



The Willard Office Building
1455 Pennsylvania Avenue, NW
10th Floor
Washington, DC 20004
Phone: (202) 434-9213
(202) 448-1985
Fax: (866) 516-6923

Security Infrastructure for SEC Filer Member Rules

Overview

The infrastructure to run the rules is comprised of a core processing engine that takes XBRL filings and analyzes the filing against a set of checks developed by XBRL US. These checks are designed to detect errors and inconsistencies in a filing related to the use of the XBRL US GAAP Taxonomy that can be resolved by an issuer prior to filing with the SEC.

To use the checks there are two implementation options available:

1. Server based service run remotely
2. Local software with check support

Server Based Solution

In this scenario the company connects to a web based service (called the service) through one of the following:

1. The XBRL US Flex application located at <http://csuite.xbrl.us>; or
2. Directly via a web link at <https://services.xbrl.us:8443/services/validate>

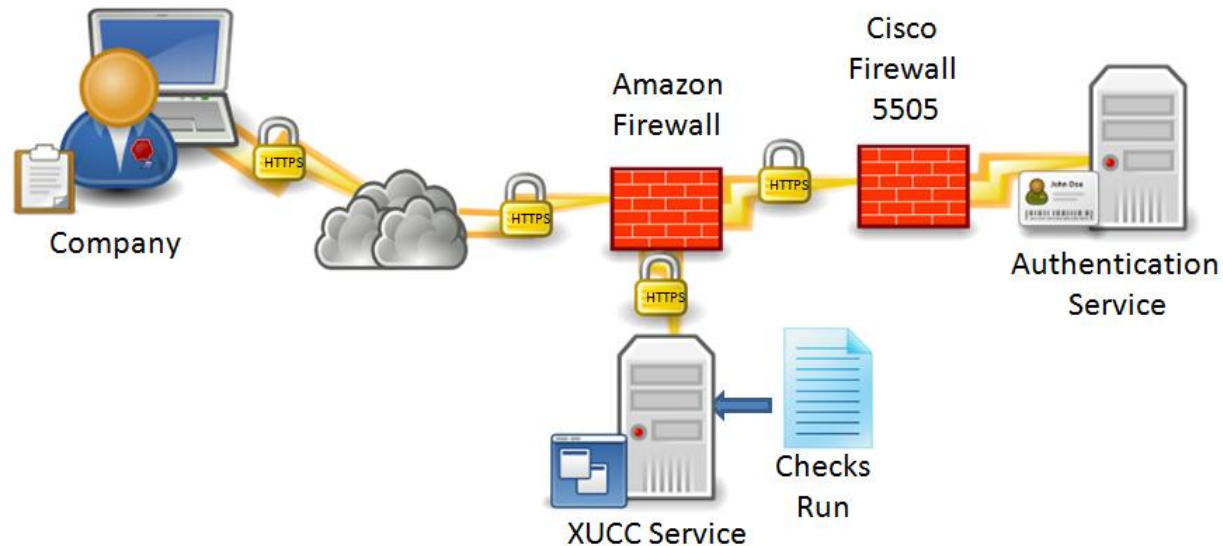
Both of these methods connect to the service located on a UNIX server running Debian Linux. This is a dedicated server that only runs the service. This server is hosted on the Amazon cloud. The server runs the following applications:

- SSH to connect to the box
- TomCat to run the service

Security Infrastructure for SEC Filer Member Rules

Figure 1 details the different components.

Figure 1 Remote Server Configuration



All communications with the service runs over https and require user authentication.

Connections to the service through the FLEX application or Web link perform in an identical manner. A username, password and CIK must be provided to run the checks. These are encrypted over the wire using https and are not stored at any point.¹ The service does not validate the user. The service passes on the authentication function to the XBRL US authentication service (Microsoft CRM V4). Upon receiving an approved authentication message from the authentication server the service will validate the filing. The service performs the following tasks:

- Receives the request from the issuer
- Authorizes the user
- Runs the checks against the latest set of rules
- Passes the results back to the user
- A log file records the user request, the file name and an error message if applicable

The service is written in Python and uses Arell to parse the XBRL file. All the XBRL filing information is read into the memory of the processor and the checks are executed.

Upon completion of the checks the application releases all references to the input XBRL documents and the results so they are no longer reachable from the code. At no point are the XBRL files stored on the service other than their temporary existence in the memory of the service.

¹ The username can be written to disk of the user using the Flex application if they indicate that they want the application to remember their username. The FLEX application does not allow the user to save their password.

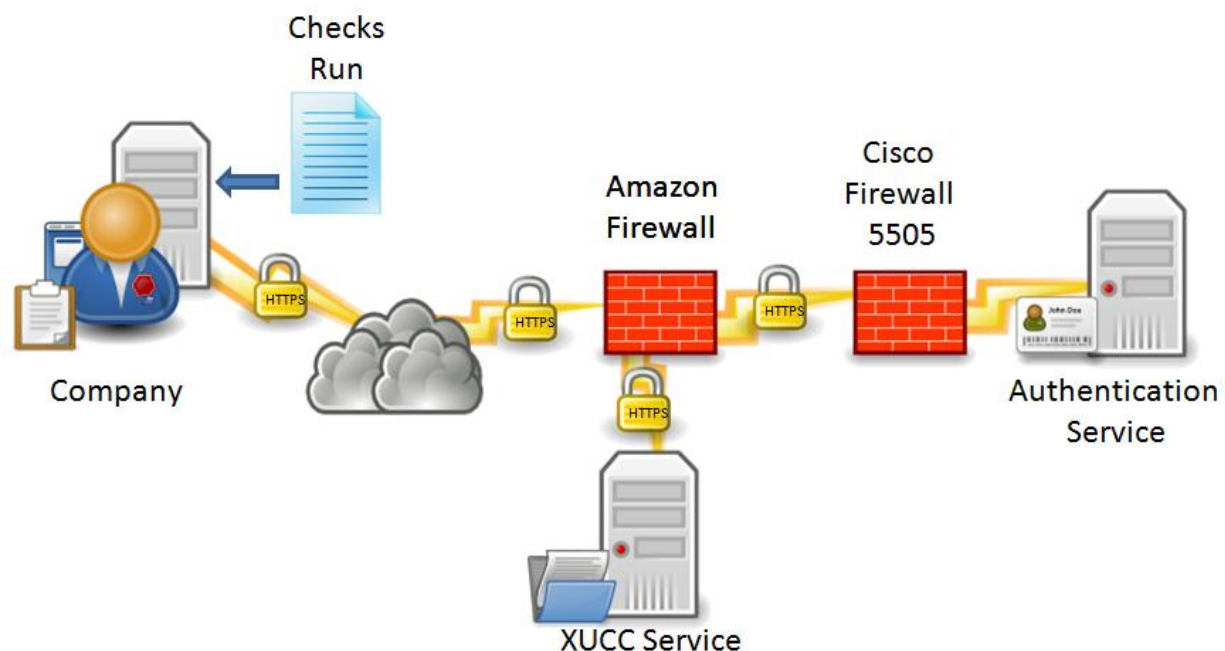
Security Infrastructure for SEC Filer Member Rules

Local Software with Support for SEC Filer Member Rules

In this scenario the company uses local software to run the checks. The software is effectively a copy of the service sitting on an individual user's computer. This implementation does require that the user is able to make a connection to the service to download the latest copies of the rules and authenticate themselves against the authentication server in order to use the checks. This option is currently supported by Magnify2.

Figure 2 shows the physical structure of how a connection is made to the server.

Figure 2 Local Software Configuration



When software is used locally, the user is asked to connect to the server to be authenticated and to get the latest rules if they do not have them. This requires an https connection.² Membership does not include the cost of purchasing software to run the checks locally as these are provided by third party vendors.

Questions

If you have any questions please contact David Tauriello at XBRL US at david.tauriello@xbrl.us.

² In some cases the IT department may have to give the user the ability to access a secure site as these are often blocked. We do not offer an unencrypted connection.