Affectation : mesure des faux positifs définie par l'organisation] et le nombre de faux négatifs à [Affectation : mesure des faux négatifs définie par l'organisation].	**Point(s) de mise en œuvre :** Service SDISF, capteurs, points d'accès et service SDI. **Description :** Le service SDISF, incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), et le service SDI analysent le trafic des communications ou la tendance des événements pour le système d'information; (**b**) développent des profils représentant les modèles de trafic ou les événements communs; et (**c**) utilisent les profils pour calibrer les dispositifs de surveillance afin de réduire le nombre de faux positifs à [Affectation : mesure des faux positifs définie par l'organisation] et le nombre de faux négatifs à [Affectation : mesure des faux négatifs définie par l'organisation].	S
SI-4 Surveillance des systèmes d'information	SI-4-14 L'organisation utilise un système de détection d'intrusions sans fil pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions ou infractions potentielles liées au système d'information.	**Point(s) de mise en œuvre :** Service SDISF, capteurs et points d'accès. **Description :** Le service SDISF, incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré), identifie les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions ou infractions potentielles liées au système d'information.	S
SI-4 Surveillance des systèmes d'information	SI-4-15 L'organisation utilise un système de détection d'intrusions pour surveiller le trafic de communications sans fil lorsqu'il	**Point(s) de mise en œuvre :** Service SDISF, points d'accès sans fil, capteurs et service SDI.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
	passe d'un réseau sans fil à un réseau filaire.	**Description :** Le service SDISF (incluant ses capteurs (SDISF en mode recouvrement) ou ses points d'accès (SDISF en mode intégré)), et le service SDI surveillent le trafic de communications sans fil lorsqu'il passe d'un réseau sans fil à un réseau filaire.	
SI-6 Vérification de la fonctionnalité de sécurité	SI-6-A Le système d'information vérifie le bon fonctionnement des fonctions de sécurité [Sélection (un ou plusieurs) : [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'un utilisateur qui possède les privilèges appropriés; périodiquement tous les [Affectation : période définie par l'organisation] et [Sélection (un ou plusieurs): informe l'administrateur de système; arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]] lorsque des anomalies sont relevées.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité vérifient le bon fonctionnement des fonctions de sécurité [Sélection (un ou plusieurs): [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'un utilisateur qui possède les droits appropriés; périodiquement tous les [Affectation : période définie par l'organisation] et [Sélection (un ou plusieurs): informe l'administrateur de système; arrête le système; redémarre le système; [Affectation : autre(s) mesure(s) définie(s) par l'organisation]] lorsque des anomalies sont relevées.	S
SI-6 Vérification de la fonctionnalité de sécurité	SI-6-1 Le système d'information fournit des notifications d'échec des tests de sécurité automatisés.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité utilisent des mécanismes automatisés pour fournir des notifications d'échec des tests de sécurité automatisés.	S
SI-6 Vérification de la fonctionnalité de sécurité	SI-6-2 Le système d'information offre un soutien automatisé pour la gestion des tests de sécurité distribués.	**Point(s) de mise en œuvre :** Capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité vérifient le bon fonctionnement de leurs fonctions de sécurité essentielles et communiquent les résultats de ces tests dans des enregistrements de vérification transmis au service de vérification.	S
SI-7 Intégrité de l'information et des logiciels	SI-7-A Le système d'information détecte les changements non autorisés apportés aux logiciels et à l'information.	**Point(s) de mise en œuvre :** SGC, SIF, service d'authentification et d'autorisation, service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité.	S

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
		Description : Les autorisations d'accès au logiciel, à l'information et aux fonctions sont configurées dans le service d'autorisation et appliquées dans la fonction de contrôle d'accès des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité. Toute mesure non autorisée est signalée par la fonction de vérification des composants au service de vérification. Le SGC permet de vérifier périodiquement les configurations du logiciel et de l'information des composants et de comparer ces résultats aux configurations approuvées dans le but de détecter tout changement non autorisé. Le SIF permet de détecter les modifications non autorisées aux fichiers des composants dans lesquels on peut installer un agent SIF. Le SGC et le SIF peuvent signaler tout changement inapproprié détecté à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification.	
SI-7 Intégrité de l'information et des logiciels	SI-7-2 L'organisation utilise des outils automatisés qui notifient les employés désignés lors de la découverte d'écarts durant la vérification de l'intégrité.	**Point(s) de mise en œuvre :** SGC et SIF. **Description :** Le SGC et le SIF peuvent signaler tout changement inapproprié détecté à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification.	C
SI-7 Intégrité de l'information et des logiciels	SI-7-3 L'organisation utilise des outils de vérification de l'intégrité gérés centralement.	**Point(s) de mise en œuvre :** SGC, SIF et service de vérification. **Description :** Le SGC permet de vérifier périodiquement les configurations du logiciel et de l'information des composants et de comparer ces résultats aux configurations approuvées dans le but de détecter tout changement non autorisé. Le SIF permet de détecter les modifications non autorisées aux fichiers des composants dans lesquels on peut installer un agent SIF. Le SGC et le SIF peuvent signaler tout changement inapproprié détecté à l'individu concerné soit directement (p. ex. courriel de notification) ou indirectement en transmettant des rapports au service de vérification.	C
SI-8 Protection antipourriel	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle, puisque les utilisateurs sans fil invités n'ont accès à aucun service de courriel ministériel.	-
SI-9 Restrictions relatives à la saisie d'information	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle, puisque les utilisateurs sans fil invités n'ont accès à aucun service d'information du réseau ministériel.	-
SI-10 Validation de la saisie d'information	S.O.	Ce contrôle de sécurité et ses éléments de contrôle techniques ne s'appliquent pas au scénario d'utilisation opérationnelle, puisque les utilisateurs sans fil invités n'ont accès à aucun service d'information du réseau ministériel.	-

Contrôle de sécurité	Élément de contrôle	Points de mise en œuvre	Type S/C/H
SI-11 Traitement des erreurs	SI-11-A Le système d'information identifie les conditions d'erreur potentielles liées à la sécurité.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de signaler au service de vérification toute condition d'erreur potentielle liée à la sécurité.	S
SI-11 Traitement des erreurs	SI-11-B Le système d'information produit des messages d'erreur qui fournissent l'information nécessaire sur les mesures correctrices sans révéler [Affectation : information sensible ou potentiellement préjudiciable définie par l'organisation] contenue dans les journaux d'erreurs et les messages administratifs qui pourrait être exploitée par des adversaires.	**Point(s) de mise en œuvre :** Service de vérification, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** La fonction de vérification des capteurs, des points d'accès, des commutateurs, de la passerelle d'authentification et des composants de périmètre d'utilisateur sans fil invité permet de configurer le type de messages d'erreur (p. ex. les enregistrements de vérification) communiqués au service de vérification pour fournir l'information nécessaire sur les mesures correctrices sans révéler [Affectation : information sensible ou potentiellement préjudiciable définie par l'organisation] contenue dans les journaux d'erreurs et les messages administratifs qui pourrait être exploitée par des adversaires.	S
SI-11 Traitement des erreurs	SI-11-C Le système d'information révèle les messages d'erreur seulement au personnel autorisé.	**Point(s) de mise en œuvre :** Service de vérification, service d'authentification et d'autorisation, capteurs, points d'accès, commutateurs, passerelle d'authentification et composants de périmètre d'utilisateur sans fil invité. **Description :** Les autorisations d'accès aux données et aux outils de vérification (incluant les messages d'erreur) accordées au personnel autorisé du service de vérification sont configurées dans le service d'authentification et d'autorisation et appliquées par le service de vérification. Les autorisations d'accès du personnel autorisé à vérifier l'information dans les capteurs, les points d'accès, les commutateurs, la passerelle d'authentification et les composants de périmètre d'utilisateur sans fil invité sont configurées dans le service d'authentification et d'autorisation et appliquées par la fonction de contrôle d'accès des composants.	S

3. Références

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

[2] *ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie,* **CSTC** (MMM AAAA)

[3] *ITSG-41, Exigences de sécurité liées aux réseaux locaux sans fil*, **CSTC** (sept. 2012)

[4] *ITSG-41, Annexe 2 – Conception de haut niveau – Connexion utilisateur sans fil/réseau câblé*, **CSTC** (sept. 2012)

[5] *ITSG-41, Annexe 3 – Conception de haut niveau – Interconnexions de réseaux câblés par un pont sans fil*, **CSTC** (sept. 2012)

[6] *ITSG-41, Annexe 4 – Détermination des éléments de contrôle en fonction des contrôles de sécurité*, **CSTC** (sept. 2012)

[7] *ITSG-38, Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones*; CSTC (mai 2009)