Security Infrastructure Overview - XBRLUS Consistency Suite

Overview

The consistency checks are 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 consistency checks there are three implementation options available:

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

Server Based Solution

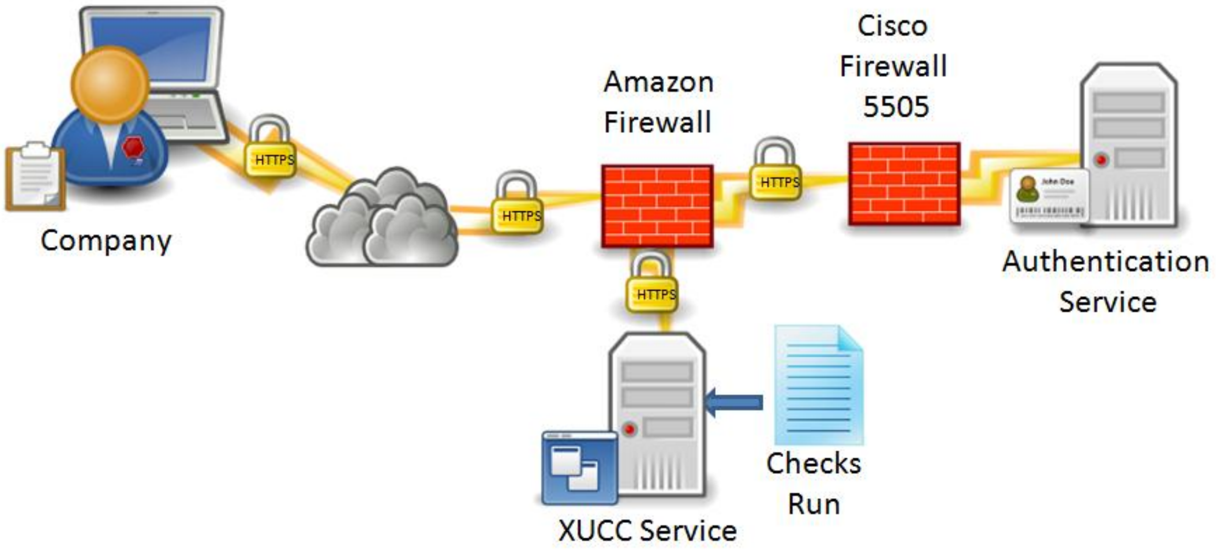
In this scenario the company connects to a web based service called the XUCC service through one of the following:

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

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

Figure 1 details the different components.

Figure 1 Remote Server Configuration



The XUCC server runs the following applications:

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

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

Connections to the XUCC service through the FLEX application or Web link perform in an identical manner. A username and password must be provided to run the checks. These are encrypted over the wire using https and are not stored at any point. [1] The XUCC service does not validate the user. The XUCC 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 XUCC service will validate the filing. The XUCC service performs the following tasks:

- Receives the request from the issuer
- Authorizes the user
- Runs the consistency 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 XUCC service is written in Java and uses the CoreFiling True North XBRL engine to parse the XBRL file. All the XBRL filing information is read into memory of the processor and the checks are executed.

Upon completion of the checks the XUCC application releases all references to the input XBRL documents and the results so they are no longer reachable from the XUCC code. The Java Virtual Machine is then responsible for final clean-up (and eventual reuse) of that memory as part of its periodic "garbage collection". At no point are the XBRL files stored on the XUCC service other than their temporary existence in the memory of the service.

In addition to the flex application and the website the XUCC service is supported with tools from XBRL Cloud which use the server based solution to check the consistency of filings.

[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 Overview - XBRLUS Consistency Suite

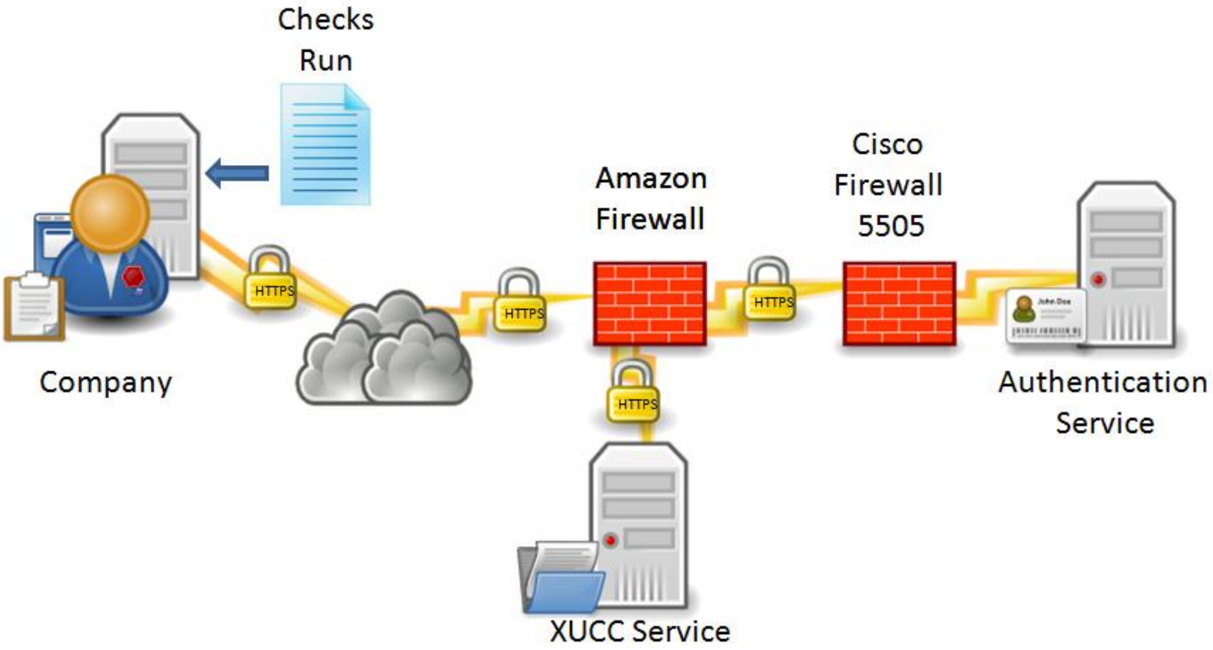
Local Software with Consistency Check Support

In this scenario the user uses local software to run the checks. The software is effectively a copy of the XUCC service sitting on an individual user's computer. This implementation does require that the user is able to make a connection to the XUCC 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 with the Magnify tool - additional vendor tools will be added over time.

Purchasing the Consistency Suite allows you to use both local and server side implementations concurrently with the same license.

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

Figure 2 Local Software Configuration



When software is used locally, the user is asked to connect to the XUCC server to be authenticated and to get the latest rules if they do not have them. This requires an https connection.[2] The cost of this solution will also include the cost of purchasing the 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.