



## Système de prévention d'intrusions (IPS) Liste de contrôle des fonctions de sécurité

### Fonctions de sécurité de base

- Attaques connues
- Nouvelles attaques
- Mises à jour des signatures
- Mises à niveau des fonctions
- Matériel spécialisé
- Mises à jour du logiciel
- Système d'exploitation renforcé
- Méthodes de détection
- IPS – Hôte
- IPS – Réseau
- Information obtenue du réseau
- Information obtenue de l'utilisateur
- Évaluation des vulnérabilités
- Rendement relatif au volume de trafic
- Correction

### Conformité aux normes sur le protocole

- Transmission Control Protocol (TCP)
- User datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)

### Authentification

- Connexion sécurisée
- Ouverture de session intégrée
- Mot de passe robuste
- Compatibilité des mots de passe

### Normes ICP

- Certificats X.509
- Annuaire LDAP
- Révocation des certificats
- Algorithmes cryptographiques

### Normes cryptographiques

*Algorithmes de chiffrement*

- Advanced Encryption Standard (AES)
- Triple-Data Encryption Standard (3DES)

### Normes en matière d'assurance

- FIPS 140-1
- FIPS 140-2

### Programme de validation des algorithmes cryptographiques

- Module cryptographique validé

### Critères communs

- Niveau d'évaluation EAL 3 ou supérieur des Critères communs (CC).
- Profil de protection ou cible de sécurité

### Configurabilité

- Valeurs par défaut modifiables
- Interventions – Paquets non standard
- Journalisation
- Mise au point adaptative

### Convivialité

- Autorisation axée sur les rôles
- Maintenance par les administrateurs
- Reconfiguration par les administrateurs

### Gérabilité

- Gestion centralisée
- Gestion à distance
- Authentification du trafic de gestion
- Chiffrement du trafic de gestion

### Extensibilité

- Degré d'extensibilité