CONCLUSION

Dans le cadre de ce projet réalisé au sein de l'entreprise de télécommunication MTN CI, et partant d'un souci de sécurité et d'un besoin de protection des ressources critiques et vitales, nous avons mis en place une solution de contrôle d'accès relative au contrôle du réseau LAN.

Une fois déployée, la solution a permis de réagir, en temps réel, à toute tentative de connexion au réseau par référence aux politiques de sécurité prédéfinies au niveau de la plate-forme Cisco ISE. En effet et en premier lieu, l'utilisateur est appelé à s'authentifier en présentant son compte utilisateur et le mot de passe associé au cas où il appartient au domaine, sinon et s'il s'agit d'un utilisateur invité, il s'authentifie à travers un portail Web en s'y inscrivant temporairement ou bien il obtient un compte créé par le responsable et autorisant aussi un accès momentané. L'étape qui suit la vérification de la légitimité de l'utilisateur est celle de la validation de l'état des machines ; chacune doit disposer d'un antivirus. Dans le cas contraire, l'utilisateur bénéficie d'une période de grâce, au cours de laquelle, un fichier de remédiation lui est offert afin de pouvoir accéder.

L'implémentation de l'ISE nous a permis de réduire à un 80% les accès non autorisés. Ce taux est dû à l'incompatibilité entre la version des switch d'accès et la plate-forme CISCO ISE. Nous prévoyons donc faire une mise à niveau des différents switch d'accès afin renforcer le niveau de contrôle d'accès. Par la suite nous devrons avoir recours à une authentification forte, concaténant au moins deux facteurs d'authentification, tels que les certificats numériques et les mots de passe à usage unique (One-Time Password) ; ceci est réalisable en intégrant la plate-forme Cisco ISE.