Pass the real client IP to the Shibboleth SP when your site is behind a load balancer

Please read this page if you are using the Shibboleth Service Provider (SP) and your website is behind a load-balancer.

Background about the problem

The Shibboleth Service Provider (SP) has some security features that watch for changes in the client's (i.e. user's or web browser's) IP address, and interpret these as potential session hijack attempts. When the client IP address changes, the SP kills the existing session and sends the user back to the IdP to log in again.

For the most part, this is probably a good behavior for it to have -- an extra layer of security.

But if your website is behind a load-balancer and not configured to use the actual client IP address instead of the load balancer IP address, there can be some unintended consequences. If the SP sees the load-balancer IP instead of the browser's IP, then the SP session will reset whenever the load balancer's IP changes. For example, when there are multiple load-balancer nodes in the pool and the user's HTTP request comes in through a random node, then the SP session will reset once every few minutes. From the end-user's perspective, it looks like the session expired early and they have to log in again.

Most of the time, this is an annoyance and a bad user experience: the user has to log in again, then can continue with whatever they were doing. It gives the impression that the Single-Sign-On (SSO) is not working, or that the application's session timeout is too short.

In some edge cases, due to interactions with browser behaviors around third-party cookies (e.g. if the affected HTTP request is in an iframe), this can cause more serious problems where the user is not easily able to log in and continue with what they were trying to do. They will get the "Stale Request" error instead of the login page.

Solution

In order to avoid this kind of problem, please make sure that your web server is passing the SP the client's actual IP address, and not the load-balancer's address. Typically, this is done by passing it the forwarded address that the load balancer tells you (e.g. "X-Forwarded-For") instead of the remote address.

The best way to accomplish this is to fix it in the web server. The Apache httpd web server comes with a module for doing this called mod_remoteip. https://httpd.apache.org/docs/2.4/mod/mod_remoteip.html
This is the best way because it will fix many similar issues in one step:

- the apache audit logs will show the correct IP address
- the application audit logs will show the correct IP address
- any application behaviors that depend on knowing the client's IP address will function
- the Shibboleth SP audit logs will show the correct IP address
- the Shibboleth SP will know the correct client IP address, which will avoid the problem described on this page

If you just want to target the change to the SP (e.g. because the application is already looking at the X-Forwarded-For header), or if you are using IIS instead of apache, you can use the "REMOTE_ADDR" setting in the SP's RequestMapper to pass the client's address to the SP module. This may not solve the other issues mentioned above (audit log accuracy, etc). https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334723/ContentSettings

Workaround

If you are being affected by this issue but are unable to implement the solution (i.e. by passing the correct IP address to the SP module), you can work around it by turning off the SP's consistency check on the IP address.

This is the "consistentAddress" setting in the Session configuration, mentioned on this page: https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334342/Sessions

Please check to make sure that you also have "checkAddress" off (that does a similar consistency check between the IP address that the SP sees, and the IP address that the login page saw when the user first logged in).

Disabling this check will create some additional risk of a successful session hijack attack, but it is not a huge amount – that kind of attack ought to be difficult to do in any case.

More Information

This is the Shibboleth team's documentation about this issue: https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2110390365/AddressChecking