



Guide de la sécurité matérielle
Publication de l'organisme-conseil G1-031

Protection matérielle des serveurs informatiques

Sous-direction de la sécurité technique
Direction des opérations techniques
Gendarmerie royale du Canada
Date de publication : Mars 2008

Vous pouvez faire des suggestions et des commentaires concernant le présent guide en vous adressant à l'officier responsable de la Sous-direction de la sécurité technique, Opérations techniques, Gendarmerie royale du Canada (GRC), 1426 boul. Saint-Joseph, Ottawa (Ontario) K1A 0R2

© (2008) SA MAJESTÉ LA REINE DU CHEF DU CANADA
représentée par la Gendarmerie royale du Canada (GRC), Ottawa, Canada K1A 0R2

La présente publication peut être reproduite intégralement sans frais à des fins éducatives et personnelles seulement. Toutefois, l'autorisation écrite de la GRC est requise pour utiliser ce document sous forme révisée ou d'extraits, ou à des fins commerciales.

TABLE DES MATIÈRES

| | | |
|----------|---|----------|
| 1 | Introduction | 1 |
| 1.1 | Objet et portée | 1 |
| 1.2 | Rôles et responsabilités..... | 1 |
| 1.3 | Méthodologie | 1 |
| 1.4 | Résumé des risques | 2 |
| 2 | Sécurité matérielle des salles de serveurs | 3 |
| 2.1 | Exigences minimales | 3 |
| 2.2 | Emplacement de la salle des serveurs | 5 |
| 2.3 | Salle de serveurs partagée | 5 |
| 3 | Résumé et recommandations | 6 |
| 4 | Conseils et orientations..... | 6 |
| 5 | Références | 6 |
| | Annexe A – Mesures de protection | 1 |
| 1. | Salle de serveurs verrouillée..... | 1 |
| 2. | Verrouillage du serveur..... | 1 |
| 3. | Salle de serveurs protégée | 2 |
| 4. | Centre de données protégé | 2 |
| | Annexe B - Exemples de salles de serveurs satisfaisant aux exigences de base | 1 |
| | Exemple B1 | 1 |
| | Exemple B2 | 1 |
| | Exemple B3 | 2 |
| | Exemple B4 | 2 |
| | Exemple B5 | 3 |
| | Exemple B6 | 3 |
| | Exemple B7 | 4 |
| | Exemple B8 | 4 |
| | Exemple B9 | 5 |

1 Introduction

L'un des biens importants que détiennent les ministères¹ du gouvernement est l'information qu'ils enregistrent et traitent sur une base quotidienne. Cette information doit être protégée contre les menaces pour la confidentialité, la disponibilité et l'intégrité. Dans le passé, l'information était principalement consignée sous forme de documents « papier ». Diverses lignes directrices et exigences ont été établies pour l'entreposage de l'information conservée sous cette forme. Aujourd'hui, l'information est également enregistrée et stockée sur des supports électroniques. L'élément le plus précieux d'un système d'information électronique est l'information qui est enregistrée dans des dispositifs réseau, comme les contrôleurs de domaine, les serveurs de fichiers, de même que les serveurs de réseau de stockage (SAN), les serveurs de stockage en réseau (NAS) et les serveurs de sauvegarde. Pour simplifier, nous utiliserons le terme « serveur » pour désigner l'ensemble de ces dispositifs.

1.1 Objet et portée

Ce document a pour objet de fournir des lignes directrices pour la protection matérielle des serveurs informatiques utilisés pour stocker de l'information classifiée et protégée.

La portée de ce guide se limite à la protection matérielle des serveurs contre les accès non autorisés. Les ministères doivent aussi assurer une protection contre les incendies, les fuites d'eau, les séismes, les pannes d'électricité, les excès de température et l'humidité. En outre, les ministères équipés de serveurs qui traitent des renseignements d'origine électromagnétique (SIGINT) doivent contacter le Centre de la sécurité des télécommunications (CST) pour obtenir des conseils sur la sécurité matérielle, la sécurité des TI et la sécurité des émissions, sécurité qui pourrait nécessiter des mesures supplémentaires d'isolement physique et l'établissement de zones.

1.2 Rôles et responsabilités

L'agent de sécurité du ministère (ASM) et le coordonnateur de la sécurité des TI (CSTI) doivent s'assurer que les responsables de la sécurité matérielle, du personnel et des TI coordonnent leurs efforts pour protéger les actifs d'information et de TI et adoptent une approche intégrée et équilibrée.

Les gardiens doivent incorporer les exigences des locataires dans l'infrastructure de base des immeubles. Lorsqu'un ministère détermine que la méthode la plus efficace pour protéger les serveurs contre les accès non autorisés nécessite des modifications qui ne relèvent pas du contrôle des locataires, le gardien doit coordonner les mesures requises par le ministère. Le ministère demeure responsable du coût des modifications, y compris l'entretien continu et les réparations nécessaires.

1.3 Méthodologie

La [Politique du gouvernement sur la sécurité](#) définit la sécurité des technologies de l'information comme les « mesures de sauvegarde visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique ». Ce document décrit les mesures de sécurité matérielle requises selon le niveau de confidentialité de l'information, et ne constitue qu'une partie du processus d'analyse du risque pour la sécurité des TI. Les ministères doivent aussi évaluer leurs exigences en matière d'intégrité et de disponibilité, et mettre en place les mesures de protection supplémentaires nécessaires. Dans ce document, des niveaux de protection progressivement plus élevés sont prescrits selon la sensibilité de l'information enregistrée dans

¹ Pour les besoins du présent document, le terme « ministère » englobe les ministères, les organismes et toutes les autres entités régis par la Politique du gouvernement sur la sécurité.

le serveur. Les ministères devraient déterminer s'ils ont besoin de mesures de protection renforcées ou supplémentaires en procédant à une évaluation interne de la menace et des risques.

Les vulnérabilités, tant logiques² que physiques, sont plus faciles à exploiter lorsque les serveurs ne sont pas protégés contre les accès physiques non autorisés. Pour atténuer ce risque, les mesures de sécurité matérielle doivent reposer sur le concept de la protection, de la détection et de l'intervention. Ce document décrit les exigences minimales de protection et de détection qui permettront de réduire le risque d'accès physique non autorisé. Les ministères doivent s'assurer de pouvoir intervenir adéquatement en cas de détection d'un accès physique non autorisé.

Il est possible d'assurer une protection contre l'accès physique non autorisé en plaçant le serveur dans un conteneur (armoire). Les serveurs peuvent être placés individuellement ou en petit nombre dans des conteneurs comme ceux qui sont listés dans le [Guide d'équipement de sécurité \(G1-001\)](#). Lorsqu'il faut protéger de nombreux serveurs, l'utilisation de conteneurs approuvés peut devenir peu pratique. Les serveurs devraient alors être placés dans des salles de serveurs construites conformément aux exigences énumérées dans le Tableau 1 et décrites à l'Annexe A.

Les moyens de détection décrits dans ce document visent à identifier les accès physiques non autorisés aux serveurs. Ces mesures ne permettent pas de détecter les activités non autorisées des utilisateurs autorisés. Les ministères doivent s'assurer que ceux qui détiennent des droits d'accès ont un réel besoin d'accès et possèdent l'autorisation de sécurité appropriée. Les ministères devraient également contacter leur CSTI ou ASM pour obtenir des lignes directrices et/ou de l'aide afin de prévenir et de détecter les activités logiques non autorisées sur les serveurs.

On trouvera des renseignements supplémentaires dans le guide [Protection, détection et intervention \(GRC G1-025\)](#).

1.4 Résumé des risques

Les mesures de protection décrites dans ce document ont été sélectionnées afin de contrer deux menaces de probabilité moyenne. La première est la perte de confidentialité due à un accès non autorisé découlant du vol d'un serveur. Bien que les serveurs aient une valeur de revente relativement faible, l'on a relevé des cas de serveurs volés et revendus. Les serveurs peuvent être volés pour l'information qu'ils contiennent ou tout simplement pour leur valeur financière. Le coût de remplacement du serveur lui-même est insignifiant comparativement à la divulgation d'information confidentielle. Le vol de serveur est généralement perpétré lors d'une attaque « à faible niveau de compétences ».

La seconde menace est la perte de confidentialité découlant de la divulgation d'information à une personne non autorisée qui dispose d'un accès physique au serveur. Cela diffère de la menace de type « piratage informatique » qui relève de la section responsable de la sécurité des TI. Dans la plupart des cas, les pirates informatiques tentent d'exploiter à distance des vulnérabilités logiques. Cependant, certaines vulnérabilités des serveurs sont parfois plus faciles à exploiter lorsque l'accès physique au serveur (l'unité physique comme telle) est possible. Il faut également examiner comment l'installation non autorisée d'un dispositif « malveillant » pourrait permettre une attaque combinée (à la fois physique et logique). Par exemple, une personne de l'intérieur pourrait brancher un enregistreur de frappe matériel

² Les vulnérabilités « logiques » découlent de la façon dont les données ou les systèmes sont organisés. Le contrôle de l'accès logique désigne l'ensemble des politiques, des structures organisationnelles et des procédures, comme l'identification, l'authentification et l'autorisation, qui visent à restreindre l'accès aux logiciels et aux fichiers informatiques. Il diffère du contrôle de l'accès physique, ou matériel, qui limite la capacité d'interagir physiquement avec les serveurs.

sur un serveur pendant une certaine période de temps, puis le débrancher ultérieurement. Il serait ensuite possible d'utiliser l'information ainsi saisie pour lancer une attaque logique/à distance via le réseau ou Internet. Ce type d'attaque nécessite un niveau de compétence moyen.

2 Sécurité matérielle des salles de serveurs

2.1 Exigences minimales

Le Tableau 1 présente les mesures de protection minimales requises pour une salle de serveurs réservée exclusivement à un ministère et ne contenant que des serveurs utilisés par ce ministère. Ces mesures de protection sont décrites à l'Annexe A. Les salles de serveurs nécessitent des mesures de protection supplémentaires lorsqu'elles contiennent des serveurs et/ou d'autres équipements de télécommunications appartenant à plusieurs ministères. Ces mesures sont décrites dans la section 2.3 et illustrées à l'Annexe B, exemples B4, B8 et B9.

Les mesures de protection spécifiées dans le Tableau 1 varient selon la sensibilité de l'information enregistrée dans le serveur et la zone depuis laquelle le serveur (la salle) est accessible. On trouvera des renseignements sur les zones de sécurité dans le guide [Établissement des zones de sécurité matérielle \(GRC G1-026\)](#).

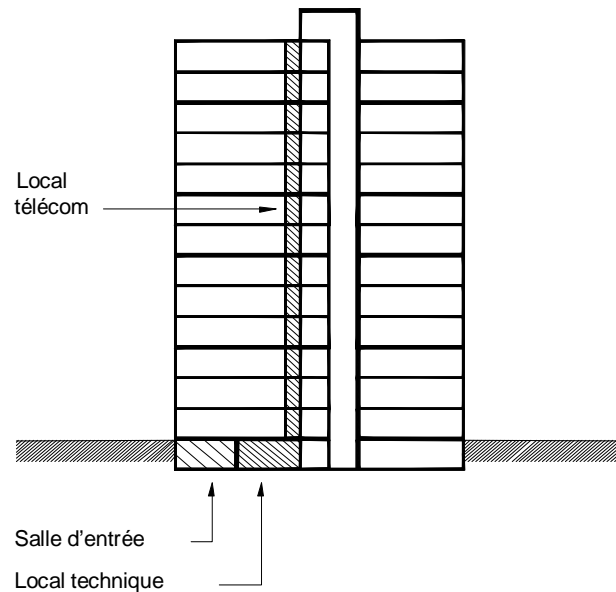
| Niveau maximum de classification de l'information | Mesures de protection minimales (voir l'Annexe A) | Exemples de zones (voir l'Annexe B) |
|---|---|-------------------------------------|
| PROTÉGÉ A | Aucune mesure de protection supplémentaire pour les serveurs situés dans une <i>zone de travail</i> ou d'un niveau de sécurité supérieur | |
| | OU Salle de serveurs verrouillée (1) | B1 |
| PROTÉGÉ B | Salle de serveurs verrouillée (1) | B2 |
| | OU Verrouillage des serveurs (2) situés dans une <i>zone de travail</i> ou d'un niveau de sécurité supérieur | |
| | OU Salle de serveurs protégée (3) | B1 |
| PROTÉGÉ C | Salle de serveurs protégée (3) | B3 |
| | OU Centre de données protégé 24/7 | B6 |
| | OU Centre de données protégé | B7 |
| CONFIDENTIEL | Centre de données protégé 24/7 (4) | B5 |
| | OU Centre de données protégé | B6 |
| | OU Salle de serveurs protégée (3) | B2 |
| | OU Salle de serveur verrouillée (1) | B3 |
| | OU Verrouillage des serveurs (2) situés dans une <i>zone de travail</i> ou d'un niveau de sécurité supérieur | |
| SECRET | Centre de données protégé 24/7 (4) | B5 |
| | OU Salle de serveurs protégée (3) | B3 |
| | OU Centre de données protégé (4) | B7 |
| | OU Conteneur listé dans le Guide d'équipement de sécurité lorsque le serveur est situé dans une <i>zone de sécurité</i> ou d'un niveau de sécurité supérieur | |
| TRÈS SECRET | Centre de données protégé 24/7 (4) | B6 |
| | OU Salle de serveurs protégée (3) | B3 |
| | OU Centre de données protégé (4) | B7 |

Tableau 1

2.2 Emplacement de la salle des serveurs

Dans de nombreux immeubles, l'endroit le plus pratique où installer les serveurs est le local principal des télécommunications, maintenant appelé « local technique principal de télécommunications » (anciennement appelé « salle principale de raccordement de l'équipement »). Ce local est souvent accessible depuis une *zone d'accès public*. Il peut être utilisé à la condition que les mesures de protection minimales décrites ici soient appliquées. Il ne faut pas confondre le local technique principal de télécommunications et la salle d'entrée des télécommunications. La salle d'entrée sert de terminal permettant au câblage appartenant à diverses entreprises de télécommunications de pénétrer dans l'immeuble depuis la rue. Les équipements appartenant aux entreprises de télécommunications servant le bâtiment peuvent aussi être installés dans cette pièce.

Les compagnies de téléphone et autres fournisseurs de services de télécommunications ont donc besoin d'accéder à la salle d'entrée. Pour que des serveurs soient installés dans le local technique principal des télécommunications (ou dans toute autre pièce), il faut que l'accès à la pièce soit contrôlé par la Couronne. En d'autres termes, cette pièce doit essentiellement être une *zone de travail* ou d'un niveau de sécurité supérieur.



Coupe transversale de l'immeuble

2.3 Salle de serveurs partagée

Les installations gouvernementales peuvent souvent servir plusieurs organisations. Dans la plupart des cas, il est plus économique de regrouper des serveurs appartenant à différentes organisations dans le même local afin de profiter d'économies d'échelle. En outre, les besoins d'espace d'une organisation peuvent varier de temps à autre à l'intérieur d'une installation. Une salle de serveurs partagée permet de tels changements sans qu'il soit nécessaire de changer de local chaque fois qu'on modifie les secteurs occupés par les locataires.

Cependant, les salles de serveurs partagées peuvent entraîner des vulnérabilités supplémentaires. Le fait de partager une salle de serveurs avec d'autres organisations accroît le risque pour les serveurs, car la probabilité de compromission augmente en fonction du nombre de personnes qui ont accès à la pièce. Les utilisateurs de salles de serveurs partagées doivent donc établir une politique conjointe sur les privilèges d'accès et les autorisations de sécurité nécessaires. Les organisations devraient ensuite évaluer le risque accru et envisager d'appliquer les mesures de protection décrites à l'Annexe A aux serveurs contenant de l'information classifiée ou protégée. Les locaux techniques de télécommunications qui abritent des serveurs devraient être traités comme des salles de serveurs partagées. Les salles de serveurs partagées sont illustrées à l'Annexe B.

Les grands centres de données partagés par plusieurs organisations comportent aussi des exigences supplémentaires, notamment lorsqu'un centre de données est trop vaste pour permettre aux personnes se

trouvant dans la pièce de surveillance de surveiller adéquatement l'accès aux serveurs. Dans un tel cas, les serveurs devraient être protégés comme s'ils étaient situés dans la *zone de sécurité* d'un même ministère (voir le Tableau 1 et l'Annexe B).

3 Résumé et recommandations

Les exigences énoncées dans la Section 2 font appel à diverses solutions de rechange pour assurer la protection matérielle des serveurs informatiques. Les ministères doivent déterminer le moyen le plus économique de satisfaire à ces exigences. Ils devraient aussi tenir compte des mesures de protection contre les incendies, les fuites d'eau, les séismes, les pannes d'électricité, les excès de température et l'humidité. Si l'on tient compte des mesures de protection telles que les génératrices auxiliaires et les appareils de climatisation, il peut être plus économique de regrouper ses serveurs avec ceux d'une autre organisation dans la même salle de serveurs ou le même centre de données afin de profiter d'économies d'échelle. Certains aménagements recommandés de salles de serveurs et de centres de données partagés sont illustrés à l'Annexe B.

4 Conseils et orientations

Si vous désirez obtenir des conseils et de l'aide sur le présent guide ou sur des questions propres au site qui ne sont pas abordées ici, veuillez communiquer avec le service suivant :

Services à la clientèle, Sous-direction de la sécurité technique
Gendarmerie royale du Canada
1426, boul. Saint-Joseph
Ottawa (Ontario) K1A 0R2
Courriel : TSB-ClientServices@rcmp-grc.gc.ca

5 Références

Politique du gouvernement sur la sécurité

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp

Norme opérationnelle sur la sécurité matérielle

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm_f.asp

Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_f.asp

Guide d'équipement de sécurité (GRC G1-001)

http://www.rcmp-grc.gc.ca/tsb-genet/seg/html/home_f.htm

Protection, détection et intervention (GRC G1-025)

Établissement des zones de sécurité matérielle (GRC G1-026)

Pièces sécuritaires (GRC G1-029)

<http://www.rcmp-grc.gc.ca/ts-st/pubs/phys-sec/index-fra.htm>

Annexe A – Mesures de protection

Voici la description des mesures de sécurité matérielle énumérées dans le Tableau 1 :

1. Salle de serveurs verrouillée

Placer le serveur dans une salle distincte et contrôler l'accès à cette pièce. Limiter l'accès aux personnes qui ont un besoin opérationnel ou relié à leur travail;

La pièce devrait être dotée de murs construits de la dalle du plancher à la sous-face du plafond/dalle de plancher de l'étage supérieur. Les pièces dont les murs sont construits jusqu'à la sous-face d'un plafond suspendu ne sont pas conformes à la définition d'une « salle de serveurs verrouillée »;

On peut utiliser divers moyens pour contrôler l'accès, notamment des serrures mécaniques à clé ou des lecteurs de cartes électroniques. De plus, de nombreux systèmes comprennent une piste de vérification permettant d'identifier qui a accédé à la pièce et quand. Pour plus de renseignements, voir [Contrôle de l'accès \(GRC G1-024\)](#).

2. Verrouillage du serveur

On peut verrouiller les serveurs à l'aide d'une variété de méthodes qui permettent d'en contrôler l'accès. On trouvera ci-après des exemples de la façon dont un serveur peut être verrouillé pour se conformer aux exigences de ce guide.

Un serveur peut être considéré comme étant « verrouillé » lorsqu'une protection physique est appliquée à l'unité (boîte) elle-même. Il s'agit de dispositifs qui sont installés directement sur le serveur, notamment :

- a. Serrure de couvercle pour prévenir l'intrusion physique dans le serveur;
- b. Serrures d'unité pour empêcher l'accès au lecteur de disquettes et/ou au lecteur de CD-ROM;
- c. Dispositifs conçus pour protéger toutes les sources possibles d'entrée/sortie, comme les ports USB, les ports série, les interfaces réseau, les ports ps/2, etc.;
- d. Plaques ou câbles d'ancrage qui fixent le serveur au bâti ou à la table où il est installé.

Un serveur peut aussi être considéré comme étant verrouillé s'il est placé dans une cage verrouillée à l'intérieur d'une salle de serveurs (voir l'exemple B4, Annexe B). Il peut être plus facile d'assurer la circulation de l'air à des fins de refroidissement en subdivisant une pièce à l'aide de cages au lieu de cloisons fixes. Les cages verrouillables peuvent incorporer des dispositifs distincts de contrôle de l'accès et de détection des intrusions, en plus des dispositifs installés pour contrôler l'accès à la salle des serveurs. On peut aussi utiliser des caméras pour surveiller l'accès aux zones contenant des cages.

Un serveur peut aussi être considéré comme étant verrouillé lorsqu'il est placé dans une armoire verrouillable. L'armoire peut incorporer des dispositifs de sécurité supplémentaires. La porte de l'armoire peut être équipée d'un contact indiquant quand la porte est ouverte. Un détecteur de mouvement peut être installé dans l'armoire. Une caméra d'équipement vidéo en circuit fermé peut aussi être installée à l'intérieur ou à l'extérieur de l'armoire.



Exemple d'armoires verrouillables pour serveurs

Un serveur peut aussi être considéré comme étant verrouillé lorsqu'il est placé dans un contenant listé dans le [Guide d'équipement de sécurité \(GRC G1-001\)](#).

3. Salle de serveurs protégée

Pour les besoins de ce guide, une « salle de serveurs protégée » est une pièce dont les murs, la porte et la quincaillerie (serrures) sont conformes à la spécification de pièce sécuritaire 1. La construction de la pièce sécuritaire 1 est décrite dans le guide [Pièces sécuritaires \(GRC G1-029\)](#).

La salle doit aussi être surveillée à l'aide d'un système électronique de détection des intrusions.

La pièce devrait être surveillée au moyen d'équipement vidéo en circuit fermé lorsque cette mesure est recommandée par une évaluation de la menace et des risques. L'équipement vidéo en circuit fermé peut décourager les accès non autorisés, tout en fournissant un enregistrement visuel des activités aux environs d'un serveur. Les caméras devraient être positionnées de manière à enregistrer les personnes qui accèdent au serveur, ainsi que la date et l'heure, mais pas d'information sensible ou protégée, tels les mots de passe.

4. Centre de données protégé

La salle des serveurs peut être surveillée par des employés se trouvant dans une salle de contrôle adjacente, séparée par un mur vitré. Pour les besoins de ce guide, cette configuration de pièces constitue un « centre de données protégé ». Le vitrage devrait permettre d'observer les serveurs. Les zones qui échappent à l'observation devraient être surveillées par des caméras. L'aménagement devrait permettre d'observer quiconque entre dans la pièce, et comporter un point de contrôle où les personnes qui pénètrent dans la pièce doivent signer et produire une pièce d'identité.

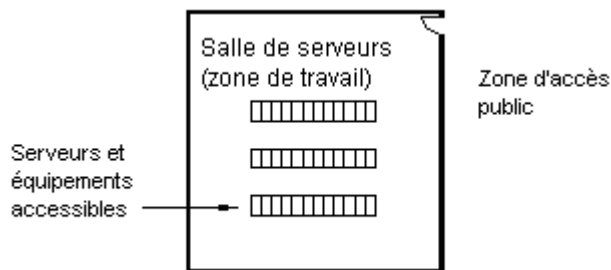
Le périmètre d'un centre de données protégé doit être conforme à toutes les exigences de construction d'une salle de serveurs protégée.

La salle de surveillance doit être occupée durant les heures où l'accès aux serveurs est autorisé. Lorsque « 24/7 » est indiqué, la salle de contrôle doit être occupée continuellement. Les centres de données protégés sont illustrés à l'Annexe B.

Annexe B - Exemples de salles de serveurs satisfaisant aux exigences de base

Voici des exemples types de salles de serveurs qui satisfont aux exigences énoncées dans ce guide :

Exemple B1

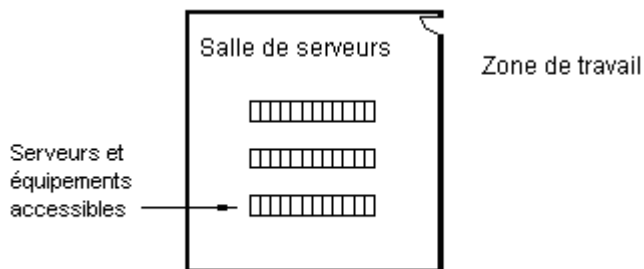


Cette salle de serveurs remplit les conditions d'une **zone de travail** si l'accès est limité aux employés qui doivent travailler sur les serveurs ou sur les équipements qu'ils contiennent.

Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé A** lorsque les mesures de protection décrites à la section « 1. Salle de serveurs verrouillée » de l'Annexe A sont appliquées.

Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** lorsque les mesures de protection décrites à la section « 3. Salle de serveurs protégée » de l'Annexe A sont appliquées.

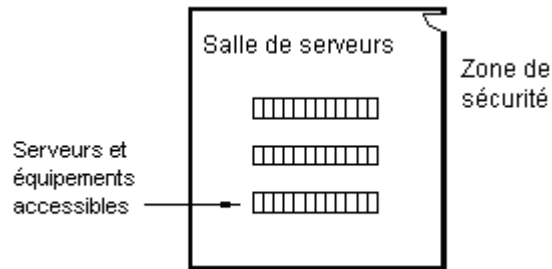
Exemple B2



Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** lorsque les mesures de protection décrites à la section « 1. Salle de serveurs verrouillée » de l'Annexe A sont appliquées et que la pièce est située à l'intérieur d'une **zone de travail** ou d'un niveau de sécurité supérieur.

Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** et de l'information **classifiée** jusqu'au niveau **Confidentiel** lorsque les mesures de protection décrites à la section « 3. Salle de serveurs protégée » de l'Annexe A sont appliquées.

Exemple B3

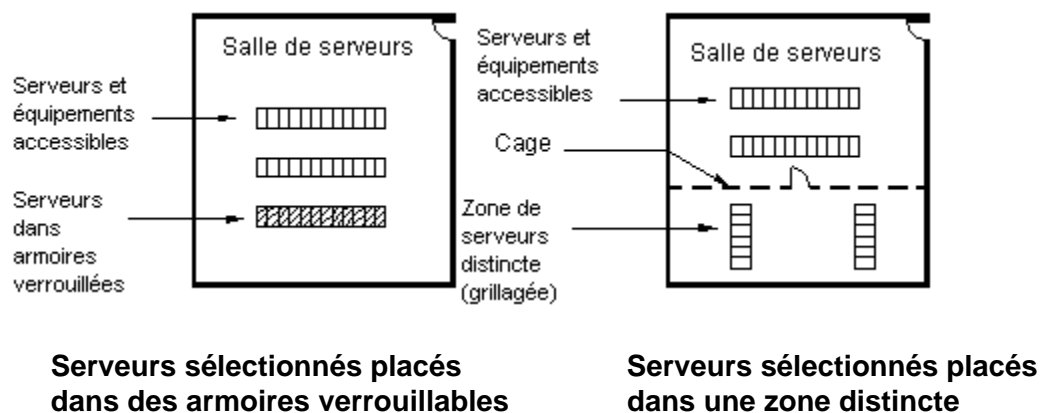


Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** et de l'information **classifiée** jusqu'au niveau **Confidentiel** lorsque les mesures de protection décrites à la section « 1. Salle de serveurs verrouillée » de l'Annexe A sont appliquées et que la pièce est située dans une *zone de sécurité* ou d'un niveau de sécurité supérieur.

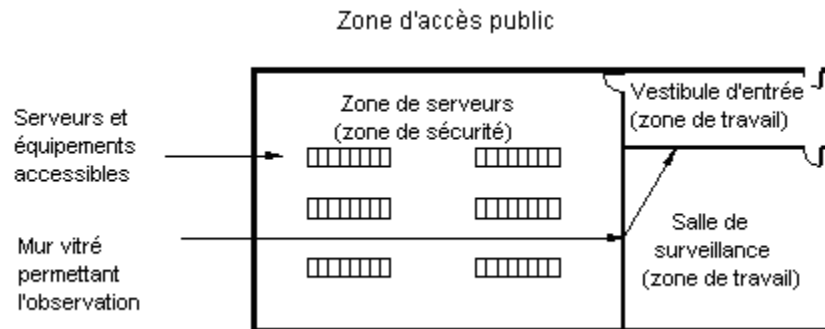
Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé C** et de l'information **classifiée** jusqu'au niveau **Très secret** lorsque les mesures de protection décrites à la section « 3. Salle de serveurs protégée » de l'Annexe A sont appliquées.

Exemple B4

Une compartimentation supplémentaire devrait être envisagée lorsque plusieurs organisations partagent une salle de serveurs (voir la section 2.3). On peut réaliser cette compartimentation en verrouillant les serveurs contenant de l'information protégée ou classifiée (voir l'Annexe A, 2 – Verrouillage du serveur). Ces exemples illustrent des salles de serveurs compartimentées à l'aide d'armoires verrouillables et de cages verrouillables.



Exemple B5

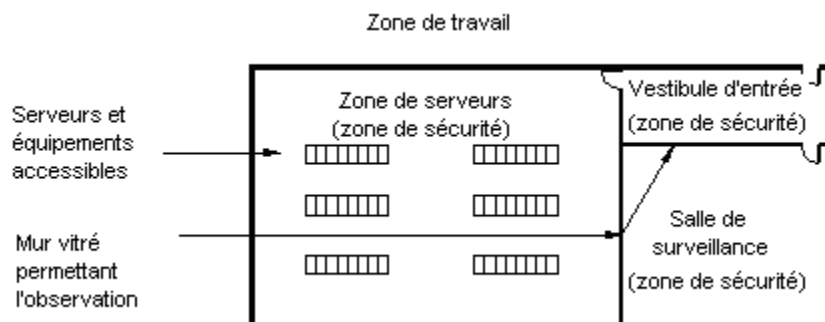


Cette zone de serveurs remplit les conditions d'une **zone de sécurité** lorsque les mesures de protection décrites à la section « 4. Centre de données protégé » sont appliquées.

Cette pièce peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** et de l'information **classifiée** jusqu'au niveau **Confidentiel**.

Lorsque la zone de surveillance est occupée 24/7, la salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** et de l'information **classifiée** jusqu'au niveau **Secret**.

Exemple B6

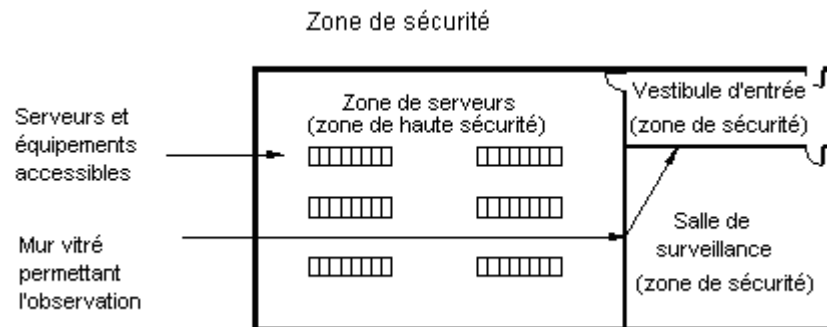


Cette salle de serveurs remplit les conditions d'une **zone de sécurité** lorsque les mesures de protection décrites à la section « 4. Centre de données protégé » sont appliquées.

Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé B** et de l'information **classifiée** jusqu'au niveau **Confidentiel** lorsque le centre de données protégé est situé dans une **zone de travail**.

Lorsque la zone de surveillance est occupée 24/7, la salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé C** et de l'information **classifiée** jusqu'au niveau **Très secret**.

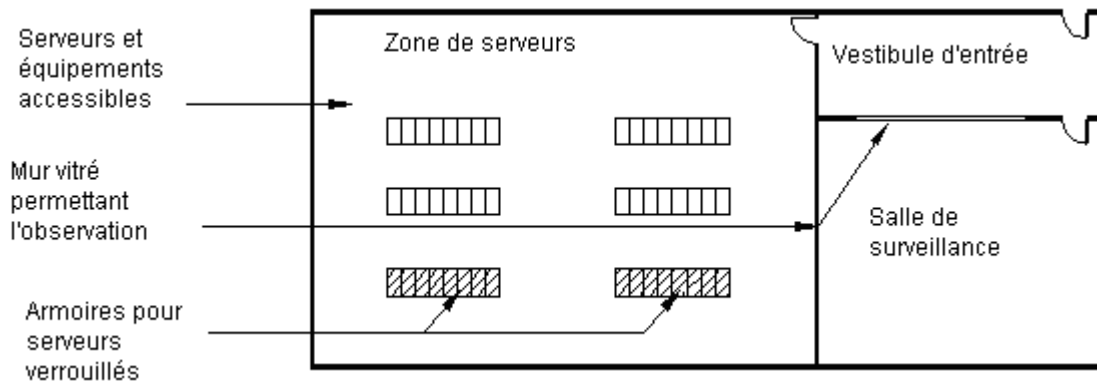
Exemple B7



Cette salle de serveurs remplit les conditions d'une *zone de haute sécurité* lorsque les mesures de protection décrites à la section « 4. Centre de données protégé » sont appliquées et lorsque le centre de données protégé est situé dans une *zone de sécurité*.

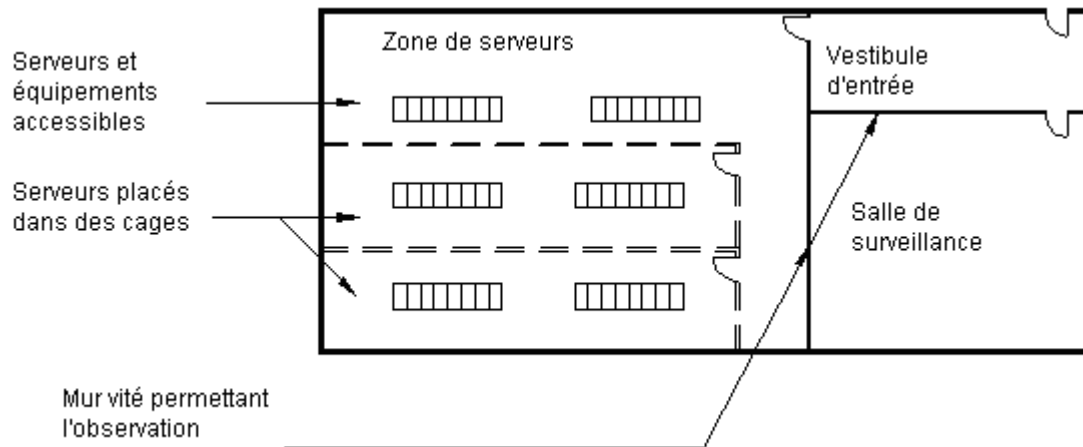
Cette salle de serveurs peut abriter des serveurs contenant de l'information **protégée** jusqu'au niveau **Protégé C** et de l'information **classifiée** jusqu'au niveau **Très secret**.

Exemple B8



Une compartimentation supplémentaire devrait être envisagée lorsque plusieurs organisations partagent une salle de serveurs (voir la section 2.3). On peut réaliser cette compartimentation en verrouillant les serveurs contenant de l'information protégée ou classifiée (voir l'Annexe A, 2 – Verrouillage du serveur). Ces exemples illustrent des salles de serveurs compartimentées à l'aide d'armoires et de cages.

Exemple B9



Cet exemple est semblable à l'Exemple B8, sauf que le centre de données est compartimenté à l'aide de cages. Cet aménagement peut être utilisé pour permettre à deux organisations de contrôler séparément l'accès à certains serveurs. Les centres de données protégés sont décrits dans la section « 4 » de l'Annexe A. Les centres de données partagés sont décrits dans la Section 2.3.