Partagé avec
TLP (Traffic Light Protocol) –
VERT

Approuvé

Norme de matière de sécurité réseau

ID du document : **SEC-07**
À l'attention de: Fédération de l'Alliance
Approuvé le 2023-06-07
Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

Le présent document décrit les exigences en matière de sécurité réseau pour la Fédération de l'Alliance. La mise en œuvre de ces exigences favorisera un niveau de sécurité réseau cohérent pour toute la Fédération de l'Alliance pour la prise en charge de l'interconnectivité et de l'interopérabilité sécuritaires du réseau.

2. Définitions

Reportez-vous à SEC-00 Glossaire de la sécurité de l'information.

3. Applicabilité

3.1. La présente norme s'applique à tous les réseaux et à l'infrastructure réseautique qui supporte les Systèmes et services de la Fédération de l'Alliance.

4 Exigences en matière de sécurité réseau

4.1 Segmentation du réseau

L'architecture du réseau doit pouvoir segmenter les services en fonction d'une évaluation des risques effectuée sur le service ou sur l'actif. Un exemple de ceci serait un serveur Web qui serait situé dans une zone de sécurité réseau différente de celle du serveur de la base de données.

Exemples de noms de zones de sécurité[1] [2] :
Zone publique
Zone d'accès public
Zones des opérations
Zone de gestion
Zone de calcul de haute performance
Zone de stockage des données

Toutes les zones de sécurité et tous les services de chaque zone doivent être documentés.

4.2. Contrôles d'accès au réseau

Les contrôles d'accès au réseau peuvent se trouver dans différentes couches du réseau et peuvent aller des simples listes de contrôle d'accès (ACL) sur un périphérique réseau de couche 3, jusqu'aux solutions d'accès réseau ZTNA (Zero Trust Network Access). Les environnements doivent implémenter les contrôles suivants :

Tout le trafic passant d'une Zone de sécurité réseau à une autre doit être filtré via un Périphérique de mise en réseau capable de restreindre le trafic à la fois par l'adresse IP et le numéro du port. Un Périphérique de mise en réseau capable de mener une inspection dynamique est recommandé.
Des règles doivent être créées pour des protocoles ou des services spécifiques connus pour être nécessaires entre deux points de chute qui se trouvent dans des Zones de sécurité réseau différentes. (Aucune règle ip any any ne sera appliquée.)

L'action par défaut sur tous les appareils utilisés pour le filtrage ou la restriction du trafic doit être de supprimer ou de bloquer le trafic.
Toutes les règles créées qui autorisent le trafic à circuler entre les Zones de sécurité réseau doivent être documentées.

Des contrôles supplémentaires doivent être envisagés pour les Zones de sécurité réseau où des données classées comme étant Élevées ou Très élevées sont consultées ou stockées.

Il est important d'évaluer les risques de sécurité lorsque le trafic est permis entre différentes Zones de sécurité réseau; par exemple les Zones de sécurité réseau utilisées pour un service

[1] Centre canadien pour la cybersécurité, Exigences de base en matière de sécurité pour les zones de sécurité de réseau.
[2] NIST Special Publication, NIST SP 800-223 ipd, High-Performance Computing (HPC) Security.

de production et celles utilisées pour le développement ou le test de ce même service ne doivent jamais, dans la mesure du possible, pouvoir communiquer les unes avec les autres.

4.3. Chiffrement

Tout le trafic réseau sortant d'un environnement de système d'information destiné à un autre réseau exploité par une organisation différente, ou lorsque le trafic réseau circule dans une infrastructure détenue ou exploitée par une organisation différente, doit être chiffré. Toutes les données à risque élevé ou très élevé doivent être chiffrées en transit. Tout le trafic réseau interne doit être crypté dans la mesure du possible et là où la technologie le permet. Les risques associés à tout flux de trafic non crypté doivent être évalués conformément à *SEC-05 Politique de gestion des risques liés à la cybersécurité*.

4.4. Détection et prévention des intrusions

Les systèmes de détection d'intrusion ou les systèmes de prévention d'intrusion doivent être utilisés à l'intérieur ou à l'extérieur d'un périphérique réseau pour surveiller tout le trafic acheminé par vos fournisseurs en amont afin de générer des alertes ou de prendre des mesures préventives. Un dispositif de système de détection ou d’intrusion doit être utilisé pour les réseaux où circuleront des données à risque élevé ou très élevé.

4.5. Journalisation

Tous les Périphériques de mise en réseau doivent produire des journaux conformément à *SEC-06 Norme de journalisation et de suivi de la sécurité des systèmes*.

4.6. Gestion des Périphériques de mise en réseau

Les Périphériques de mise en réseau sont un élément essentiel de la confidentialité, de l'intégrité et de la disponibilité d'un environnement de système d'information. Les mesures de sécurité qui s’y appliquent doivent être de classification équivalente ou supérieure à celles qui s’appliquent aux données qui y circulent. Les Périphériques de mise en réseau doivent être configurés conformément à *SEC-06 Norme de journalisation et de suivi de la sécurité des systèmes.*

Partagé avec TLP (Traffic Light Protocol) – VERT	**Approuvé**

4.7. Schémas d'architecture réseau

Tous les sites, groupes et équipes qui exploitent des environnements composés de plusieurs Zones de sécurité réseau doivent tenir des diagrammes d'architecture à jour. Ces diagrammes doivent représenter les connexions physiques et virtuelles entre tous les Périphériques de mise en réseau où le trafic circulera entre des Zones de sécurité réseau, les appareils de sécurité, les fournisseurs de services Internet et les connexions VPN.

5. Information connexe

SEC-00 Glossaire de la sécurité de l'information
SEC-02 Politique de classification des données
SEC-06 Norme de journalisation et de suivi de la sécurité des systèmes
Centre canadien pour la cybersécurité, Exigences de base en matière de sécurité pour les zones de sécurité de réseau