Adding security to existing unsecured web services

V.F. Pais, V. Stancalie

National Institute for Laser, Plasma and Radiation Physics, Laser Department, Association EURATOM/MEdC

Introduction

- Web services are starting to be widely used for accessing remote data and implementing distributed applications[1].
- A lot of services constructed for internal usage are usually without user authentication; access to these services is controlled only by IP filtering, based on the source address.
- For the purposes of a national research project, "Research on laser-atoms, laser plasma interactions, towards inertial confinement fusion"[2], project TICF, several web services were developed to provide remote data access and remote processing for applications. Initially access was restricted to several trusted partners. Because of this, there were no provisions for user authentication.
- When access was required to the existing services over the Internet, it was decided to construct a new web service that will provide authentication and accounting for the existing services.
- In order to properly forward web service traffic, after authentication and authorisation, several changes are required:
  1. Web Service description (WSDL) must be modified to point to the "proxy" endpoint, instead of the real server(s)
  2. All XML Schema references must also point to the "proxy" server
  3. Additionally, web service methods may return IP addresses in their response, thus making it necessary to process return messages prior to forwarding them to the client

Network Topology

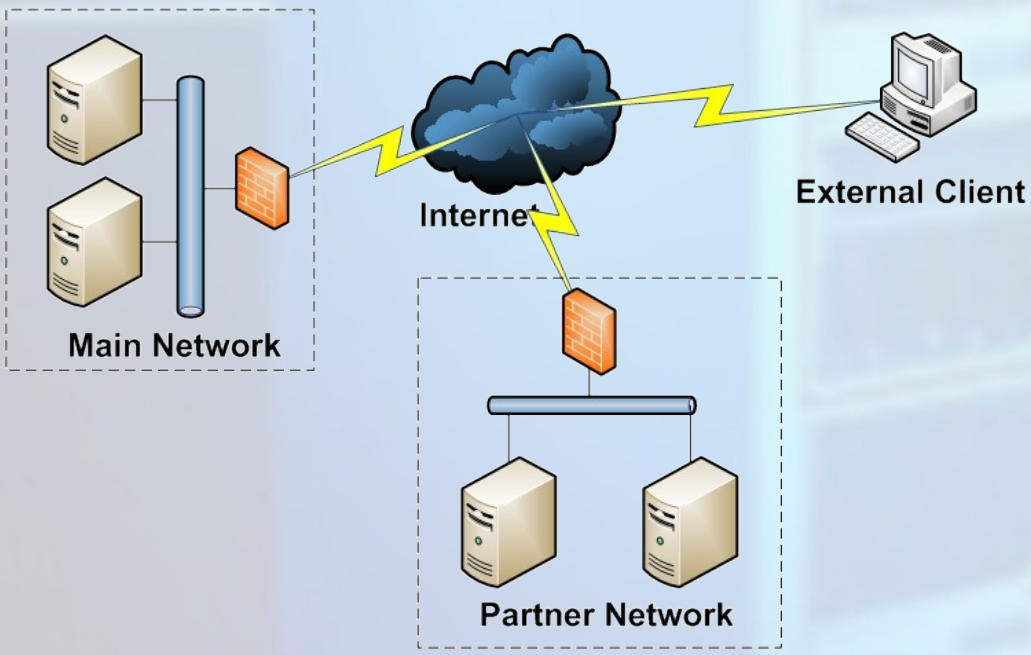

Figure 1. General network topology, identifying web service servers and their connection to external clients

- Web services are distributed in several networks; Interactions between networks, at web service level, exists, but are rather infrequent.
- In the original setup, every connection is filtered by the network firewall; as a result trust is established based on IP address, thus leading to weak security and the impossibility to properly track user activity.
- Any external users can access the provided services only from their base networks.

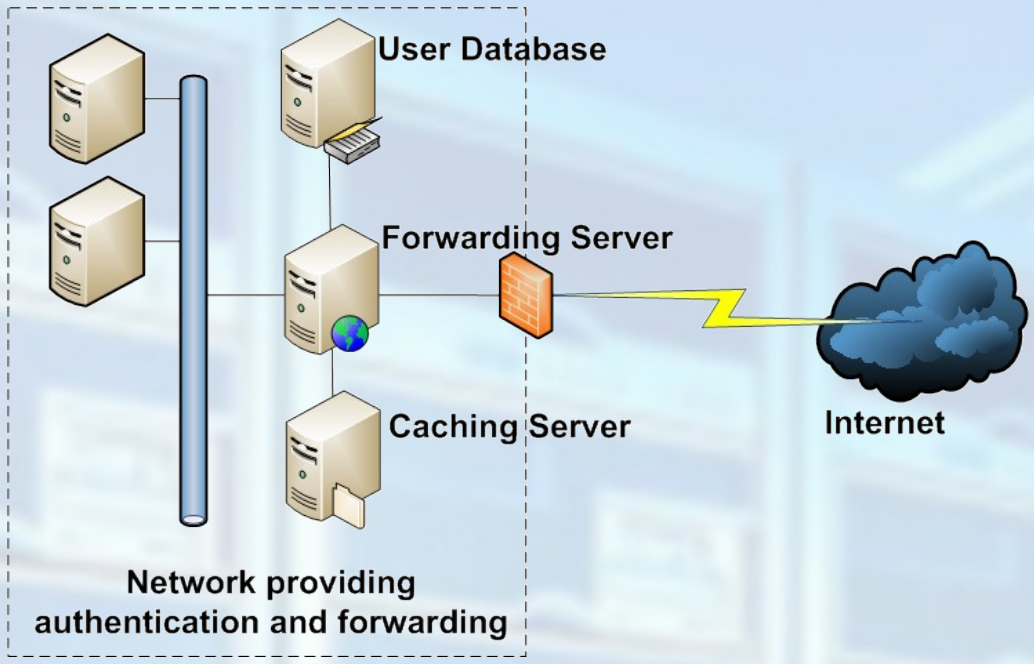

Figure 2. Network topology changes due to the introduction of the forwarding server, combined with a user directory and a caching server

- The forwarding server is placed in the main network and behaves as a proxy for all services (including those available from partner networks).
- In the main network, is established a user database, holding authentication and authorisation information. Furthermore, this database is also used for tracking user activity.
- In order to improve response times for several services, an additional caching server [3] is used.

Conclusions

- As a direct result of having this forwarding server, all web service related traffic, that was previously unsecured, now becomes secured. In addition, user rights can be assigned on a per method basis.
- Network topology is completely hidden to the end-user. The client sees only the forwarding server and is unaware of the presence of other servers.
- Combined with the caching mechanism, network throughput is increased. Due to the nature of data being used in the TICF project, a lot of web service responses can be stored locally for several months, thus reducing the traffic to other partner networks.
- Further work is required mainly in two areas:
  - development of new plugins allowing for more authentication mechanisms and exploring other technologies, like data compression and encryption
  - because several web services are invoked from within web portals, the ability to use single sign on technologies for authentication will be investigated (especially Shibboleth [4] and PAPI [5])

References

[1] "Using Web Services for Remote Data Access and Distributed Applications", V.F. Pais, V. Stancalie, 2006, Fusion Engineering and Design, Volume 81, Issues 15-17, July 2006, Pages 2013-2017

[2] "Forbidden transitions in excitation by proton impact in Li-like Al ions", V. Stancalie, V.F. Pais, M. Totolici, A. Mihailescu, 2007, Laser and Particle Beams, Volume 25, in press

[3] "Caching Web Service for TICF Project", V.F. Pais, V. Stancalie, will be presented at "6th IAEA Technical Meeting on Control, Data Acquisition and Remote Participation for Fusion Research", 4-8 June 2007, Inuyama, Japan

[4] http://shibboleth.internet2.edu

[5] http://papi.rediris.es