Scenario 2 material
"Transformation of the Pulse Secure Remote Access"

1 Introduction

The purpose of completing this case study is for the Tenderer to demonstrate the capabilities required to carry out a demanding transformation project within the realm of ECHA infrastructure, integration points, security best-practices, financial constraints and business requirements.

2 Reference material

2.1 IT Infrastructure Architecture

The Annex 1 - IT Infrastructure Architecture (CMO) contains the high-level design information of ECHA Secure Remote Access architecture (ref. section 4.7 SSLVPN) and it must be carefully checked to fully understand the context.

2.2 Volumes

In September of 2017 the volumes of the ECHA SSL VPN Remote Access were as follows:

- 2 physical appliances PSA7000 (in HA) + License for up to 5000 concurrent users
- Average number of concurrent users around 150 (with few significant spikes per year). That number is growing year by year
- Average daily throughput of 2-4 Mbs (with few significant spikes per year)
- 600 ECHA users, 2400 Authority users, 100 ECHA Contractors

3 Objective

ECHA currently owns the Pulse Secure hardware (2xPSA7000), the licenses and the maintenance. The objective of the case study is for the Tenderer to provide a plan to transform the current SSL VPN Remote Access solution from the existing to a new service offered by the Tenderer as a Service. The Tenderer is free to propose the solution that fulfil the requirements defined in the section 4.

4 Key considerations

4.1 Cost effectiveness

This is a key component of this case study, the Tenderer shall provide a secure and scalable solution with a lower TCO *total cost of ownership* (considering the end to end service and including the hardware/software/license/maintenance/user support) that should be reflected as:

- cost for the running service (cost per user/per month)
- Cost for Changes over the first year (with the estimated associated Packaged Effort Band).

4.2 Security and technical requirements

Many details on the current implementation are described in the Annex 1.IT Infrastructure Architecture Document, the Tenderer should propose a new solution keeping in mind at least the following points:

- The solution should be aligned with the latest security best-practices (including auditability/access log), easy to implement, easy to use, scalable and fully compatible with the main client OS and the latest versions of the main browsers (at least IE-FF-Edge).

- ECHA users need a full L3 remote access from their corporate laptop for teleworking purposes. A client software/tool compatible with Windows 10 can be used. A certificate based device authentication and RSA token based two-factor user authentication must be supported.

- For the Authority users a *light* access to the specific ECHA IT Tools is preferred. ECHA doesn't manage the Authority end user devices (Windows-Mac-Linux), so the deployment and support of any client software/tool should be limited or avoided. In some cases a direct L3 tunnel from the Authority clients to the ECHA environment could be explicitly prohibited by the Authority security policy. A strong authentication via RSA tokens (two-factor) and source IP restriction is a must have. Most of ECHA's IT Tools used by the Authority users are web-based, but a key one is not (it's a client-server application which requires JAVA installed locally) and its specific requirements have to be taken in to consideration. The solution must have capability to be able to limit users (groups) access only to the specific ECHA application (e.g. URL) as different users in the same Authority could have access to different ECHA IT Tools based on their ECHA AD group/role following ECHA's standard access management approach

4.3 Integration

There are several integration points, the most important ones are the RSA Servers for the multi-factor authentication and the Active Directory servers for the AD-group based granular access to ECHA's IT tools

4.4 User experience

The SSL VPN service is a critical service for ECHA therefore any migration or maintenance should be as transparent to the user as possible. Any maintenance that impacts access to the service should be clearly defined and communicated to end users. A clear and well designed roll-out plan to replace the current solution minimizing the impact on the users has to be included in the Case Study output. On top of that, any clear improvement or simplification of the user experience has to be highlighted in the proposal.