CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SC-07

Protection des frontières

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-07 — Protection des frontières (PaFF)

Énoncés :

a. Surveiller et contrôler les communications des interfaces externes gérées vers le système et celles des principales interfaces internes gérées au sein du système
b. Mettre en oeuvre des sous-réseaux pour les composants de systèmes à accès public qui sont séparés [Sélection (un choix) : physiquement; logiquement] des réseaux internes de l'organisation
c. Se connecter aux réseaux ou aux systèmes externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité et de protection de la vie privée de l'organisation

Paramètres :

b. à définir par l'organisme

Responsable : OP

Discussion :

Les interfaces gérées incluent les passerelles, les routeurs, les pare-feu, les mécanismes de protection, les analyseurs réseau de code malveillant, les systèmes de virtualisation et les tunnels chiffrés mis en oeuvre au sein d'une architecture de sécurité. Les sous-réseaux qui sont séparés physiquement ou logiquement des réseaux internes sont appelés communément des zones démilitarisées (ZD) ou, en anglais, DMZ (Demilitarized Zones). La restriction ou l'interdiction relative aux interfaces des systèmes organisationnels peut inclure le fait de diriger le trafic Web externe vers les serveurs Web désignés en utilisant des interfaces gérées, le fait d'interdire tout trafic externe qui semble usurper une adresse interne ou le fait d'interdire tout trafic interne qui semble usurper une adresse externe. Le document SP 800-189 du NIST donne plus d'information sur les techniques de validation des adresses sources pour prévenir l'entrée et la sortie du trafic utilisant les adresses usurpées. Les services de télécommunications commerciaux sont fournis par des composants réseau et des systèmes de gestion consolidés utilisés conjointement par les clientes et clients. Ces services peuvent également inclure des lignes d'accès et d'autres éléments de service fournis par des tiers. Ils peuvent représenter des sources de risque supplémentaire, malgré les dispositions du contrat en matière de sécurité. La protection de la frontière peut être mise en oeuvre comme contrôle commun sur l'ensemble ou une partie d'un réseau organisationnel de manière à ce que la frontière à protéger soit plus grande que la frontière du système (c'est-à-dire une limite d'autorisation).