

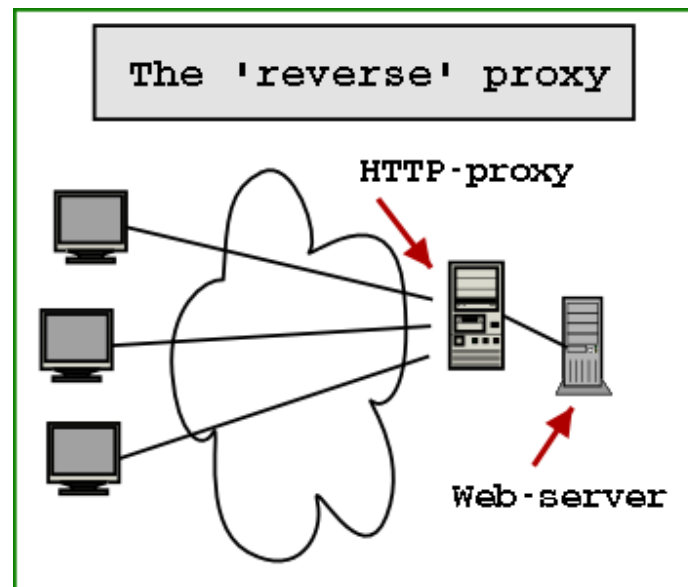
SWITCHaai & Swiss edu-ID Update 2015

SP REVERSE PROXY SERVER AT ZHAW

- What are we talking about?
- Why we operate one at ZHAW?
- Why this could be interesting for others, too.
- How it's done.
- Getting help.

SP Reverse Proxy Server at ZHAW

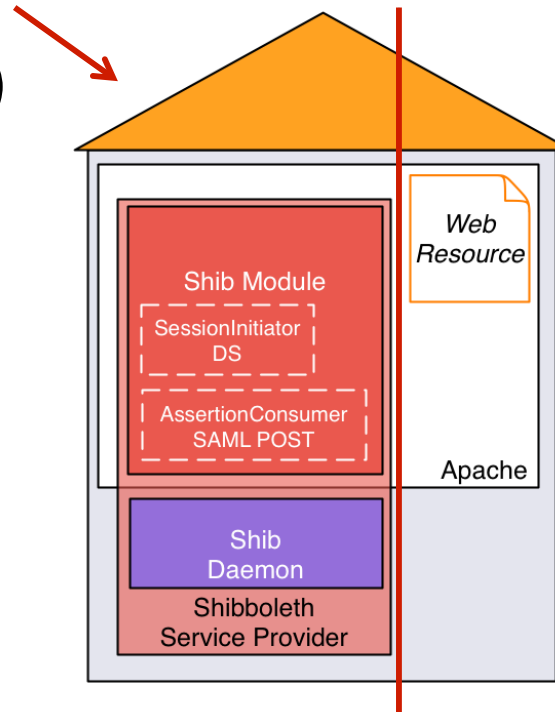
Reverse Proxy 101



SP Reverse Proxy Server at ZHAW

How to reverse proxify a Shibboleth SP?

**HTTP-proxy
(with mod_shib)**



Web-server

SP Reverse Proxy Server at ZHAW

But why?

In 2011, only one reason:

Compiling library dependencies on Solaris 

Moving web server to another OS 

Split the SP functionality and the web server 

SP Reverse Proxy Server at ZHAW

It's a good thing...

Pros:

- Less time to add new SPs
- Reduced complexity on web servers
- No need to update 23958 systems on a new SP version
- Option to use different web servers
- Security
- Easy to set up

SP Reverse Proxy Server at ZHAW

... but it has its drawbacks.

Cons:

- Easy to upset: Single Point of Failure
- Debugging web traffic involves (at least) two systems
- May get difficult to use with load balancing / clustering
- Configuration may get complex if every SP has other settings
- Security

SP Reverse Proxy Server at ZHAW

Configuration overview – Shibboleth

- ApplicationOverrides

```
<ApplicationOverride
```

```
  id="webtools"  
  entityID="https://webtools.zhaw.ch/shibboleth">
```

```
  <CredentialResolver
```

```
    type="File"  
    key="/etc/pki/tls/private/webtools.zhaw.ch.key"  
    certificate="/etc/pki/tls/certs/webtools.zhaw.ch.crt.pem"/>
```

```
</ApplicationOverride>
```

SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Authentication

```
<Location />  
    AuthType shibboleth  
    ShibRequestSetting requireSession 1  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require valid-user  
</Location>
```


SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Reverse Proxy directives

```
SSLProxyEngine On  
ProxyRequests Off  
ProxyPass / http://webtools-intern.zhaw.ch/  
ProxyPassReverse / http://webtools-intern.zhaw.ch/  
ProxyPreserveHost On
```

SP Reverse Proxy Server at ZHAW

Configuration overview – HTTPD

- Authentication for subdirectories

```
# The Shibboleth handler shall process all HTTPS requests...
```

```
<Location />  
    AuthType shibboleth  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require shibboleth  
</Location>
```

```
# ...but only enforce a session for the locations below.
```

```
<Location /secure>  
    AuthType shibboleth  
    ShibRequestSetting requireSession 1  
    ShibRequestSetting applicationId webtools  
    ShibUseHeaders On  
    Require valid-user  
</Location>
```

SP Reverse Proxy Server at ZHAW

Where can I get help?

Shibboleth Wiki:

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplicationOverride>

SWITCH AAI Wiki:

<https://wiki.aai.switch.ch/twiki/bin/view/AAIResources/ShibbolethReverseProxy>

aai@switch.ch