ID de Contribution: **7** Type: **Exposé (20 + 10 min)**

Création d'un bastion SSH sécurisé et redondé

mercredi 16 novembre 2022 09:00 (30 minutes)

Dans le cadre de la rénovation de l'infrastructure ainsi que l'amélioration de l'expérience utilisateur, les administrateurs informatiques de l'IRFU cherchent à proposer un cluster de bastions SSH en haute disponibilité, tout en mettant en place une sécurité suffisante pour un service ouvert sur internet.

Plusieurs problèmes se posent alors: Comment diminuer au maximum la surface d'attaque ? Comment proposer une haute disponibilité intelligente ? Quelle niveau de sécurité est demandé par le RSSI pour ces serveurs ? Comment le mettre en place ? Comment séparer le flux d'administration du flux ssh des utilisateurs ?

Nous verrons l'architecture de la solution technique envisagé (Haproxy+keepalived pour le "front", et un Double SSH + SELinux + fail2ban + clamAV + rkhunter + check_mk + filebeat pour le "back"), ainsi que ses limites et son évolution (actuelle ou futur).

Auteur principal: MARE, Benjamin

Co-auteur: GAUTIER, anthony (CEA/irfu)

Orateur: MARE, Benjamin

Classification de Session: Sécurité