CERN
CH-1211 Geneva 23
Switzerland

Document **Security Implementation**
CERN Div./Group or Supplier/Contractor Document No. **IT/ES – ATLAS/CMS VOC**
EDMS Document No. **[ASSIGNED by CSO]**

MAY 20TH 2010

SECURITY IMPLEMENTATION FOR ATLAS/CMS WEB REDIRECTOR

ABSTRACT A "Security Baseline" defines a set of basic security objectives which must be met by any given service or system. The objectives are chosen to be pragmatic and complete, and do not impose technical means. Therefore, details on how these security objectives are fulfilled by a particular service/system must be documented in a separate "Security Implementation Document" (this document). These details depend on the operational environment a service/system is deployed into, and might, thus, creatively use and apply any relevant security measure. Derogations from the baseline are possible and expected, and must be explicitly marked.

At CERN, for each service/system used in production, such a Security Implementation Document must be produced by its system/service owner, and be accepted and approved by the Computer Security Officer. All systems/services must be implemented and deployed in compliance with their corresponding Security Implementation Document. Non-compliance will ultimately lead to reduced network connectivity for the affected services and systems (i.e. closure of CERN firewall openings, ceased access to other network domains, and/or disconnection from the CERN network).

This document describes the Security Implementation for the abovementioned system/service.

Prepared by:	***Checked by:***	***Approved by:***
Flavia Donno	Computer Security Team	Computer Security Officer

Distribution:	Flavia Donno, Computer Security Team

History of Changes

Rev. No.	***Date***	***Pages***	***Description of Changes***
0.1	2010/04/26	7	Preliminary Draft
0.2	2010/05/07	8	Integrated comments received from S. Lueders
1.0	2010/06/04	8	Integrated further comments, adapted to the latest version of the template. Final version

1. SECURITY IMPLEMENTATION

The structure of this document should reflect the different Security Baselines applicable for the system/service at hand. For each Security Baseline Document, a corresponding chapter must be created. The individual requirements, then, should be answered in the corresponding sections while being as detailed and specific as possible. The first chapter should provide a general description of the system/service and the extent to which the Security Baselines apply (e.g. to all production servers, to all hosted web-pages, to a given list of servers).

2. SCOPE

The ATLAS/CMS Web Redirector is a reverse proxy used in front of other ATLAS/CMS Web services in order to mitigate potential threats coming from the underlying network, managed and unmanaged clients and hosts, potential untrustworthy users. In this document we limit our scope to the ATLAS/CMS Web Redirector. The ATLAS/CMS specific web services behind the Web Redirector are described elsewhere. The ATLAS/CMS Web Redirector runs on VOBOXes as described by the CERN/IT VOBOX SLA [1]. The required OS is SLC5.

All connections coming from the Internet addressed to one of the ATLAS/CMS Web servers are routed through the Web Redirector via a DNS alias. The Web Redirector may either deal with the request itself or pass the request wholly or partially to the main ATLAS/CMS web server/s dealing with the request.

The ATLAS/CMS Web Redirector provides:

- Web Application Firewall (WAF) through the Apache ModSecurity [2] module.
- SSL based authentication. The CERN Shibboleth [3] service is used for this purpose.
- Load distribution. Requests can be served by several ATLAS/CMS web servers, each serving the same or its own application area.
- Caching support. The reverse proxy can offload the web servers behind it by caching static content through the frontier-squid [4] server.
- Special configuration. The ATLAS/CMS Web Redirector offers the possibility of redirecting requests depending on the source generating the request. For instance, special requests coming from machines at the experiment pit are served without imposing SSO authentication. Web sites behind the Web Redirector could provide access to areas protected by AFS Kerberos.
- Hardware sparing by supporting virtualization.
- Web analytics [5].

Three configurations are at the moment supported:

1. The Web Redirector is hosted on the same machines running some of the experiment specific Web services.
2. The Web Redirector is hosted on a physical machine that hosts no other services.
3. The Web Redirector is hosted on a virtual machine as well as other experiment specific web services and they can run on the same or different hardware.

3. SECURITY BASELINE FOR SERVERS VERSION 1.0 EDMS ID 1062500

The ATLAS/CMS Web Redirector runs on VOBOXes and as such it obeys to the CERN/IT VOBOX SLA. Machines are managed through the ELFms tool suite [6]. Everything that is described below is achieved through such tool suite.

3.1 SRV-AC-1

Interactive access to the ATLAS/CMS Web Redirector is granted to the VO Contacts (VOCs). ATLAS/CMS service managers might also be granted interactive access whenever specific ATLAS or CMS services are hosted on the same machine. In particular, ssh logins are allowed only from lxvoadm using personal accounts. After that, only VOCs are allowed to sudo to root. VOCs can grant themselves root access to the machine if the need arises to use the remote console administrative interface. ATLAS or CMS service managers are never allowed to acquire root privileges on the machine. They can sudo to specific non-root service administration accounts.

3.2 SRV-AC-2

All processes running on the Web Redirector service run under a non-priviledged account. Login for such an account is disabled.

3.3 SRV-AC-3/4/5

Ssh logins are allowed only from lxvoadm using personal accounts. After that, only VOCs are allowed to sudo to root. VOCs can grant themselves root access to the machine if the need arises to use the remote console administrative interface. ATLAS or CMS service managers are never allowed to acquire root privileges on the machine. They can sudo to specific non-root service administration accounts.

3.4 SRV-AC-6

We prefer to avoid hosting ATLAS/CMS specific services on the same box where the Web Redirector runs. We are waiting for the IT/PES "VOBOX Consolidation Project" results in order to benefit from virtualization. Whenever we do host experiment specific services on the Web Redirector, we use local accounts. In particular 2 accounts per service are used: an administrative account to customize the service and an account used to run the service. Logins are disabled for the account running the service. Service managers can sudo to these accounts. The service contacts are reminded every three months to renew the password of the local service administrative and running accounts.

3.5 SRV-AC-7

No shared folders are used for the moment. We have no plans to use them in the future.

3.6 SRV-IF-1

Only the following actively used network services are enabled: ssh, http, https, arc.

3.7 SRV-IF-2/3/4/5

Incoming connections are only allowed on ports 80 and 443 which are open in the CERN central firewall. We are planning to review the usage of port 80 to make it available only for CERN intranet. No external outgoing connections are needed at the moment. All this is done using the local firewall. We are planning to improve our customization of the apache ModSecurity to reject well-known dangerous connections.

3.8 SRV-IF-6/7

All local modems, GPRS modems and USB ports are disabled by the SysAdmin CERN IT Team in the machine Quattor/ELFms configuration provided.

3.9 SRV-PS-1/2/3/4

All machines are remotely managed through the ELFms suite. Initial configuration is ensured by the CERN System Administration Team.

3.10 SRV-PR-1/3

ATLAS/CMS VOCs are reported as responsible people for the machines in LANDB. ATLAS/CMS VOCs are registered as main users. These are the security contact people to be notified in case of a security incident. This information is reviewed everytime there is a change in the machine configuration or network configuration or in case of VOCs departures.

3.11 SRV-PR-2

ATLAS/CMS VOCs are bounded to the CERN/IT SLA in terms of VOBOX management.

3.12 SRV-PR-4

All ATLAS/CMS Web Redirector machines are managed through quattor. Web Redirector software and configuration files are stored in ATLAS/CMS quattor repositories in rpms format. Furthermore, all ATLAS/CMS web services configuration files for the Web Redirector are also stored as rpms in ATLAS/CMS quattor repositories. Quattor components such as filecopy, dirperm, accounts, etc. are used in order to avoid any manual intervention and to recover the machine quickly in case of a disaster. We avoid specifying versions in templates so that updates can be propagated. Versions are specified whenever unavoidable. We have a well defined set of templates with an agreed organization for the configuration of the Web Redirector services and the services behind it running on the same machine.

3.13 SRV-PR-5

The Web Redirector itself does not use configuration files with sensitive information. For services hosted on the same machine where the Web Redirector runs, we impose the compilation of service documentation cards in order to make sure such services are well under control and secure.

3.14 SRV-PR-6/7/8

ATLAS has established a set of procedures to handle emergency measures (https://twiki.cern.ch/twiki/bin/view/Atlas/ADCMachinesHowto#Procedures). We are working with ATLAS to improve and complete such set. We intend to discuss the same procedures with CMS.

3.15 SRV-PR-9

The procedures for the re-installation of a Web Redirectors are documented [7]. At the moment the documentation is ATLAS specific. We are working on more detailed and general instructions. Furthermore, we are preparing a tutorial for ATLAS and CMS VOCs.

3.16 SRV-SW-1

For what concerns OS security updates, we react within hours to the security announcements by CERN/IT. In case the security update requires a reboot of the service we apply the procedures in place [8]. VOCs are bounded by the availability constrains of the services behind the Web Redirector. Some of the services behind the ATLAS/CMS Web Redirector can be moved behind other Web Redirectors in order to apply the requested security patch. Sometimes this operation might take long since IP addresses of Web Redirectors are hardcoded by machines at the pit in order to strictly control access.

3.17 SRV-SW-2

We would like to have support from CERN/IT for the software we use for the ATLAS/CMS Web Redirector service. Besides the OS, we depend on specific versions of Apache and its modules to make the service work. Therefore, it is not easy to apply automatic patching/updating procedures. Please, check 3.21 for further details.

3.18 SRV-SW-3

The ATLAS/CMS web service redirector runs under SLC5. Only the basic SLC5 OS installation is needed for these machines.

3.19 SRV-SW-4

No special virus signature files are available. As a protective measure, the list of files and their checksum is stored. Files checksums can be compared in case of problems. It is in the plans to write small tools to automate such operation.

3.20 SRV-SW-5

The list of installed applications is kept to the minimum and reviewed everytime a new feature or modifications to the services are introduced.

Each ATLAS or CMS service running on or behind the Web Redirector is described by a service documentation card in which the contact people and the people needing administrative access to the service are clearly listed. Such service documentation card is reviewed on a quarterly base, after the reminder sent by the VOC. An example of such a service documentation card can be found here:

https://twiki.cern.ch/twiki/bin/view/Atlas/AtlasLarMonService

Specific software needed by a service hosted on the same machine where the Web Redirector runs is installed on the machine.

3.21 SRV-SW-6

We try to be pro-active and check for security updates for the software used. We manually check on a monthly base for security updates for the packages/versions we use. We would appreciate very much to have CERN/IT support for the software modules we depend on. The request has already been put forward.

3.22 SRV-SW-7

The Web Redirector runs under the “apache” account. Other ATLAS/CMS specific services that might be hosted on the same machine run under non-priviledged accounts with no login access.

3.23 SRV-SW-8/9

For activities executed with system privileges, we are planning to use secure bash. However, at the moment this is not done.
Off-server storage for the logs is in the plans but not yet done. We plan to contact IT/PES to implement that.

3.24 SRV-SW-10

The monitoring of the logs is done on a best-effort base. This is because of man power reasons. We plan to contact IT/PES to implement that.

3.25 SRV-SW-11/12

We use the Apache ModSecurity module. In particular we use the “negative security model”. We will follow further recommendations coming from the CERN Security Team.

3.26 SRV-TR-1/2/3

We are planning to organize ATLAS/CMS web service redirector traning. We will also focus on security. We would like to review our training material with the CERN Security Team in order to receive advice.

4. SECURITY BASELINE FOR WEB HOSTING VERSION 1.0 EDMS ID 1062502

As previously stated the ATLAS/CMS Web redirector is a web application firewall providing the features stated in the “Scope” section.

4.1 WEB-AC-1/2/3

The CERN Shibboleth2 SSO service is used to allow access to CERN-authenticated users. Normally access is granted through experiment specific e-groups. The management of these e-groups is done within the experiment. The documentation about who has access to a web service hosted behind a Web Redirector is done by the experiment service providers.

4.2 WEB-PRV-1

This web service is indeed a reverse proxy and as such WEB-PRV-1 does not apply.

4.3 WEB-PRV-2/3/4/5

This is done through the Quattor/ELFms templates as described in the service baseline sections. The Web Redirector is also well documented as specified before.

4.4 WEB-PRV-6

This is done either by running the Web Redirector on a physical machine where nothing else runs or by using virtual machines. For the latest, the results of the "VOBOX Consolidation Project" will be used.

4.5 WEB-PRV-7

Please check section 3.10.

4.6 WEB-ADD-1

Please, check previous sections.

5. REFERENCES

[1] CERN/IT VOBOX SLA https://twiki.cern.ch/twiki/pub/FIOgroup/FsSLA/sla-v1.2.1.pdf
[2] Apache ModSecurity http://www.modsecurity.org/documentation/
[3] https://espace.cern.ch/authentication/CERN%20Authentication%20Help/Shibboleth.aspx
[4] Frontier-squid https://twiki.cern.ch/twiki/bin/view/PDBService/SquidRPMsTier1andTier2
[5] The Webalizer http://www.webalizer.org/
[6] ELFms and other related tools https://twiki.cern.ch/twiki/bin/view/FIOgroup/ServiceManagersStartHere
[7] Installing a Web Redirector https://twiki.cern.ch/twiki/bin/view/Atlas/WebRedirectorService
[8] ATLAS Procedures https://twiki.cern.ch/twiki/bin/view/Atlas/ADCMachinesHowto#Procedures