Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI : N° 5, Segmenter et séparer l'information

GESTIONNAIRES

Canada

Avant-propos

La présente est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, envoyez un courriel ou téléphonez au Centre d'appel du Centre pour la cybersécurité :

Centre d'appel

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

La présente publication entre en vigueur le XX novembre XXXX.

Historique des révisions

Version	Modifications	Date
1	Première publication.	XX mois 20XX

D97-1/00-188-2023F-PDF

978-0-660-48517-1

Aperçu

La présente publication fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'*Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)* [1][1]. Une partie des mesures de sécurité des TI consiste à segmenter et à séparer l'information.

Les organisations devraient disposer d'un registre faisant état de leur information opérationnelle essentielle. Les fonds d'informations doivent être classifiés et catégorisés en tenant compte des exigences en matière de protection qu'il convient d'appliquer aux informations sensibles ou aux renseignements personnels. Il est recommandé d'établir les zones des réseaux en segmentant les services d'infrastructure en groupes logiques répondant aux mêmes stratégies de sécurité des communications et aux mêmes exigences en matière de protection de l'information. Ce type de conception logique permet de contrôler et de limiter l'accès de même que les flux de communication de données. Les organisations devraient également surveiller et appliquer les contrôles visant à maintenir la protection et l'intégrité des différentes zones. Pour obtenir de plus amples conseils, prière de consulter les documents que le Centre pour la cybersécurité a préparés à cet effet : *Exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022)* [2] et ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* [3].

Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité des TI recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer s'il convient de prendre des mesures supplémentaires. Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, veuillez communiquer par téléphone ou par courriel avec le :

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

[1] Les numéros entre les crochets renvoient à des références figurant à la section Contenu complémentaire du présent document.

Table des matières

1 Introduction 6

1.1 Les 10 mesures de sécurité des TI 6

1.2 Processus de gestion des risques liés à la sécurité des TI 7

2 Contrôles prenant en charge la segmentation de réseaux 10

2.1 Application du contrôle de flux d'information 10

2.2 Catégorisation de sécurité 10

2.2.1 Établissement de la valeur 11

2.2.2 Classification et catégorisation 11

2.3 Partitionnement des applications 11

3 Segmentation réseau – Introduction 13

4 Segmentation réseau – Mise en pratique 15

4.1 Points à considérer en matière de segmentation 15

4.2 Segmentation sur site 16

4.2.1 Réseau local virtuel (VLAN) 17

4.2.2 Pare-feu 17

4.2.3 Réseau à définition logicielle (réseau SDN) 18

4.2.4 Microsegmentation 18

4.2.5 Enjeux liés à la segmentation réseau 19

4.2.6 Modèle à vérification systématique (MVS) 20

4.3 Segmentation dans le nuage 20

4.3.1 Responsabilités liées à l'établissement de zones dans le nuage 22

4.4 Segmentation aux fins de la technologie opérationnelle 22

5 Résumé 23

6 Contenu complémentaire 24

6.1 Liste des acronymes, des abréviations et des sigles 24

6.2 Glossaire 24

6.3 Références 26

Liste des figures

Figure 1 : Les 10 mesures de sécurité des TI – Nº 5, Segmenter et séparer l'information 7

Figure 2 : Classes et familles de contrôles de sécurité décrites dans l'ITSG-33 9

Liste des tableaux

Tableau 1 : Contrôles de sécurité de l'ITSG-33 liés au contrôle de l'accès : AC-4 27

Tableau 2 : Contrôles de sécurité de l'ITSG-33 liés à la protection des systèmes et des communications : SC-2, SC-3, SC-7, SC-32 32

Tableau 3 : Contrôles de sécurité de l'ITSG-33 liés à l'évaluation des risques : RA-2 37

Liste des annexes

Annexe A Catalogue des contrôles de sécurité de l'ITSG-33 27

A.1 Contrôles de sécurité techniques 27

A.1.1 Contrôle de l'accès 27

A.1.2 Protection des systèmes et des communications 32

A.2 Contrôles de sécurité de gestion 37

A.2.1 Évaluation des risques 37

1 Introduction

Le présent document fournit de l'orientation sur la façon de segmenter vos réseaux en diverses zones de sécurité. La segmentation réseau sépare les biens de technologies de l'information (TI) similaires, comme le matériel, les logiciels et les données, en groupements logiques comportant des stratégies et exigences de sécurité identiques. La segmentation réduit le degré d'exposition de votre organisation aux menaces qui pourraient exploiter des vulnérabilités et compromettre vos réseaux, vos systèmes et vos biens de TI. La présente est fondée sur les conseils formulés dans *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)* [1] et les contrôles de sécurité indiqués dans l'Annexe 3A, *Catalogue de contrôles de sécurité* de l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [4].

1.1 Les 10 mesures de sécurité des TI

Les 10 mesures de sécurité des TI recommandées par le Centre pour la cybersécurité, qui sont mentionnées à la figure 1 ci-dessous, sont fondées sur une analyse des tendances inhérentes aux activités de cybermenace et des répercussions de ces activités sur les réseaux connectés à Internet. Les 10 mesures de sécurité comprennent les mesures prioritaires que votre organisation devrait adopter comme base de référence pour renforcer son infrastructure TI et protéger ses réseaux. Bien qu'il soit recommandé de suivre l'ordre numérique de ces mesures (en commençant par la mesure nº 1) pour accroître vos efforts de protection contre les cybermenaces, vous pouvez changer la séquence des mesures de manière à répondre aux besoins et aux exigences de votre organisation. À mesure que vous ajoutez des mesures de sécurité dans votre environnement, votre exposition aux menaces (c.-à-d., tous les points terminaux disponibles que des auteurs de menace peuvent tenter d'exploiter) diminue, alors que votre posture de sécurité s'améliore.

Il convient de se rappeler que ces mesures ne sont qu'un point de départ et qu'aucune stratégie ne peut à elle seule prévenir tous les cyberincidents. Étant donné l'évolution constante du contexte des cybermenaces, vous devriez veiller à réévaluer vos risques et à revoir les efforts déployés sur le plan de la sécurité de sorte à pouvoir tenir compte de toute lacune ou faiblesse.

Au moment de déterminer vos besoins en matière de sécurité, vous devriez également établir si votre organisation optera pour un modèle sur site ou externalisera la solution à un fournisseur de services gérés (FSG) ou à un fournisseur de services infonuagiques (FSI). Si vous décidez de recourir à un FSG ou à un FSI, vous devriez évaluer les menaces, les vulnérabilités, les responsabilités partagées et les capacités de la plateforme infonuagique afin de pouvoir appliquer les contrôles de sécurité appropriés. La mise en œuvre des 10 mesures de sécurité peut varier selon les types de services utilisés. Par exemple, les rôles et les responsabilités de votre organisation et de votre FSG ou FSI dépendront des services que vous utilisez, ainsi que de vos modèles de services et de déploiement. En revanche, même si elle fait appel à des services infonuagiques ou gérés, votre organisation est toujours responsable sur le plan juridique d'assurer la sécurité de ses données et de rendre des comptes à cet égard. Pour de plus amples renseignements sur la sécurité et les services infonuagiques ou gérés, veuillez consulter *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)* [5], et *Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)* [6].

Figure 1 : Les 10 mesures de sécurité des TI – Nº 5, Segmenter et séparer l'information

1.2 Processus de gestion des risques liés à la sécurité des TI

Les 10 mesures de sécurité des TI du Centre pour la cybersécurité découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [4]. L'ITSG-33 [4] est un cadre de gestion des risques qui décrit les rôles, les responsabilités et les activités permettant à une organisation de gérer les risques relevant de la sécurité des TI. Il comprend un catalogue de contrôles de sécurité, dont un ensemble normalisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI. Ces contrôles de sécurité sont regroupés en trois classes, puis subdivisés en plusieurs familles (ou regroupements) de contrôles de sécurité connexes :

- **Contrôles de sécurité techniques :** contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;

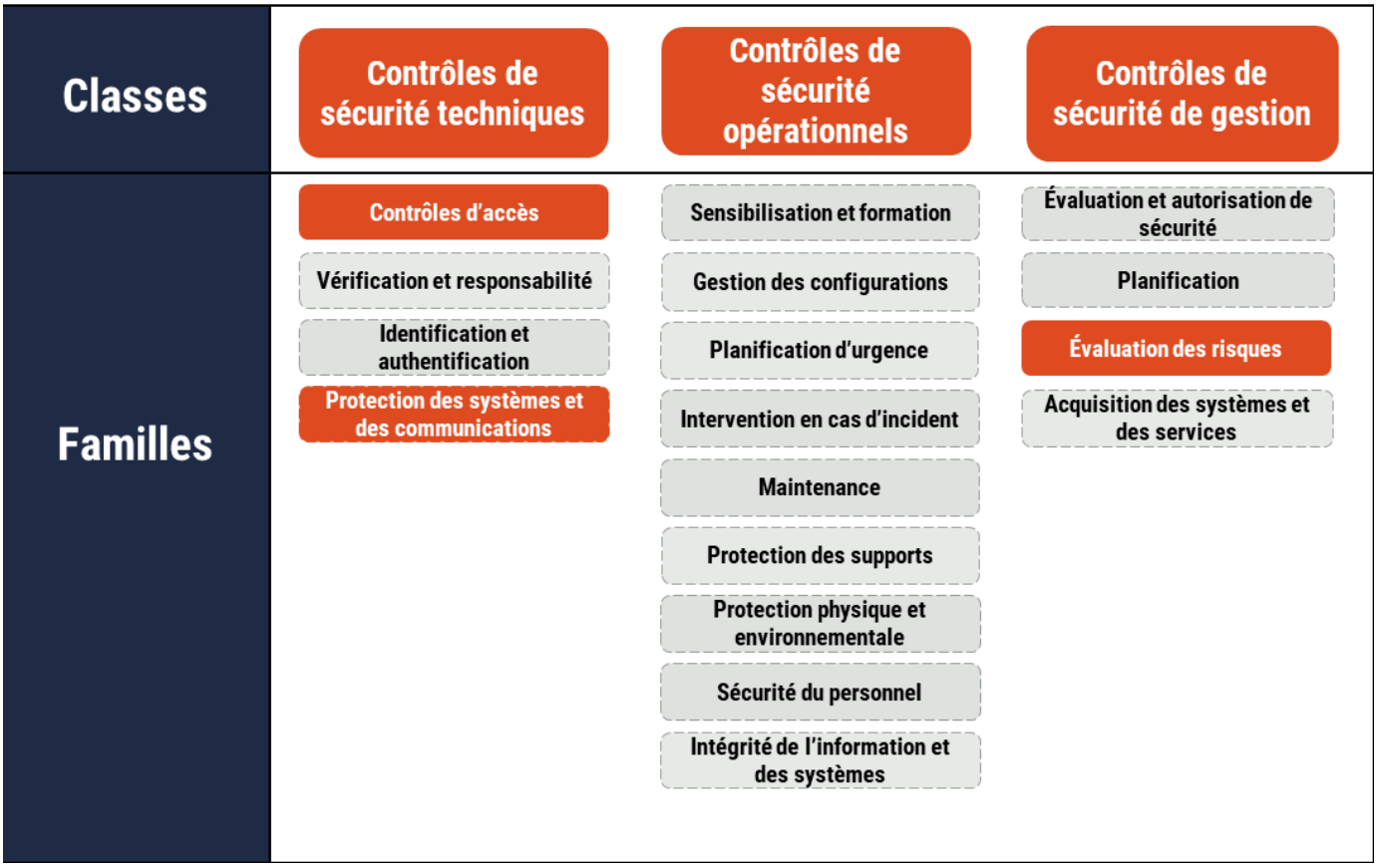
- **Contrôles de sécurité opérationnels :** contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien;
- **Contrôles de sécurité de gestion :** contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Tel qu'il est indiqué à la figure 2, les conseils formulés dans la présente concernent les contrôles de sécurité techniques associés aux familles Contrôle de l'accès (AC pour *Access Control*) et Protection des systèmes et des communications (SC pour *System and Communications Protection*). Ils concernent également les contrôles de sécurité de gestion associés à la famille Évaluation des risques (RA pour *Risk Assessment*). Ce document fait mention de mesures qui permettent de satisfaire les contrôles de sécurité suivants :

- **AC-4 Application des contrôles du flux d'information;**
- **SC-2 Partitionnement des applications;**
- **SC-3 Isolement des fonctions de sécurité;**
- **SC-7 Protection des frontières;**
- **SC-32 Partitionnement des systèmes d'information;**
- **RA-2 Catégorisation de sécurité.**

De plus amples renseignements sur les contrôles AC-4, SC-2, SC-3, SC-7, SC-32 et RA-2 sont fournis à l'annexe A du présent document.

Figure 2 : Classes et familles de contrôles de sécurité décrites dans l'ITSG-33



Vous pouvez utiliser les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [4] pour déterminer la façon de gérer les risques liés à la cybersécurité de votre organisation et de protéger vos réseaux, vos systèmes et vos biens de TI. Il convient toutefois de garder à l'esprit que la mise en œuvre de ces contrôles ne constitue qu'une partie du processus de gestion des risques liés à la sécurité des TI.

L'ITSG-33 [4] décrit un processus fondé sur deux niveaux d'activités de gestion des risques liés à la sécurité des TI, à savoir les activités menées au niveau organisationnel et celles menées au niveau du système d'information. Ces deux niveaux d'activités vous aideront à déterminer les besoins en matière de sécurité pour l'ensemble de votre organisation et pour ses systèmes d'information. Après avoir compris vos besoins pour chaque niveau, vous serez en mesure d'établir les contrôles de sécurité que votre organisation doit mettre en place et maintenir pour satisfaire un niveau de risque acceptable.

2 Contrôles prenant en charge la segmentation de réseaux

2.1 Application du contrôle de flux d'information

Les conseils énoncés dans la présente section sont fondés sur le contrôle **AC-4 Application des contrôles du flux d'information**.

Au moment d'établir des zones de sécurité dans votre environnement, en plus de déterminer qui aura accès aux données qu'elles contiennent, il est également nécessaire de décider quelle information pourra être acheminée d'une zone à l'autre. L'application du flux de l'information entre les zones et à l'intérieur de celles-ci permet à votre organisation de contrôler le flux de données dans l'ensemble de votre réseau. Il sera ainsi possible de veiller à ce que l'information sensible ou classifiée ne puisse pas transiter par vos systèmes à moins que cela ne soit autorisé dans vos règles de segmentation. Les restrictions en matière de contrôle de flux peuvent comprendre le blocage du trafic externe qui prétend provenir de l'intérieur de l'organisation ou la restriction des demandes Web sur Internet qui ne proviennent pas d'un serveur mandataire Web interne. Ce concept s'applique tant à l'établissement de zones traditionnel qui fait souvent appel à des sous-réseaux IP (Internet Protocol) routables, ainsi qu'aux réseaux à définition logicielle (réseau SDN pour *Software-Defined Network*) ou à la segmentation infonuagique que l'on peut appliquer par étiquetage dynamique des stratégies ou des biens.

Votre organisation devrait développer des stratégies de contrôle des flux d'information qui définissent clairement les frontières à travers lesquelles l'information peut transiter depuis vos systèmes d'information ou au sein de ces derniers. Ces stratégies devraient être clairement rédigées, facilement accessibles et révisées fréquemment pour veiller à ce que votre information soit bien protégée. Parmi les stratégies ou les règles de contrôles de sécurité que vous pourriez vouloir mettre en œuvre, on retrouve l'interdiction des transferts d'information entre des systèmes interconnectés ou le recours à du matériel pouvant protéger les flux d'information unidirectionnels dans votre réseau.

Des mécanismes d'application de ces stratégies et règles devraient être mis en place pour contrôler le flux d'information entre des sources et des destinations précises, comme vos réseaux, vos dispositifs et leurs utilisatrices et utilisateurs, à l'intérieur de vos systèmes ou entre ces ceux-ci. Pour y arriver, il est possible d'avoir recours aux contrôles et dispositifs de protection des frontières de votre organisation, comme vos routeurs, vos pare-feu et vos passerelles protégées. Ces contrôles et dispositifs ont été configurés de manière à restreindre les services offerts par les systèmes d'information et à fournir des capacités de filtrage, comme le filtrage de paquets ou de message basé sur des règles ou des paramètres prédéfinis.

2.2 Catégorisation de sécurité

Les conseils énoncés dans cette section sont fondés sur le contrôle **RA-2 Catégorisation de sécurité**.

Sans compréhension exhaustive de l'information que traite et conserve votre organisation, vous ne pouvez pas la protéger complètement. Dans le cadre de vos activités liées à la gestion des risques et à la cybersécurité, vous devriez examiner l'information de votre organisation pour en établir la valeur, la classer en fonction de son niveau de sensibilité et la catégoriser en groupes.

2.2.1 Établissement de la valeur

En établissant la valeur de l'information de votre organisation, vous pouvez classer par ordre de priorité ce qui doit être protégé.

Vous pouvez déterminer la valeur de l'information organisationnelle en évaluant les préjudices possibles pouvant résulter d'une inaptitude à protéger sa confidentialité, son intégrité et sa disponibilité. Lorsque vous déterminez la valeur de l'information, tenez compte des types d'information suivants :

- **Information essentielle aux activités :** Information sur laquelle compte votre organisation pour ses activités courantes, comme l'information sur les ventes ou les plans d'intervention en cas d'urgence;
- **Information sensible :** Information devant rester confidentielle ou à laquelle seules certaines personnes peuvent accéder, comme des données personnelles ou financières ou la propriété intellectuelle;
- **Documents et preuves :** Information devant être protégée contre toute modification non autorisée, comme des contrats ou des reçus.

Pour obtenir de plus amples renseignements sur la façon de déterminer la valeur des biens et des systèmes d'information, prière de consulter *Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)* [7] et la section 2.3 des *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [8].

2.2.2 Classification et catégorisation

Parallèlement à l'établissement de la valeur de l'information organisationnelle, vous devriez également la classer par groupes ou classes en fonction de son niveau de sensibilité. Les mentions de classification qu'applique votre organisation peuvent varier selon que vous faites partie d'un ministère ou d'une organisation non gouvernementale ou privée. La classification appropriée de votre information vous permet de mieux la gérer et de la protéger contre tout accès non autorisé ou toute distribution non autorisée, ainsi que contre une conservation et une élimination inappropriées.

La catégorisation de l'information organisationnelle répond à plusieurs objectifs, comme le démontrent les exemples suivants :

- elle reflète la valeur que votre organisation a attribuée à l'information;
- elle représente la tolérance au risque de l'organisation;
- elle détermine comment votre organisation assure la confidentialité, l'intégrité et la disponibilité de l'information.

Lorsque l'information organisationnelle est correctement classifiée et catégorisée, votre organisation est mieux placée pour la gérer tout au long de son cycle de vie, la conserver et l'éliminer de façon appropriée, ainsi que la protéger contre tout accès et toute distribution non autorisés. De plus, en ayant une bonne connaissance de votre information, vous pouvez mettre en œuvre les contrôles de sécurité appropriés et gérer les risques en fonction de la tolérance au risque définie par votre organisation.

2.3 Partitionnement des applications

Les conseils énoncés dans cette section sont fondés sur le contrôle **SC-2 Partitionnement des applications**.

Il est essentiel de séparer la fonctionnalité de l'utilisateur de la fonctionnalité de gestion du système d'information. La fonctionnalité de gestion du système d'information comprend, par exemple, les fonctions nécessaires à l'administration des bases de données, des composants réseau, des postes de travail ou des serveurs, et exige normalement un accès utilisateur

privilégié. Votre organisation devrait configurer vos systèmes d'information de manière à distinguer les fonctionnalités et privilèges des utilisatrices et utilisateurs des fonctions et privilèges administratifs des systèmes de TI.

Pour déterminer et séparer les fonctions administratives des fonctions non administratives, il convient de tenir compte de ce qui suit :

- les rôles d'utilisateur exigeant un accès aux données sensibles (y compris les utilisatrices et utilisateurs de votre FSI et FSG);
- les responsabilités, l'imputabilité et les tâches associées à chaque rôle d'utilisateur;
- les tâches exigeant des privilèges d'administrateur;
- les utilisatrices et utilisateurs qui doivent effectuer des tâches administratives et sont autorisés à le faire;
- la période (c.-à-d., en permanence ou pour une durée prédéterminée) durant laquelle les utilisatrices et utilisateurs doivent accomplir des tâches administratives (p. ex. tâches permanentes ou urgentes).

Vous devriez interdire aux utilisatrices et utilisateurs avec accès privilégié d'avoir un compte lui accordant à la fois un accès utilisateur normal aux réseaux, dont Internet et les services de courrier, et des privilèges d'administrateur. Les utilisatrices et utilisateurs disposant de privilèges d'administrateur devraient avoir un compte d'administrateur séparé avec des justificatifs d'identité distincts, peu importe l'environnement de votre organisation (en nuage, sur site ou hybride). Assurez-vous que ces comptes d'administrateur ne permettent pas d'accéder à Internet ou aux services de courrier, puisque cela pourrait exposer inutilement votre organisation aux auteurs de menace. Vous devriez mettre en place une stratégie ou une directive pour vous assurer que les tâches administratives sont effectuées sur des ordinateurs administratifs dédiés qui ne peuvent pas accéder à Internet ou aux services de courrier. Pour ce qui est de l'accès à distance, la section AC-17(100) de l'annexe 3A de l'ITSG-33 [4] stipule que l'accès à distance à des comptes privilégiés devrait s'effectuer à partir de consoles de gestion spécialisées régies entièrement par les stratégies de sécurité du système et utilisées exclusivement à cette fin (p. ex. l'accès à Internet n'est pas autorisé). Pour l'administration du nuage à partir de ce poste de travail dédié, il convient d'utiliser un réseau privé virtuel (RPV) ou des listes d'applications autorisées, et de faire appel à l'authentification multifacteur (AMF) pour accéder à l'architecture du nuage.

Pour en savoir plus sur les mesures ci-dessus, prière de consulter *Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094)* [9].

3 Segmentation réseau – Introduction

La segmentation réseau est une approche à la sécurité des TI qui consiste à diviser un réseau en plusieurs segments plus petits afin d'accroître les performances et la sécurité de votre environnement informatique. Elle sépare les biens de TI similaires, comme le matériel, les logiciels et les données, en groupements logiques comportant des stratégies et exigences de sécurité identiques. Plus particulièrement, la segmentation réseau est une technique d'architecture de sécurité qui tire avantage de sous-réseaux ou d'autres méthodes de groupement pour diviser un réseau en des groupes compartimentés distincts et plus petits et permettre à votre organisation de fournir des contrôles de sécurité et des services uniques.

Qu'il s'agisse de sous-réseaux, de l'étiquetage ou d'une autre méthode, l'objectif est d'utiliser le groupe comme son propre réseau distinct dans votre environnement informatique afin que les administratrices ou administrateurs puissent contrôler le flux de trafic entre les groupes définis de manière à se conformer aux stratégies et aux contrôles de sécurité appliqués par votre organisation. Les contrôles de sécurité uniques qui s'appliquent au flux qui transite entre les groupes sont définis dans un point d'interface de zone (PIZ).

Dans une architecture avec zones de sécurité traditionnelles, un PIZ est un système qui surveille et contrôle le flux d'information entre deux zones de sécurité. La ligne de démarcation entre les zones se nomme la frontière. Celle-ci contient des PIZ qui représentent les seuls points de connexion entre les zones. Toutes les données doivent être transmises d'une zone à l'autre par un PIZ qui connecte exclusivement ces deux zones et crée un chemin de communication distinct.

Bien que le concept d'un PIZ soit toujours présent dans les réseaux SDN ou en nuage, on le décrit généralement comme étant une pile composée d'une ou plusieurs appliances virtuelles qui, une fois combinées, permettent de surveiller et de contrôler le flux d'information entre les groupes de biens. Alors que l'architecture traditionnelle des zones de sécurité offre une frontière claire entre les zones où réside le PIZ, on peut y arriver dans un réseau SDN ou en nuage en acheminant virtuellement le trafic à travers la pile de sécurité.

Les conseils formulés dans la présente section sont fondés sur les contrôles de sécurité **SC-3 Isolement des fonctions de sécurité**, **SC-7 Protection des frontières** et **SC-32 Partitionnement des systèmes d'information**.

Le contrôle **SC-3 Isolement des fonctions de sécurité** indique que le système d'information doit isoler les fonctions de sécurité des autres fonctions au moyen d'un périmètre d'isolement. L'isolement renforce le contrôle de l'accès et assure l'intégrité du matériel, des matériels et des micrologiciels de votre organisation. Cette dernière devrait veiller à configurer son réseau de manière à ce que les fonctions liées à la sécurité soient isolées des autres fonctions. Pour permettre à votre organisation de mieux configurer son réseau de manière à isoler les fonctions liées à la sécurité des fonctions non liées à la sécurité, vous devriez faire comme suit :

- mettre en place le principe de droit d'accès minimal qui accorde aux utilisatrices et aux utilisateurs le niveau d'accès minimal requis pour réaliser leurs tâches;
- appliquer des mécanismes de contrôle de l'accès;
- mettre en place des mécanismes de double autorisation pour les tâches administratives et fondamentales;
- appliquer l'AMF dans la mesure du possible (en particulier pour les comptes d'administrateur);
- dédier des postes de travail aux utilisatrices et utilisateurs avec accès privilégié afin qu'ils puissent réaliser des tâches administratives;

- miser sur une administration collaborative lorsque plusieurs administratrices et administrateurs sont nécessaires pour confirmer les opérations administratives;
- faire appel aux mécanismes de séparation matérielle, comme la configuration de domaines de protection hiérarchiques (anneaux de protection) sur vos systèmes d'exploitation;
- mettre en œuvre des technologies de virtualisation pour isoler les processus associés aux fonctions de sécurité;
- configurer des comptes d'administrateur distincts à partir des comptes d'utilisateur avec le niveau d'accès et les privilèges appropriés.

Le contrôle **SC-7 Protection des frontières** indique que le système d'information doit permettre de faire ce qui suit :

- surveiller et contrôler les communications à sa frontière externe et à ses principales frontières internes;
- mettre en œuvre des sous-réseaux pour les composants du système accessibles au public qui sont physiquement ou logiquement séparés des réseaux organisationnels internes;
- se connecter aux réseaux ou aux systèmes d'information externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité de l'organisation.

Le contrôle **SC-32 Partitionnement des systèmes d'information** indique que l'organisation doit partitionner le système d'information en composants de systèmes d'information désignés par l'organisation se trouvant dans des domaines ou environnements physiques distincts en fonction de circonstances propices à la séparation physique des composants définis par l'organisation. La catégorisation de la sécurité peut aider à identifier les composants devant être partitionnés et pouvant être gérés par une interface qui limite ou interdit l'accès au réseau et le flux d'information parmi les composants partitionnés. Dans votre réseau segmenté, on recommande que les applications Web ne puissent pas accéder au réseau ou communiquer avec d'autres systèmes d'information à l'extérieur du sous-réseau ou de la zone dans laquelle elles résident. Il est ainsi possible de renforcer la protection de votre réseau, puisqu'un maliciel arrivant à infecter ou à exploiter les applications ne pourra pas se propager aux autres parties de votre environnement et infecter les autres hôtes ou systèmes.

4 Segmentation réseau – Mise en pratique

La segmentation de vos réseaux en diverses zones de sécurité est un élément de l'approche de défense en profondeur à la cybersécurité. Elle limite l'accès aux systèmes, aux applications, aux dispositifs et aux données qui y sont connectés. La segmentation restreint la communication entre les réseaux, isolant ainsi les données sensibles et empêchant les utilisatrices et utilisateurs non autorisés d'y accéder. Les zones de sécurité de réseau peuvent prendre en charge toute une gamme de solutions de sécurité répondant à vos besoins opérationnels. Ces zones proposent également une infrastructure réseau commune pour assurer la prise en charge de la prestation électronique de services, de l'interconnectivité et de l'interopérabilité. Si votre organisation partage une infrastructure commune pour la prestation électronique de services ou d'autres fins, vous devez vous conformer à toutes les normes de sécurité établies pour l'infrastructure en question.

La segmentation réseau réduit la surface d'attaque, car elle empêche une compromission étendue des réseaux de votre organisation. Advenant la compromission de l'hôte d'un réseau, les hôtes des autres segments du réseau ne sont pas touchés, puisqu'on ne peut les atteindre au-delà des frontières du sous-réseau compromis.

4.1 Points à considérer en matière de segmentation

La segmentation réseau dépend d'une bonne planification et de l'adoption de pratiques exemplaires standards. La liste ci-dessous indique certaines des pratiques exemplaires acceptées par l'industrie que vous devriez mettre en œuvre avant de procéder à la segmentation de vos réseaux dans les zones de sécurité.

- Procéder à l'inventaire de vos données et de vos biens
- Classer vos données et vos biens selon leur valeur (élevée, moyenne ou faible)
- Élaborer et mettre en place des stratégies de sécurité à appliquer à chaque type de données et de biens devant être protégés
    - Le niveau de risque attribué aux données ou aux biens dictera le niveau de sécurité nécessaire pour les protéger, ainsi que les détails de la stratégie de sécurité adoptée
- Appliquer le principe du droit d'accès minimal selon lequel il convient de n'accorder aux utilisatrices et utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches autorisées
    - Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée, incorrecte ou accidentelle d'un système d'information
- Déterminer qui doit accéder à vos données et mettre en place un modèle de contrôle d'accès basé sur les règles (RuBac pour *Rule-Based Access Control*) ou sur les rôles (RBAC pour *Role-Based Access Control*)
- Limiter l'accès des tierces parties à votre réseau pour éviter qu'elles ne créent des points d'entrée additionnels susceptibles d'être exploités par des auteurs de menace
- Identifier le flux de données pour chacune de vos applications et mettre en place une liste d'applications autorisées pour faire en sorte que les applications non approuvées ne puissent pas s'exécuter sur vos systèmes

- Pour de plus amples renseignements sur les listes d'applications autorisées, prière de consulter la publication *Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées (ITSM.10.095)* [10] du Centre pour la cybersécurité

- Surveiller et vérifier votre réseau sur une base continue afin de relever toute anomalie dans les modèles de trafic
  - Pour de plus amples renseignements sur la vérification, la surveillance et la journalisation, prière de consulter les publications *Journalisation et surveillance de la sécurité de réseau (ITSAP.00.085)* [11] et *Vérification de la sécurité des réseaux (ITSAP.80.086)* [12] du Centre pour la cybersécurité
- Mettre en place des capteurs dans chacun des segments de votre réseau pour alerter lors de possibles intrusions
  - Les journaux de ces capteurs devraient être conservés et sauvegardés dans des dispositifs de stockage sécurisés hors ligne

La mise en œuvre de zones de sécurité de réseau devrait convenir aux activités actuelles de votre organisation en matière de gestion des risques liés à la sécurité des TI, notamment à ce qui suit : la définition des besoins organisationnels en matière de sécurité des TI et de contrôles de sécurité, le déploiement des contrôles de sécurité, de même que la surveillance et l'évaluation des performances des contrôles de sécurité. La mise en œuvre devrait également convenir aux activités du niveau des systèmes d'information pour garantir le bon fonctionnement de la solution.

La segmentation réseau peut être mise en œuvre dans divers environnements informatiques. Que votre organisation dispose d'un environnement informatique sur site, en nuage ou hybride, la segmentation de vos réseaux en zones de sécurité permettra d'accroître la sécurité de vos données et de réduire les risques d'accès non autorisé ou de compromission des données.

Les sous-sections ci-dessous proposent de l'information et des pratiques exemplaires sur la mise en œuvre de la segmentation réseau dans un environnement informatique sur site, en nuage ou hybride. Elles fournissent également aux organisations des conseils sur la technologie opérationnelle (TO).

Remarque : Dans le cas des environnements hybrides, il convient de consulter simultanément les conseils formulés dans les sections traitant des environnements sur site et en nuage pour connaître les pratiques exemplaires en matière de segmentation.

4.2 Segmentation sur site

Dans les environnements sur site où l'infrastructure de TI et les éléments de sécurité sont gérés à l'interne, on fait traditionnellement appel à une segmentation basée sur le périmètre. Dans ce modèle, les sous-réseaux et les réseaux externes ne se connectent les uns aux autres que par l'intermédiaire d'interfaces gérées, comme des passerelles, des routeurs ou des pare-feu. Par exemple, un pare-feu peut être mis en œuvre sur une passerelle Internet pour protéger les réseaux internes. On peut également utiliser des pare-feu pour définir et protéger un sous-réseau hébergeant des applications en particulier.

Les sous-réseaux qui séparent physiquement ou logiquement les réseaux externes non fiables des réseaux internes font partie de ce que l'on appelle communément les zones démilitarisées (ZD). Les ZD sont généralement protégées par des pare-feu et défendent les réseaux internes contre les auteurs de menace externes qui cherchent à obtenir un accès non

autorisé. Les interfaces gérées dans la ZD limitent souvent le trafic Web externe vers les serveurs Web organisationnels ou interdissent tout trafic externe qui semble mystifier une adresse interne.

4.2.1 Réseau local virtuel (VLAN)

Un réseau local virtuel (VLAN pour *Virtual Local Area Network*) est une connexion virtualisée qui relie les dispositifs et les nœuds dans l'ensemble de votre réseau. On utilise ce type de connexion pour faciliter la division d'un réseau en sous-réseaux et isoler le trafic provenant des autres VLAN mis en place. Votre organisation peut avoir recours aux VLAN pour l'aider à limiter le trafic en provenance d'autres secteurs de votre environnement et permettre aux sous-réseaux d'établir des connexions et de dépasser votre réseau, peu importe leur emplacement physique.

Vous pouvez améliorer les performances de votre réseau en le segmentant en sous-réseaux et en VLAN, puisqu'ils réduisent le volume du trafic de diffusion en provenance ou en direction de votre réseau.

Les VLAN sont souvent utilisés avec des listes de contrôle d'accès (LCA) pour améliorer le filtrage du trafic sur votre réseau. Votre organisation peut mettre en place des LCA sur vos routeurs et commutateurs pour renforcer sa posture de sécurité des TI. Les LCA permettront d'isoler plus efficacement les dispositifs et les systèmes, aidant ainsi votre organisation à empêcher les auteurs de menace de déployer et de propager des maliciels dans l'ensemble de son réseau.

Remarque : Les VLAN servent aux fins de gestion des adresses IP et bien qu'ils puissent s'avérer utiles pour limiter le trafic de diffusion et permettre la gestion des biens sur le réseau, ils ne sont pas une bonne solution de sécurité pour la séparation des réseaux.

4.2.2 Pare-feu

Les pare-feu (ou les dispositifs dotés des capacités de pare-feu) sont essentiels à la segmentation réseau. Un pare-feu est une barrière de sécurité érigée entre deux réseaux pour contrôler le volume et le type de trafic qui passe d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur. Les pare-feu peuvent se situer physiquement dans le chemin d'accès du trafic réseau (en ligne) ou ce trafic peut tomber sur eux de façon logique en raison des règles de routage appliquées sur le réseau. Avant de les laisser passer, un pare-feu évalue tous les paquets du réseau pour veiller à ce qu'ils soient conformes aux règles établies dans la stratégie et appliquées par l'administratrice ou l'administrateur.

Les pare-feu peuvent également comprendre des fonctions additionnelles, comme un antimaliciel, des capacités de détection et de prévention des intrusions, ou servir à titre de points terminaux du RPV aux fins de la connexion à distance. Tout le trafic transitant par votre pare-feu devrait faire l'objet d'une journalisation détaillée, car ces journaux peuvent fournir de l'information importante sur les modèles du trafic normal et aider à repérer du trafic irrégulier ou malveillant. Les journaux peuvent servir à établir une référence pour les modèles du trafic normal de votre organisation et vous aider à relever les anomalies dans ces modèles. Ces anomalies peuvent être signe d'une activité malveillante. Votre organisation devrait également sauvegarder ses journaux dans un emplacement en lecture seule, comme un autre courriel ou dispositif de stockage hors ligne, pour les protéger de toute compromission par des auteurs de menace.

Les pare-feu peuvent être physiques, comme un appareil matériel, ou virtuels, comme un pare-feu en nuage ou virtuel s'exécutant dans un environnement virtuel. Selon l'architecture et la criticité des systèmes, il pourrait être conseillé d'utiliser plusieurs pare-feu pour sécuriser encore davantage les réseaux critiques. Par exemple, un des pare-feu peut servir de

gardien pour un autre pare-feu dans l'environnement sur site ou hybride. Certaines organisations choisissent également de faire appel à différents fournisseurs lorsqu'ils utilisent plusieurs pare-feu. De cette manière, si un fabricant signale une défaillance ou une vulnérabilité informatique, l'autre pourrait ne pas être touché par les mêmes vulnérabilités.

Si les capacités des pare-feu traditionnels ne sont pas suffisantes, votre organisation pourrait déployer des pare-feu de prochaine génération. Ceux-ci offrent des fonctionnalités avancées, comme le filtrage de contenu à la couche la plus élevée du modèle d'interconnexion de systèmes ouverts (OSI pour *Open System Interconnection*).

4.2.3 Réseau à définition logicielle (réseau SDN)

Le réseau SDN est une approche qui mène à la virtualisation des réseaux. Sur ces réseaux, l'infrastructure du réseau physique est isolée dans une couche de structure et tout le flux de trafic est contrôlé par un ou plusieurs contrôleurs centraux. Le réseau SDN peut être adapté selon votre architecture existante et faciliter la virtualisation de vos réseaux. Il fait appel à des programmes logiciels ou à des interfaces de programmation d'applications (API pour *Application Programming Interface*) pour communiquer avec l'infrastructure de votre organisation et aider à diriger le trafic dans votre réseau segmenté. Comme il est fondé sur un logiciel, le réseau SDN est plus polyvalent que les réseaux traditionnels et permet aux administratrices et administrateurs de gérer et de contrôler plusieurs composants depuis une seule interface. Il est impératif que votre organisation sécurise cette interface, puisqu'elle pourrait constituer un point de défaillance unique s'il était compromis par un auteur de menace.

Par virtualisation, on entend la technologie que votre organisation peut utiliser pour créer des environnements simulés ou des ressources virtuelles, comme des serveurs, des postes de travail, des systèmes d'exploitation, du stockage ou des composants réseau. Elle distingue le poste de travail logique de l'appareil physique. Une utilisatrice ou un utilisateur interagit avec l'ordinateur logique (virtuel) au moyen d'un dispositif connecté au réseau de votre organisation. Ce dispositif peut être un poste de travail ou un appareil mobile possédant son propre bureau distinct. Vous pouvez utiliser des bureaux virtuels pour contrôler de façon centralisée les applications auxquelles les utilisatrices et utilisateurs peuvent accéder depuis leur poste de travail.

Alors que les dispositifs virtualisés peuvent toujours être gérés selon une approche informatique traditionnelle, le réseau SDN exige que les dispositifs soient physiquement connectés à la gestion centrale sous-jacente.

4.2.4 Microsegmentation

Selon les approches traditionnelles à la segmentation réseau, l'accent est mis sur le trafic réseau qui transite entre un client et le serveur de votre organisation. Si les données proviennent de l'extérieur de votre réseau organisationnel, les contrôles de sécurité les filtrent et les acheminent vers le sous-réseau approprié. Il existe toutefois certaines limites, puisque la segmentation traditionnelle ne peut pas surveiller le trafic dans les zones de sécurité de votre réseau. Pour segmenter et surveiller davantage le trafic dans votre réseau, vous pourriez envisager de mettre en œuvre la microsegmentation.

La microsegmentation permet d'assurer une segmentation plus poussée en appliquant des contrôles de sécurité et des protocoles au trafic dans les zones de sécurité de votre réseau. La microsegmentation permet à votre organisation d'isoler des applications en particulier, ce qui signifie qu'advenant la compromission de l'application en tant que telle, la menace ne peut pas se propager aux autres secteurs de votre réseau.

Une microsegmentation divise logiquement les environnements infonuagiques et de centre de donnée en segments de sécurité distincts pouvant aller jusqu'au niveau des charges de travail des individus. Une telle segmentation dépend fortement de l'utilisation de points d'application de stratégies au sein du réseau afin de contrôler dynamiquement les communications entre les composants en fonction de la stratégie. Cela sert à protéger les données et les services sensibles contre les menaces internes et externes. La microsegmentation offre une sécurité multicouche et permet de restreindre l'accès aux biens à un niveau granulaire. On peut ainsi s'assurer que même si des auteurs de menace arrivent à pénétrer dans le réseau, les dommages qu'ils pourront causer seront limités.

Contrairement à la segmentation réseau traditionnelle, qui tire avantage des PIZ pour gérer l'accès aux zones de sécurité du réseau, la microsegmentation peut restreindre l'accès des utilisatrices et utilisateurs à un dispositif ou à un groupe de dispositifs en particulier, ainsi que restreindre l'accès aux points terminaux et aux applications, peu importe le VLAN auquel ils ont été assignés. La direction du flux de trafic constitue une autre des principales différences entre la segmentation traditionnelle et la microsegmentation. La segmentation traditionnelle met l'accent sur le trafic nord-sud qui circule en provenance ou en direction du réseau. La microsegmentation vise à contrôler le trafic est-ouest, qui circule dans une zone de sécurité du réseau ou entre des zones de sécurité similaires. Le fonctionnement de la microsegmentation comporte d'autres différences par rapport à la segmentation traditionnelle, dont les suivantes :

- elle s'applique à des sous-ensembles de composants plus petits qui sont souvent composés d'un seul dispositif;
- elle convient mieux aux réseaux virtuels;
- elle est régie par des stratégies plus granulaires;
- elle est mise en œuvre au niveau logiciel.

4.2.5 Enjeux liés à la segmentation réseau

Segmenter un réseau à des fins de sécurité pose certains défis. Souvent, la segmentation n'a pas besoin de correspondre à l'architecture du réseau. Il peut être difficile et laborieux de refaire l'architecture des réseaux ou de reconfigurer les VLAN et les sous-réseaux afin de répondre aux exigences de la segmentation.

Restructurer les réseaux segmentés dans un environnement informatique déjà établi peut prendre du temps et poser de nombreux défis. Si votre organisation ne dispose pas de l'expertise interne nécessaire, elle pourrait devoir externaliser la reconstruction de son environnement à une professionnelle ou un professionnel de la sécurité des TI. Ces services peuvent être coûteux et hors de prix pour plusieurs organisations dont les ressources sont limitées.

Bien que la segmentation de votre réseau puisse ultimement améliorer ses performances, elle peut aussi avoir des conséquences négatives si elle est mise en œuvre de façon excessive. Une plus grande granularité de la segmentation de vos réseaux pourrait créer un goulot d'étranglement et en ralentir les performances.

La mise en place d'une structure fiable est un autre défi de la segmentation traditionnelle ou basée sur le périmètre. Dans le cas de la segmentation basée sur le périmètre, on fait confiance aux composants qui se trouvent dans le périmètre du réseau et rejette tout ce qui se trouve à l'extérieur de ce périmètre. Bien qu'il s'agisse, dans une certaine mesure, d'une approche efficace à la sécurité, les changements apportés à la technologie et aux environnements informatiques, ainsi que la capacité des auteurs de menace à raffiner leurs méthodes d'attaques, font en sorte qu'il soit nécessaire de mettre en place des règles de fiabilité rigoureuses sur les réseaux.

Une solution à ce défi consiste à appliquer le principe de vérification systématique (en anglais, ZT pour *Zero Trust*) à votre environnement. Fondamentalement, le principe de vérification systématique veille à ce qu'aucune confiance inhérente ne soit accordée par défaut au moindre objet, et ce, qu'il se trouve à l'intérieur ou à l'extérieur de votre environnement. On peut appliquer ce principe à l'architecture de votre organisation en faisant appel au modèle à vérification systématique (MVS ou, en anglais, ZTA pour *Zero Trust Architecture*).

Enfin, les mesures de prévention mentionnées dans les sections précédentes de la présente publication, comme les pare-feu, les LCA, les VLAN, les ZD et les réseaux SDN, présentent toutes des vulnérabilités qui leur sont propres. Que votre équipement soit matériel ou virtuel, les auteurs de menace peuvent employer des méthodes d'attaques courantes comme, entre autres, tenter d'obtenir un accès interne, de contourner les pare-feu et d'exploiter les VLAN. Pour atténuer les risques associés à ces mesures de prévention, votre organisation devrait les passer en revue, les mettre à jour et les reconfigurer de façon régulière.

4.2.6 Modèle à vérification systématique (MVS)

Le principal objectif de la vérification systématique est de faire en sorte qu'il ne soit plus nécessaire de faire appel à des stratégies d'approbation implicites pour assurer le traitement des flux de trafic. La vérification systématique permet également de prévenir les mouvements latéraux dans votre environnement informatique. Le MVS n'a pas pour but d'éliminer la défense des frontières patrimoniale que votre organisation pourrait avoir mise en place.

Il s'assure plutôt que chaque interaction qu'établit une utilisatrice ou un utilisateur à une ressource fasse l'objet d'une authentification et d'une autorisation rigoureuses. Le contrôle et les autorisations d'accès sont mis en œuvre de façon la plus granulaire possible et les décisions prises concernant les accès sont basées sur une évaluation dynamique du contexte de confiance de chaque demande d'accès.

Dans le cadre d'une approche à vérification systématique, les communications entre les utilisateurs, les systèmes et les appareils sont authentifiées, autorisées et validées en continu. La vérification systématique repose sur des contrôles d'accès basés sur les stratégies (PBAC pour *Policy-Based Access Control*), comme les RBAC et les contrôles d'accès basés sur les attributs (ABAC pour *Attribute-Based Access Control*). Un MVS applique les stratégies d'accès en fonction du contexte, tenant compte par exemple du rôle de l'utilisatrice ou de l'utilisateur, du moment de la journée, de la géolocalisation, du dispositif et des données demandées. Le niveau d'accès accordé est ajusté dynamiquement selon le niveau de confiance conféré au sujet. En d'autres mots, plus grande est la confiance qu'un système d'information peut acquérir par rapport à un sujet, plus élevé sera le niveau d'accès accordé à ce dernier.

Pour en savoir plus sur le modèle à vérification systématique, prière de consulter l'*Approche à vérification systématique pour l'architecture de sécurité (ITSAP.10.008)* [13].

4.3 Segmentation dans le nuage

Les principes d'établissement de zones continuent de s'appliquer si votre organisation fait appel à des services infonuagiques ou gérés. Si vous avez recours à un modèle de déploiement infonuagique partagé, par exemple, vous devriez vous assurer que vos données sont séparées de celles appartenant aux autres locataires.

Comme pour la segmentation sur site, la segmentation dans le nuage utilise des PIZ pour décrire l'interface contrôlée qui connecte les deux zones. D'autres mécanismes de segmentation logiques peuvent être employés dans un environnement en nuage. Même s'ils ne répondent pas nécessairement à toutes les exigences fonctionnelles de sécurité d'un PIZ, ces mécanismes peuvent jouer un rôle dans l'établissement de zones dans les réseaux.

Les ressources infonuagiques sont déployées dans ces zones précises. Dans un environnement réseau traditionnel, on s'attend à trouver un PIZ à la frontière d'une zone. Dans un environnement en nuage, un PIZ peut être situé à la frontière d'une zone ou dans une zone associée à des interfaces réseau de ressources infonuagiques précises, comme une machine virtuelle (VM pour *Virtual Machine*) ou un hôte.

Dans un environnement en nuage, la réseautique a évolué et utilise désormais des réseaux SDN. Comparativement à l'approche traditionnelle, un réseau SDN présente différentes caractéristiques et capacités qu'il faut prendre en considération lors de la segmentation d'un environnement en nuage en différentes zones de sécurité réseau.

Voici certaines des principales différences par rapport à une mise en réseau traditionnelle :

1. dissociation du plan de contrôle, qui indique comment le trafic est acheminé dans le réseau SDN, du plan de données des dispositifs, qui gère physiquement le trafic selon les règles imposées par le plan de contrôle;
2. point de provisionnement et de gestion centralisé et unique des configurations;
3. point de contrôle centralisé pour une réglementation rigoureuse de l'information relative à la sécurité et aux stratégies.

Il est important de savoir que même si le FSI offre un accès à la gestion et au plan de contrôle de son réseau SDN, cet accès est offert en faisant appel à l'abstraction des ressources et à une couche de contrôle similaire à celle employée dans le modèle de logiciel-service (SaaS pour *Software as a Service*). Le FSI ne fournit pas un accès direct à ses réseaux SDN ni à leur mise en œuvre sur le plan logiciel ou matériel. Il s'agit d'une partie de sa structure informatique.

Les environnements sur site et en nuage partagent tous deux les mêmes principes de base pour ce qui est de contrôler et de restreindre les accès et le trafic des communications de données à certains composants et utilisatrices ou utilisateurs. Ces deux types d'environnements établissent les périmètres du réseau et les contrôles des frontières connexes au moyen des fonctions suivantes :

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

Pour de plus amples conseils sur l'approche de défense en profondeur et la segmentation, prière de consulter les documents *Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104)* [14] et *Zones de sécurité de réseau en nuage (ITSP.80.023)* [15].

4.3.1 Responsabilités liées à l'établissement de zones dans le nuage

Dans le cas d'un SaaS, le FSI est responsable d'établir les zones de réseau dans l'environnement en nuage. Quant à la plateforme-service (PaaS pour *Platform as a Service*), dans laquelle le FSI héberge généralement plusieurs locataires, les plateformes seront fort probablement sujettes aux pratiques du FSI en matière d'établissement de zones de réseau. Il incombe à votre organisation de s'assurer que les applications SaaS et PaaS respectent la stratégie de sécurité établie, en particulier en ce qui concerne l'établissement de zones de réseau. Les exigences de sécurité devant être respectées par les applications d'entreprise sont tirées de la stratégie de sécurité ou du cadre de gestion des risques de votre organisation. L'ITSG-33 [4] peut également être utilisé à titre de cadre de gestion des risques afin de déterminer les contrôles de sécurité devant être mis en œuvre par votre organisation. La modélisation des menaces, ce qui comprend l'identification de menaces particulières, doit faire partie du cadre de gestion des risques de votre organisation.

Votre organisation devrait restreindre l'accès à son réseau par les fournisseurs de services tiers. Les points d'accès à distance accroissent le nombre de points d'entrée à votre réseau. Les auteurs de menace peuvent exploiter ces points d'entrée et les utiliser comme vecteur d'attaque pour mener des activités malveillantes, comme déployer des maliciels sur votre réseau.

4.4 Segmentation aux fins de la technologie opérationnelle

Plusieurs des pratiques exemplaires en matière de segmentation réseau et des recommandations formulées à la section 2.0 s'appliquent aux environnements de TO. Cela dit, les organisations du secteur des infrastructures essentielles devraient mettre en place certains éléments pour mieux protéger leurs systèmes de TO et leurs systèmes de contrôle industriels (SCI). Il est primordial de séparer la TO de vos TI pour assurer l'efficacité d'une stratégie de cybersécurité. Cette séparation permettra d'assurer le bon fonctionnement des SCI, sans qu'ils aient à être connectés à des réseaux qui pourraient avoir été infectés par des maliciels.

Les pare-feu sont un outil de sécurité efficace et il est fortement recommandé de les mettre en œuvre dans les environnements de TO. Il est possible d'adopter une approche par couche et de les superposer dans l'environnement de TO. Par exemple, un seul pare-feu de TO pourrait sécuriser les connexions en provenance du réseau des TI et les transmettre aux fournisseurs de services externes, tout en isolant l'ensemble du trafic de la ZD. Parallèlement, des stratégies très granulaires peuvent être appliquées aux pare-feu internes pour contrôler les flux entre les réseaux et dispositifs essentiels, comme les systèmes de télésurveillance et acquisition de données (SCADA *Supervisory Control and Data Acquisition*). En règle générale, on recommande d'adopter une approche « Refuser tout » à la connectivité de TO. Votre organisation pourrait ainsi mettre en œuvre des pare-feu pour empêcher un système de communiquer avec les autres systèmes, interdisant du coup toute connectivité ponctuelle ou tout mouvement latéral. Il s'agit d'une autre approche que votre organisation peut adopter pour renforcer sa stratégie défensive et mieux protéger son réseau, ses systèmes et ses données.

5 Résumé

Les biens de TI et l'information de votre organisation sont importants et essentiels à la conduite de ses activités. Ces biens représentent également une cible de choix pour les auteurs de menace. Votre organisation a toujours la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité de vos réseaux, de vos systèmes et de votre information. Vous devriez mettre en œuvre des contrôles de sécurité qui répondent aux exigences opérationnelles et de sécurité de votre organisation.

Une des 10 mesures de sécurité des TI recommandées consiste à segmenter et à séparer l'information. Les conseils formulés dans le présent document sont basés sur plusieurs des contrôles de sécurité détaillés à l'annexe 3A de l'ITSG-33 [4]. Le présent document n'est pas exhaustif. Pour mieux segmenter et séparer votre information, vous devriez passer en revue les conseils formulés dans la présente publication et appliquer les contrôles de sécurité qu'on y aborde. Vous devriez également consulter les autres mesures de sécurité recommandées dans l'ITSM.10.089 [1].

6 Contenu complémentaire

6.1 Liste des acronymes, des abréviations et des sigles

Terme	Définition
ABAC	Contrôle d'accès basé sur les attributs (*Attribute-Based Access Control*)
LCA	Liste de contrôle d'accès
AMF	Authentification multifacteur
API	Interface de programmation d'applications (*Application Program Interface*)
CST	Centre de la sécurité des télécommunications
FSG	Fournisseur de services gérés
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
IE	Infrastructures essentielles
MVS	Modèle à vérification systématique
OSI	Interconnexion de systèmes ouverts (*Open Systems Interconnection*)
PIZ	Point d'interface de zone
RBAC	Contrôle d'accès basé sur les rôles (*Role-Based Access Control*)
RPV	Réseau privé virtuel
RuBAC	Contrôle d'accès basé sur les règles (*Rule-Based Access Control*)
SCI	Système de contrôle industriel
SDN	Réseau à définition logicielle (*Software-Defined Network*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TO	Technologie opérationnelle
ZD	Zone démilitarisée
ZT	À vérification systématique (*Zero Trust*)

6.2 Glossaire

Terme	Définition
Authentification	Processus qui consiste à vérifier l'identité déclarée par ou pour une entité du système [14].
Authentification multifacteur	Mécanisme pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un numéro d'identification personnel [NIP] ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.

Terme	Définition
Autorisation	Privilèges d'accès accordés à une utilisatrice, à un utilisateur, à un programme ou à un processus [15].
Besoin de connaître	Principalement associé aux organisations qui attribuent des niveaux d'habilitation à toutes les utilisatrices et à tous les utilisateurs et des niveaux de classification à tous les biens, le principe du besoin de connaître empêche les utilisatrices et utilisateurs détenant le même niveau d'habilitation d'échanger de l'information à des personnes qui ne prennent pas part aux mêmes initiatives. Passe par la compartimentation. (Glossaire ISC² [en anglais seulement]).
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des biens de TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des stratégies, des pratiques et des procédures de sécurité.
Droit d'accès minimal	Principe selon lequel il convient de n'accorder aux utilisatrices et utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation accidentelle, incorrecte ou non autorisée d'un système d'information.
Frontière	Partie du périmètre d'une zone ou d'un réseau qui sert de point de connexion entre deux zones ou réseaux.
Pare-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur.
Périmètre	Frontière entre deux zones de sécurité de réseau par laquelle le trafic est acheminé.
Périmètre de sécurité	Frontière d'un domaine où s'applique une stratégie ou architecture de sécurité : par exemple, la limite de l'espace dans lequel les services de sécurité protègent les ressources du système [14].
Point d'interface de zone	Interface entre deux zones de sécurité de réseau à travers laquelle le trafic est acheminé.
Réseau privé virtuel	Réseau de communication privé généralement utilisé au sein d'une organisation ou par plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisatrices et utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
Sous-réseau	Portion d'un réseau pouvant constituer un segment physique distinct, qui partage une adresse réseau avec d'autres portions du réseau, dont il se distingue par son numéro de sous-réseau. Le sous-réseau est au réseau ce que le réseau est à l'interréseau.
Surface d'attaque	Ensemble de points sur le périmètre d'un système, d'un élément du système ou d'un environnement par lesquels une attaquante ou un attaquant peut tenter d'entrer, d'extraire des données ou de causer des dommages.
Technologie opérationnelle	Systèmes ou dispositifs programmables qui interagissent avec l'environnement physique (ou gèrent les dispositifs qui interagissent avec un tel environnement). Ces systèmes ou dispositifs détectent ou provoquent un changement direct en misant sur la surveillance et/ou le contrôle des dispositifs, des processus et des événements.
Virtualisation	Technologie qui fait appel aux logiciels pour créer des versions logicielles des systèmes et des services de TI qui étaient traditionnellement mis en œuvre sur du matériel physique distinct. Simulation d'un logiciel ou du matériel utilisé pour exécuter d'autres logiciels.
Zone de sécurité de réseau	Environnement de réseau clairement délimité relevant d'une autorité de zone de sécurité de réseau et caractérisé par un niveau standard de vulnérabilité aux menaces. On distingue les types de zones d'après les exigences de

Terme	Définition
	sécurité s'appliquant aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte et au contrôle de la configuration du réseau.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)*, septembre 2021.
2	Centre canadien pour la cybersécurité. *Exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022)*, janvier 2021.
3	Centre canadien pour la cybersécurité. ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones*, mai 2009.
4	Centre canadien pour la cybersécurité. ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, novembre 2012.
5	Centre canadien pour la cybersécurité. *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*, mars 2019.
6	Centre canadien pour la cybersécurité. *Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)*, octobre 2020.
7	Centre canadien pour la cybersécurité. *Protection de l'information de grande valeur : Conseils pour les petites et moyennes entreprises (ITSAP.40.001)*, avril 2019.
8	Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, février 2020.
9	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI : No 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094)*, juillet 2022.
10	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI : No 10, Mettre en place une liste d'applications autorisées (ITSM.10.095)*, août 2022.
11	Centre canadien pour la cybersécurité. *Journalisation et surveillance de la sécurité de réseau (ITSAP.00.085)*, décembre 2022.
12	Centre canadien pour la cybersécurité. *Vérification de la sécurité des réseaux (ITSAP.80.086)*, décembre 2022.
13	Centre canadien pour la cybersécurité. *Approche à vérification systématique pour l'architecture de sécurité (ITSM.10.008)*, février 2023.
14	Centre canadien pour la cybersécurité. *Guide sur la défense en profondeur pour les services fondés sur l'infonuagique (ITSP.50.104)*, mai 2020.
15	Centre canadien pour la cybersécurité. *Zones de sécurité de réseau en nuage (ITSP.80.023)*, juin 2023.

Annexe A Catalogue des contrôles de sécurité de l'ITSG-33

A.1 Contrôles de sécurité techniques

A.1.1 Contrôle de l'accès

Le tableau 1 décrit le contrôle de l'accès applicable mentionné à l'annexe 3A de l'ITSG-33 [4].

Tableau 1 : Contrôles de sécurité de l'ITSG-33 liés au contrôle de l'accès : AC-4

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AC-4	Application du contrôle de flux d'information	(A) Le système d'information applique des autorisations approuvées pour contrôler le flux d'information dans le système et entre les systèmes interconnectés en fonction des [*stratégies de contrôle de flux d'information définies par l'organisation*].	**Attributs de sécurité des objets :** Le système d'information utilise des [*attributs de sécurité définis par l'organisation*] associés aux [*objets d'information, de source et de destination définis par l'organisation*] pour appliquer les [*stratégies de contrôle de flux d'information définies par l'organisation*] comme base pour les décisions concernant le contrôle de flux. Voir le contrôle de sécurité AC-16 connexe. **Domaines de traitement :** Le système d'information utilise des domaines de traitement protégés pour appliquer les [*stratégies de contrôle de flux d'information définies par l'organisation*] comme base pour les décisions concernant le contrôle de flux. **Contrôle dynamique de flux d'information :** Le système d'information applique le contrôle dynamique de flux d'information en fonction des [*stratégies définies par l'organisation*]. Voir le contrôle de sécurité SI-4 connexe.	AC-3 AC-16 AC-17 AC-19 AC-21 CM-6 CM-7 IA-2 IA-3 IA-4 IA-5 SA-8 SC-2 SC-5 SC-7 SC-18

			Vérification du contenu de l'information chiffrée : Le système d'information empêche l'information chiffrée de contourner les mécanismes de vérification de contenu en [*déchiffrant l'information; bloquant le flux d'information chiffrée; en mettant fin aux sessions de communication qui tentent d'acheminer l'information chiffrée; [procédure ou méthode définie par l'organisation*]]. Voir le contrôle de sécurité connexe SI-4. **Types de données intégrés :** Le système d'information applique les [*restrictions définies par l'organisation concernant l'intégration de types de données dans d'autres types de données*]. **Métadonnées :** Le système d'information applique le contrôle de flux d'information en fonction des [*métadonnées définies par l'organisation*]. Voir les contrôles de sécurité AC-16 et SI-7 connexes. **Mécanismes de flux unidirectionnels :** Le système d'information applique des [*flux unidirectionnels définis par l'organisation*] en utilisant des mécanismes matériels. **Filtres de stratégie de sécurité :** Le système d'information applique le contrôle de flux d'information en utilisant des [*filtres de stratégie de sécurité définis par l'organisation*] comme base pour les décisions de contrôle de flux pour les [*flux d'information définis par l'organisation*]. **Vérifications manuelles :** Le système d'information applique l'utilisation de vérifications manuelles pour les [*flux d'information définis par l'organisation*] selon les modalités suivantes : [*conditions définies par l'organisation*].	SI-3 SI-4 SI-7

			Activation et désactivation des filtres de stratégie de sécurité : Le système d'information permet à une administratrice ou à un administrateur privilégié d'activer ou de désactiver les [*filtres de la stratégie de sécurité définis par l'organisation*] selon les modalités suivantes : [*conditions définies par l'organisation*]. **Configuration des filtres de stratégie de sécurité :** Le système d'information permet à une administratrice ou à un administrateur privilégié de configurer les [*filtres de la stratégie de sécurité définis par l'organisation*] pour appuyer les différentes stratégies de sécurité. **Identificateurs de type de données :** Le système d'information, lors du transfert d'information entre différents domaines de sécurité, utilise des [*identificateurs de type de données définis par l'organisation*] pour valider les données essentielles aux décisions liées au flux d'information. **Décomposition en sous-composantes pertinentes :** Le système d'information, lors du transfert d'information entre différents domaines de sécurité, décompose l'information en [*sous-composantes pertinentes définies par l'organisation*] pour la présenter aux mécanismes d'application de la stratégie. **Contraintes relatives aux filtres de stratégie de sécurité :** Le système d'information, lors du transfert d'information entre différents domaines de sécurité, applique des [*filtres de stratégie de sécurité définis par l'organisation*] qui exigent des formats entièrement énumérés limitant le contenu et la structure des données.	

			Détection de l'information non autorisée : Le système d'information, lors du transfert d'information entre différents domaines de sécurité, examine l'information afin de détecter la présence de [*information non autorisée définie par l'organisation*] et interdit le transfert de cette information, conformément à la [*stratégie de sécurité définie par l'organisation*]. Voir le contrôle de sécurité connexe SI-3. **Authentification des domaines :** Le système d'information identifie de façon unique et authentifie les points source et destination par [*organisation, système, application, personne*] à des fins de transfert d'information. Voir les contrôles de sécurité IA-2, IA-3, IA-4 et IA-5 connexes. **Liaison d'attribut de sécurité :** Le système d'information lie des attributs de sécurité à l'information au moyen de [*techniques de liaison définies par l'organisation*] pour faciliter l'application de la stratégie sur le flux d'information. **Validation des métadonnées :** Le système d'information, lors du transfert d'information entre différents domaines de sécurité, applique le même filtrage de stratégie de sécurité aux métadonnées qu'aux données utiles. **Solutions approuvées :** Les organisations utilisent des [*solutions définies par l'organisation dans les configurations approuvées*] pour contrôler le flux de [*information définie par l'organisation*] dans les domaines de sécurité.	

			Séparation physique et logique des flux d'information : Le système d'information sépare les flux d'information de façon logique ou physique au moyen de [*mécanismes et/ou techniques définis par l'organisation*] pour accomplir les [*séparations requises par type d'information définies par l'organisation*]. **Accès seulement :** Le système d'information fournit à un seul dispositif l'accès aux plateformes informatiques, aux applications ou aux données contenues dans des domaines de sécurité différents tout en empêchant le flux d'information entre les différents domaines de sécurité.	

A.1.2 Protection des systèmes et des communications

Le tableau 2 décrit le contrôle de sécurité de protection des systèmes et des communications applicable mentionné à l'annexe 3A de l'ITSG-33 [4].

Tableau 2 : Contrôles de sécurité de l'ITSG-33 liés à la protection des systèmes et des communications : SC-2, SC-3, SC-7, SC-32

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SC-2	Partitionnement des applications	(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.	**Interfaces pour les utilisatrices et utilisateurs non privilégiés :** Le système d'information empêche la présentation de la fonctionnalité liée à la gestion du système d'information à une interface pour les utilisatrices et utilisateurs non privilégiés. Voir le contrôle de sécurité AC-3 connexe.	AC-3 SA-4 SA-8 SC-3
SC-3	Isolement des fonctions de sécurité	(A) Le système d'information isole les fonctions de sécurité des autres fonctions.	**Structures en couches :** 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.	AC-2 AC-6 SA-4 SA-5 SA-8 SA-13 SC-2 SC-7 SC-39

SC-7	Protection des frontières	(A) Le système d'information surveille et contrôle les communications à sa frontière externe et à ses principales frontières internes. (B) Le système d'information utilise des sous réseaux pour les composants qui sont accessibles au public et qui sont [*physiquement; logiquement*] séparés des réseaux internes organisationnels. (C) Le système d'information se connecte aux réseaux ou aux systèmes d'information externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité de l'organisation.	**Systèmes de télécommunications externes :** i. L'organisation applique une interface gérée à chaque service de télécommunications externe. ii. L'organisation établit une stratégie de flux de trafic pour chaque interface gérée. iii. L'organisation protège la confidentialité et l'intégrité de l'information transmise par l'intermédiaire des interfaces. iv. L'organisation documente chaque exception à la stratégie de flux de trafic en précisant le besoin de la mission ou de l'activité opérationnelle donnant lieu à l'exception et la durée de ce besoin. v. L'organisation examine les exceptions à la stratégie relative aux flux de trafic [*fréquence définie par l'organisation*] et retranche les exceptions qui ne sont plus justifiées par une mission ou par un besoin opérationnel. **Refus par défaut et permission par exception :** Le système d'information, au niveau des interfaces gérées, interdit tout trafic de communication réseau par défaut et ne l'autorise qu'exceptionnellement (c.-à-d., interdit tout trafic, permet le trafic par exception). **Prévention de la tunnellisation à double circuit pour les dispositifs distants :** Le système d'information, en conjonction avec un dispositif éloigné, empêche que celui-ci établisse simultanément des connexions à des ressources locales du système et à d'autres ressources de réseaux externes. **Acheminement du trafic vers les serveurs mandataires authentifiés :** Le système d'information achemine [*trafic de communications interne défini par l'organisation*] vers [*réseaux externes définis par l'organisation*] à travers des serveurs mandataires authentifiés à proximité des interfaces gérées. **Restriction du trafic de communications malveillant sortant :**	AC-4 AC-17 CA-3 CM-7 CP-8 IR-4 RA-3 SC-5 SC-13

			i. Le système d'information détecte et bloque le trafic de communications sortant pouvant constituer une menace aux systèmes externes d'information. ii. Le système d'information vérifie l'identité des utilisatrices et utilisateurs internes associés aux communications bloquées. **Prévention des exfiltrations non autorisées :** L'organisation empêche l'exfiltration d'information non autorisée à travers les interfaces gérées. **Restrictions du trafic de communications entrant :** Le système d'information ne permet que les communications entrantes provenant de [*sources autorisées désignées par l'organisation*] acheminée vers [*destinations autorisées désignées par l'organisation*]. **Protection au niveau de l'hôte :** Les organisations mettent en œuvre [*mécanismes de protection de la frontière au niveau de l'hôte définis par l'organisation*] à [*composants des systèmes d'information désignés par l'organisation*]. **Isolement des outils de sécurité, des mécanismes et des composants de soutien :** L'organisation isole les [*outils, mécanismes et composants de soutien clés de 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. **Protection contre les connexions physiques non autorisées :** L'organisation assure une protection contre les connexions physiques non autorisées à [*interfaces gérées désignées par l'organisation*]. **Prévention de la découverte des composantes et des dispositifs :** Le système d'information empêche la découverte des composants de système particuliers d'une interface gérée.	

			Application automatisée des formats de protocoles : Le système d'information applique la stricte adhésion aux formats de protocoles. **Fonctionnement à sécurité intégrée :** 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. **Blocage des communications provenant d'hôtes non configurés par l'organisme :** Le système d'information bloque le trafic de communications entrant et sortant entre [*clients en communication désignés par l'organisation*] qui est configuré indépendamment par les utilisatrices, les utilisateurs et les fournisseurs de services externes. **Isolement dynamique et séparation :** Le système d'information fournit la capacité d'isoler/de séparer dynamiquement [*composants du système d'information définis par l'organisation*] des autres composants du système. **Isolement des composants de systèmes d'information :** L'organisation emploie des mécanismes de protection de la frontière dans le but de séparer [*composants du système d'information définis par l'organisation*] assurant le soutien aux [*fonctions opérationnelles/missions désignées par l'organisation*]. **Sous-réseaux distincts pour la connexion à des domaines de sécurité différents :** Le système d'information applique des adresses réseau distinctes (p. ex. sous-réseaux différents) pour établir une connexion à des systèmes se trouvant dans des domaines de sécurité différents. **Désactivation de la rétroaction à l'expéditeur après l'échec de validation d'un protocole :**	

			Le système d'information désactive la fonction de rétroaction à l'expéditeur lorsqu'il y a échec de la validation d'un format de protocole.	
SC-32	Partitionnement des systèmes d'information	L'organisation partitionne le système d'information en [*composants de systèmes d'information désignés par l'organisation*] se trouvant dans des domaines ou environnements physiques distincts en fonction de [*circonstances propices à la séparation physique des composants définis par l'organisation*].	Aucune	AC-4 SA-8 SC-2 SC-3 SC-7

A.2 Contrôles de sécurité de gestion

A.2.1 Évaluation des risques

Le tableau 3 décrit le contrôle de sécurité d'évaluation des risques applicable mentionné à l'annexe 3A de l'ITSG-33 [4].

Tableau 3 : Contrôles de sécurité de l'ITSG-33 liés à l'évaluation des risques : RA-2

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
RA-2	Catégorisation de sécurité	(A) L'organisation catégorise l'information et les systèmes d'information conformément aux lois du GC et aux prescriptions du SCT. (B) L'organisation documente les résultats de la catégorisation (y compris les justifications) dans le plan de sécurité du système d'information. (C) L'organisation s'assure que la décision concernant la catégorisation de sécurité est examinée et approuvée par l'autorité responsable ou par son représentant désigné.	Aucune.	CM-8 MP-4 RA-3 SC-7