



Arnaud Perrin, IT Security – CISSP
at a Private Bank in Geneva

Traceability and control of privileged access to infrastructures

How can access to sensitive IT infrastructures be controlled? Institutions that handle confidential information need to know who is accessing resources, when they are accessing it and for what reason. Indeed, in order to comply with operational risk regulations, every access must be traceable. This is not always as easy as it seems. The Geneva branch of a private bank has found an effective way of solving the problem.

The banking group as a whole is active in the areas of commercial, private and international banking. The Geneva site complies with the prescribed regulations issued by its head office, which are based on international standards with regard to operational risks, and adapts them, where necessary, to Swiss standards. However, the administrators' privileged access to the Unix servers turned out to be insufficiently controllable.

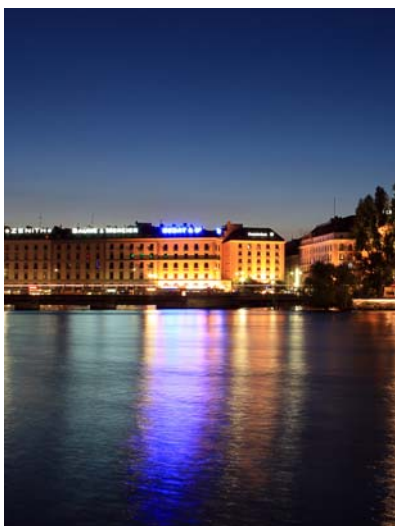
Arnaud Perrin, IT Security - CISSP, explains: *"The administrators had access rights to about a hundred Unix servers, some of which held sensitive applications."* The security department wanted to standardize the management of password practices and retake full control of privileged access. *"We wanted to limit administrators' rights and get sufficient visibility of actions carried out. Not because we were suspicious, but because our role is to set up controls that allow risk situations to be anticipated."*

"We wanted to limit administrators' rights and get sufficient visibility of actions carried out. Not because we were suspicious, but because our role is to set up controls that allow risk situations to be anticipated."

e-DMZ : privileged access on demand

Navixia therefore proposed that the bank adopt the eGuardPost solution from the American company e-DMZ Security. This consists of a highly secured appliance that requires administrators to prove their identity in order to make a connection request. The approval of this request can be automatic (for test systems, for example) or given manually by one or more

A highly secured appliance requires administrators to prove their identity in order to make a connection request.



It is also possible to apply for access at a later date, which is particularly useful for actions programmed outside office hours.

people authorized according to the degree of criticality. All the process steps are logged.

Arnaud Perrin: *"At the time of our search, e-DMZ was the only solution advanced enough to meet our requirements. We were used to working with Navixia and we had every confidence in them. We therefore accepted the proposed solution without hesitation. A trustworthy service provider is important when making decisions and for having peace of mind during the utilization phase."*

The bank then proceeded to the test phase. This consisted of installing an e-DMZ certificate on a few Unix servers, then verifying if the eGuardPost appliance managed to grant the necessary rights for managing accounts. Arnaud Perrin adds: *"We took maximum precautions with regard to the choices of solution architecture and implementation. The tool is very reliable and has never yet been found wanting. Nevertheless, considering its position at the nerve centre, we had to proceed with the greatest caution."*

The tests proved to be successful. *"We then introduced the solution progressively and registered an eDMZ certificate on all the servers to be managed. The whole process, including the test phase, took about two months. In order to facilitate matters, from now on, the certificate will be included as standard in the package we install on every new server. We now only have to manually introduce its IP address into the system and create accounts and users."* The solution has now been operational for eighteen months. *"The managed infrastructure is constantly evolving, with servers being regularly added and removed. Any equipment with an IP address can be managed. Today, we are profiting from extreme reliability coupled with increased flexibility."*

The operating principle is simple. An administrator wishing to access a given server actually enters his request in the system. He states his reason for the connection, the date and desired duration. It is also possible to apply for access at a later date, which is particularly useful for actions programmed outside office hours. The request is registered and a mail is sent to security according to a predefined distribution list. The persons responsible verify all reasons for access and then validate or refuse the request. If validation is obtained, the password is made available at the user interface. The procedure is registered in a log file.

How long does it take for an administrator to get authorized access? Arnaud Perrin: *"Our internal working rules envisage a response time of 30 minutes maximum. In the majority of cases, the request is handled in less than 15*

“A trustworthy service provider is important when making decisions and for having peace of mind during the utilization phase.”



“It is essential to involve administrators in the process right from the start and to get them on board in advance, so that efficient utilization is guaranteed.”

minutes. For certain test or production systems, access is approved automatically and a trace of the process recorded. However, when defining internal rules, team reaction times must not be underestimated.”

In the end, who controls the managers of the control process? *“An eGuard-Post administrator is not authorized to request access for himself. This can only be done from a user account. In effect, in his role as a user, an administrator must not necessarily be able to access a system which he manages. The appliance adheres to the principle of least privilege.”*

Access to sensitive information = heightened precautions

Controlling access is sometimes not enough, emphasizes Arnaud Perrin: *“In the case of the most sensitive applications, the administrator could, in theory, give a legitimate motive in order to get a password and then use it for other purposes.”* For this reason, eGuardPost also offers the possibility to record sessions in video. In such cases, an interactive window opens at the interface, allowing all movements and commands carried out during the session to be recorded. These can later be examined in case of doubt. *“We intend to generalize the use of this method, which does not produce excessive log files. The e-DMZ appliance has 250 GB of redundant storage and it is always possible to save the logs on a backup server, if necessary.”* For the bank, such recordings are not intended for the constant surveillance of employees, but rather for keeping a trace of actions carried out. *“Our objective is to be able to consult the videos in case there is a problem, not to look over administrators’ shoulders! More to the point, replaying the recordings takes time. Continuous surveillance would require resources we simply do not have.”*

The installation of the eGuardPost system allows verification of whether access rights are being suitably managed. Arnaud Perrin: *“We know that organization is good if the administrators can avoid using privileged accounts too often. It should be possible to carry out most actions by making full use of normal user accounts. If this is not the case, the access process should be changed so that the subsequent installation of eGuardPost is effective. Furthermore, errors stemming from a privileged account could have serious consequences. Refraining from using them too frequently is also a way to protect administrators in their work.”* In practice, it is preferable for super administrator access to be reserved for special actions, such as restarting machines or installing patches.

What did the administrators think of these changes? Arnaud Perrin: *“All security comes at a price. Today, obtaining privileged access is slightly more*

"Today, we are profiting from extreme reliability coupled with increased flexibility."

"We have never succeeded in finding fault with eGuardPost and have never had a single bug. In addition, the support is very reactive in case of need. We are satisfied."

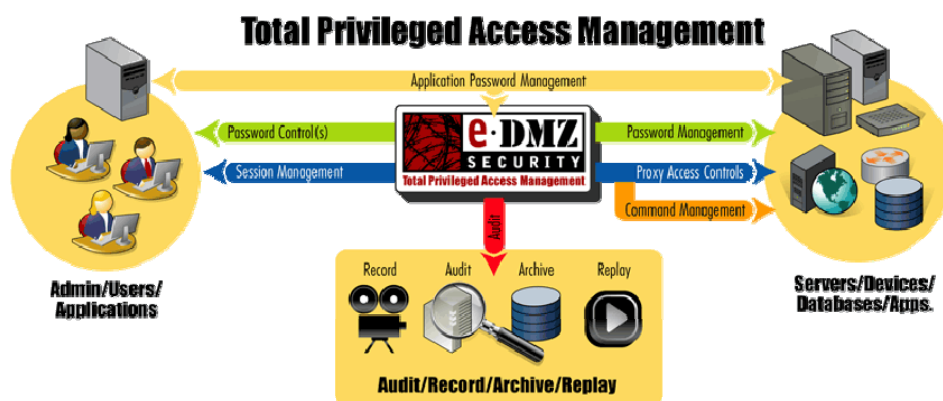
complicated than before, but it is primarily a question of embracing a work routine. In return, no longer having permanent possession of, and temptation to use, privileged access to systems is a relief to our administrators. Since every access is validated, errors are even rarer."

Arnaud Perrin, moreover, issues a warning to future purchasers of such a solution, *"Pay heed to the old habits of system administrators. It is essential to involve them in the process right from the start and to get them on board in advance, so that efficient utilization is guaranteed."*

From now on, the bank conforms to operational risk regulations, and Arnaud Perrin's assessment is entirely positive. *"The installation and utilization of the system are trouble-free. Users simply have to familiarize themselves with small details with regard to ergonomics. The problems we have been made aware of always arise from inappropriate use. We have never succeeded in finding fault with eGuardPost and have never had a single bug. In addition, the support is very reactive in case of need. We are satisfied."*

The e-DMZ solution for the management of privileged access is attractive for any company wishing to control access to its sensitive information and assure its traceability.

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

eGuardPost by e-DMZ

manages, controls and traces all privileged accesses

- Easy to implement and use
- Conforms to the SOX, PCI, HIPAA, Basel II regulations
- Compatible with Unix, Linux, Windows, AS/400, Mainframe 3270 as well as many others.