



Arnaud Perrin, IT Security - CISSP  
auprès d'une banque privée à Genève

## Traçabilité et contrôle des accès privilégiés aux infrastructures

*Comment contrôler les accès aux infrastructures informatiques sensibles ? Pour les institutions qui traitent des informations confidentielles, savoir qui accède aux ressources, quand et dans quel but est une nécessité. En effet, la mise en conformité avec les réglementations du risque opérationnel exige la traçabilité de tout accès. Cela n'est pas toujours facile à assurer. La succursale genevoise d'une banque privée a trouvé une réponse efficace à ce problème.*

Le groupe bancaire dans son ensemble est actif dans les domaines de la banque commerciale, privée et internationale. Le site de Genève se conforme aux directives réglementaires émises par le siège sur la base des standards internationaux du risque opérationnel, et les adapte si nécessaire aux normes suisses. Or les accès privilégiés des administrateurs aux serveurs Unix se révélaient insuffisamment contrôlables.

Arnaud Perrin, IT Security - CISSP, explique : « *Les administrateurs possédaient les droits d'accès à une centaine de serveurs Unix comportant pour certains des applications sensibles.* » Le département sécurité souhaitait uniformiser les pratiques de gestion des mots de passe et reprendre le contrôle des accès privilégiés en intégralité. « *Nous désirions limiter les droits des administrateurs et acquérir une visibilité suffisante des actions effectuées. Non parce que nous avons des soupçons, mais parce que notre rôle est de mettre en place des contrôles permettant de prévenir les situations à risques.* »

---

« *Nous désirions limiter les droits des administrateurs et acquérir une visibilité suffisante des actions effectuées. Non parce que nous avons des soupçons, mais parce que notre rôle est de mettre en place des contrôles permettant de prévenir les situations à risques.* »

---

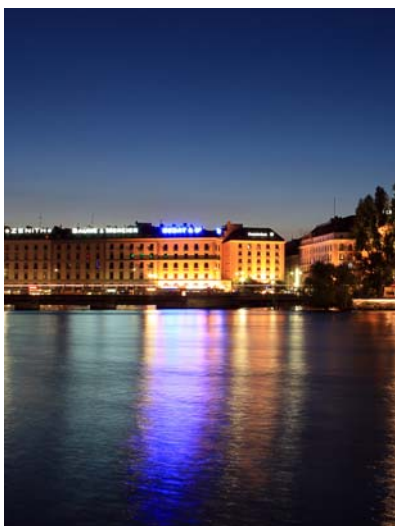
### e-DMZ : accès privilégiés sur demande

Navixia propose alors à la banque la solution eGuardPost de la société américaine e-DMZ Security. Il s'agit d'un boîtier hautement sécurisé sur lequel les administrateurs doivent s'authentifier pour effectuer une demande de

---

*Les administrateurs doivent s'authentifier via un boîtier hautement sécurisé pour effectuer une demande de connexion.*

---



---

*Solliciter un accès pour une date ultérieure est possible, ce qui s'avère particulièrement utile pour les actions programmées hors des heures de bureau.*

---

connexion. L'approbation de cette demande peut être automatique (pour des systèmes de test par exemple) ou donnée manuellement par une ou plusieurs personne(s) autorisée(s) selon le degré de criticité. Toutes les étapes du processus sont loguées.

Arnaud Perrin : « A l'époque de notre recherche, e-DMZ était la seule solution assez aboutie pour répondre à nos besoins. Nous avons l'habitude de travailler avec Navixia en qui nous avons confiance. Nous avons donc retenu sans hésitation la solution proposée. Un prestataire de confiance est important pour aider à la décision et être serein lors de la phase de déploiement. »

La banque passe alors à la phase de test. Il s'agit d'installer un certificat e-DMZ sur quelques serveurs Unix, puis de vérifier si le boîtier eGuardPost parvient à s'octroyer des droits nécessaires pour la gestion des comptes. Arnaud Perrin raconte : « Nous avons pris un maximum de précautions dans les choix d'architecture et d'implémentation de la solution. L'outil est très fiable et il n'a encore jamais été mis en défaut, néanmoins compte tenu de sa position de centre névralgique il fallait faire preuve de la plus grande prudence. »

Les tests s'avèrent concluants. « Nous avons déployé progressivement la solution et déposé un certificat e-DMZ sur tous les serveurs à gérer. Toute la démarche, y compris la phase de test, a pris environ deux mois. Pour faciliter la procédure, le certificat est désormais inclus d'office dans le package que nous installons sur chaque nouveau serveur. Il ne nous reste plus ensuite qu'à introduire manuellement son adresse IP dans le système et créer les comptes et utilisateurs. » La solution est maintenant opérationnelle depuis dix-huit mois. « L'infrastructure gérée est en constante évolution, avec des ajouts et des effacements de serveurs réguliers. Tout équipement possédant une adresse IP peut être géré. Nous bénéficions aujourd'hui d'une grande fiabilité doublée d'une flexibilité accrue. »

Le principe d'utilisation est simple. Un administrateur souhaitant accéder à un serveur donné en fait la demande dans le système. Il annonce le but de la connexion, la date et la durée souhaitées. Solliciter un accès pour une date ultérieure est possible, ce qui s'avère particulièrement utile pour les actions programmées hors des heures de bureau. La requête est enregistrée ; un mail est envoyé à la sécurité selon une liste de distribution prédéfinie. Les responsables vérifient toutes les justifications d'accès, puis valident ou refusent la demande. En cas de validation le mot de passe devient disponible dans l'interface utilisateur. La procédure est enregistrée dans un fichier log.

Combien de temps faut-il à un administrateur pour obtenir un accès autorisé ? Arnaud Perrin : « Nos règles de fonctionnement internes prévoient un temps de réponse maximum de 30 minutes. Dans la majorité des cas, la demande est traitée en moins de 15 minutes. Pour certains systèmes de test ou de

---

*Un prestataire de confiance est important pour aider à la décision et être serein lors de la phase de déploiement.*

---

*production, l'accès est approuvé automatiquement en laissant une trace du processus. Mais il ne faut pas sous-estimer le temps de réaction des équipes lors de la définition des règles internes. »*

Au final, qui contrôle les gestionnaires du processus de contrôle ? « *Un administrateur eGuardPost n'est pas habilité à faire une demande d'accès pour lui-même. Cela ne peut être fait qu'à partir d'un compte utilisateur. Un administrateur ne doit en effet pas forcément pouvoir accéder en tant qu'utilisateur au système dont il a la gestion. L'outil respecte le principe des moindres privilèges. »*

### Accès aux applications sensibles = précautions accrues



Contrôler les accès n'est parfois pas suffisant, comme le souligne Arnaud Perrin : « *Dans le cas des applications les plus sensibles, l'administrateur pourrait en théorie avancer un motif légitime pour demander un mot de passe, puis s'en servir à d'autres fins. »* Pour cette raison, eGuardPost offre également la possibilité d'enregistrer une session en vidéo. Une fenêtre interactive s'ouvre alors dans l'interface, l'intégralité des mouvements et commandes effectués durant la session est enregistrée et peut être revue en cas de doute. « *Nous avons l'intention de généraliser l'utilisation de cette méthode, qui ne produit pas de fichiers logs démesurés. Le boîtier e-DMZ possède 250 Go de stockage redondant et il est toujours possible de stocker les logs sur un serveur de backup si nécessaire. »* Pour la banque, de tels enregistrements ne servent pas à exercer une surveillance constante sur les collaborateurs mais à garder une trace des actions effectuées. « *Notre objectif est de pouvoir consulter les vidéos en cas de problème, pas de regarder par-dessus l'épaule des administrateurs ! De plus, visionner les enregistrements prend du temps. Une surveillance en continu supposerait des ressources que nous n'avons pas. »*

---

*« Il est essentiel d'impliquer les administrateurs dès le départ dans le processus et de remporter leur adhésion au préalable pour assurer un déploiement efficace. »*

---

La mise en place du système eGuardPost permet de vérifier si les droits d'accès sont gérés avec pertinence. Arnaud Perrin : « *On sait que l'organisation est bonne si les administrateurs peuvent se passer d'utiliser des comptes privilégiés trop souvent. La plupart des actions devraient pouvoir être effectuées à partir de comptes utilisateurs normaux. Dans le cas contraire, il faudra corriger les schémas d'accès avant de pouvoir implanter eGuardPost efficacement. Par ailleurs, les erreurs faites à partir d'un compte privilégié peuvent avoir des conséquences graves. Éviter leur utilisation trop fréquente est aussi un moyen de protéger les administrateurs dans leur travail. »* Dans la pratique, il est préférable que l'accès super administrateur soit réservé à des actions particulières, comme le redémarrage de machines ou le déploiement de patches.

Qu'ont pensé les administrateurs de ces changements ? Arnaud Perrin : « *Toute sécurité a un prix : aujourd'hui, il est légèrement plus compliqué*

« Nous bénéficions aujourd'hui d'une grande fiabilité doublée d'une flexibilité accrue. »

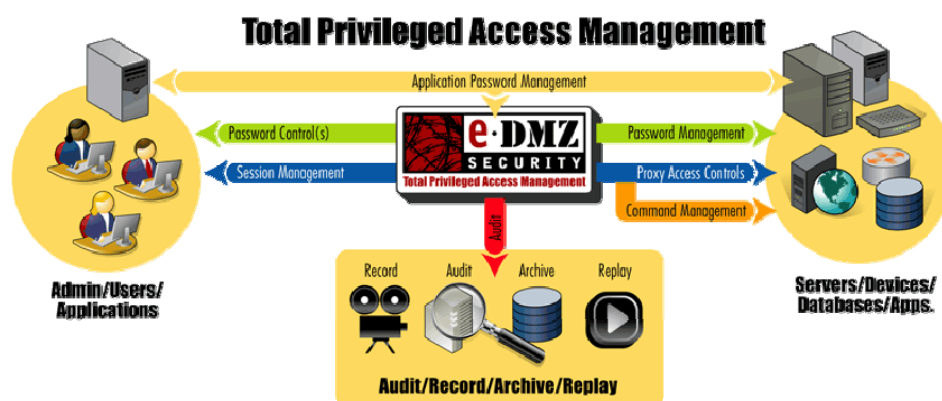
« Nous n'avons jamais réussi à mettre eGuardPost en défaut et nous n'avons jamais eu un seul bug. De plus le support est très réactif en cas de besoin. Nous sommes satisfaits. »

qu'auparavant d'obtenir un accès privilégié, mais c'est surtout une question d'habitude de travail à prendre. En contrepartie nos administrateurs se voient soulagés de la possession et tentation permanente d'utiliser l'accès privilégié aux systèmes. Tout accès étant validé, les erreurs sont encore plus rares. » Arnaud Perrin met d'ailleurs en garde les futurs acquéreurs d'une telle solution: « Attention aux vieilles habitudes des administrateurs système. Il est essentiel de les impliquer dès le départ dans le processus et de remporter leur adhésion au préalable pour assurer un déploiement efficace. »

La banque est désormais en conformité avec les réglementations du risque opérationnel et le bilan d'Arnaud Perrin est entièrement positif : « L'installation et l'utilisation du système ne posent aucun problème. Les utilisateurs ont simplement à se familiariser avec de petits détails d'ergonomie. Les problèmes qui ont pu nous être signalés provenaient toujours d'un mode d'utilisation inadéquat. Nous n'avons jamais réussi à mettre eGuardPost en défaut et nous n'avons jamais eu un seul bug. De plus le support est très réactif en cas de besoin. Nous sommes satisfaits. »

La solution de gestion d'accès privilégiés de e-DMZ est intéressante pour toute entreprise qui souhaite instaurer un contrôle des accès à ses informations sensibles et assurer leur traçabilité.

## Exemple d'architecture



**Navixia SA**  
 Route du Bois 1  
 CH - 1024 Ecublens  
 Tél.:  
 + 41 (0)21 324 32 00  
 Fax:  
 + 41 (0)21 324 32 01  
 E-mail:  
 info@navixia.com  
 Web:  
 www.navixia.com

La solution de gestion d'accès privilégiés eGuardPost de e-DMZ permet d'assurer leur contrôle et leur traçabilité.

- Elle est simple à installer et à utiliser
- Conforme aux réglementations SOX, PCI, HIPAA, Basel II
- Compatible avec Unix, Linux, Windows, AS/400, Mainframe 3270 et bien d'autres.