CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SC-07(09)

Restriction du trafic de communications malveillant sortant

Juill. 2026

Votre gouvernement

Québec

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-07(09) — Restriction du trafic de communications malveillant sortant (-F-)

Énoncés :

a. Détecter et bloquer le trafic de communications sortant susceptible de constituer une menace pour les systèmes externes
b. Vérifier l'identité des utilisatrices et utilisateurs internes associés aux communications bloquées

Responsable : Aucun

Discussion :

La détection du trafic de communications sortant provenant d'activités internes et susceptible de poser une menace pour les systèmes externes est désignée sous le nom de détection d'extrusion. La détection d'extrusion est effectuée dans le système des interfaces gérées. Elle comprend une analyse du trafic de communications entrant et sortant qui vise à trouver des indications de menaces internes ciblant la sécurité des systèmes externes. Les menaces internes visant les systèmes externes comprennent le trafic annonciateur d'attaques par déni de service, du trafic utilisant des adresses sources usurpées et du trafic contenant du code malveillant. Les organisations devraient définir les critères pour déterminer, mettre à jour et gérer les menaces relevées par rapport à la détection d'extrusion.