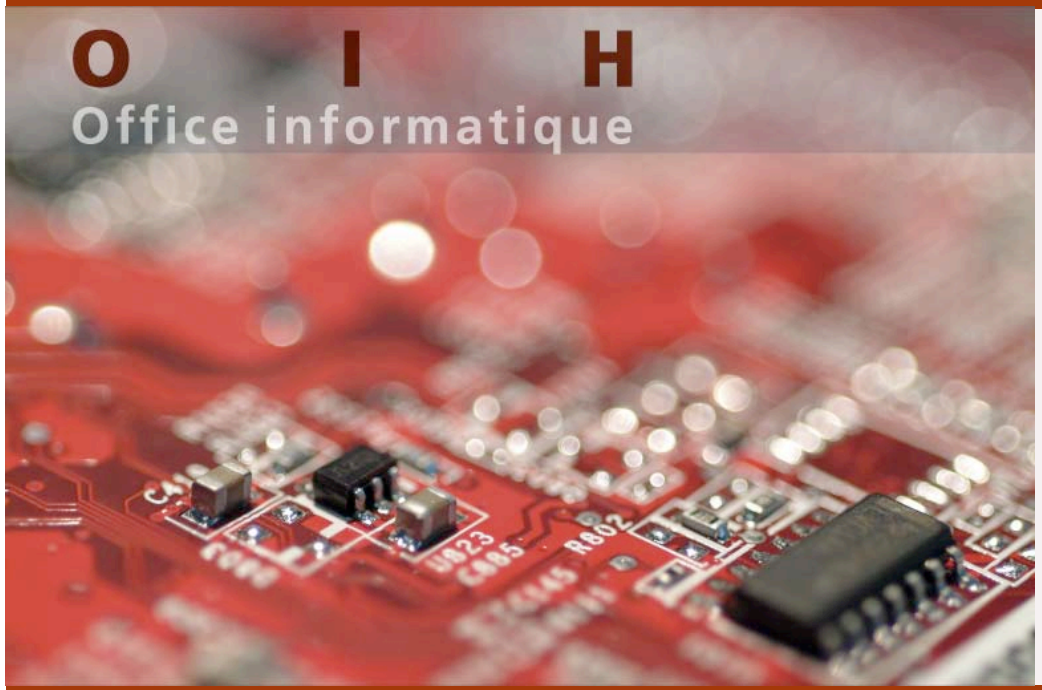


AAI @ CHUV

Vincent Bex
Systems Engineer
Vincent.Bex@chuv.ch

Patrick Zosso
Infrastructure Project Manager
Patrick.Zosso@chuv.ch

Agenda

- Presentation of the CHUV
- Security concepts at CHUV
- The challenge
- AAI implementation for UNIL students

Some indicators

- 7100 Employees + 400 Students
- 1300 Beds
- 2 campuses and several small remote sites

O I H Office informatique

- Equipments
  - PC 7000
  - Printers 1930
  - Servers 250
  - Applications 750
  - Storage
    - 70Tbytes

O I H Office informatique

- Locations
  - One LAN spread on 2 main campuses
  - 23 Small remote sites
- 385 network equipments
  - VPN
  - Firewalls
  - Routers
  - Switches
  - WiFi
  - …

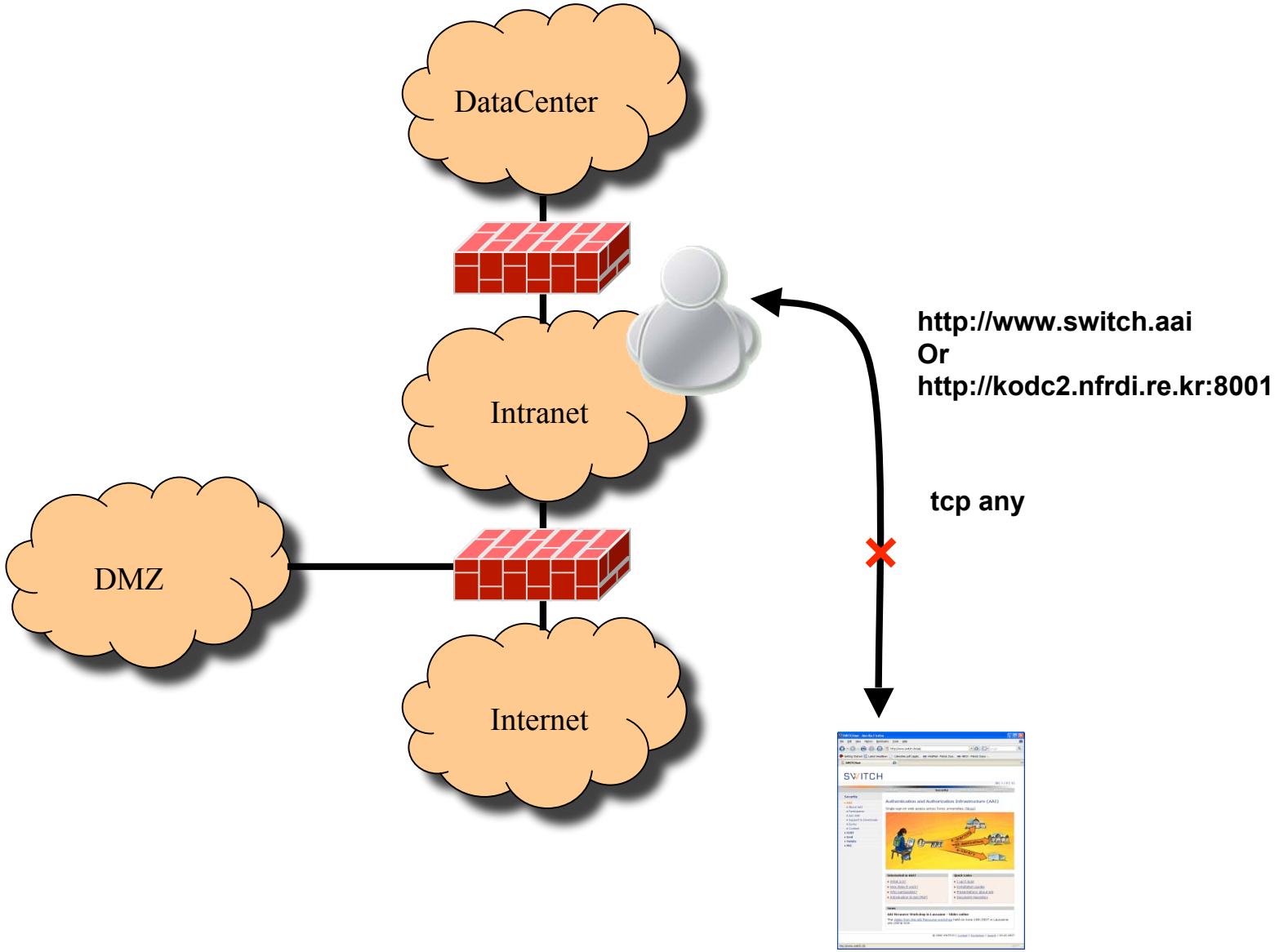
Agenda

O I H Office informatique

- Security concepts at CHUV
- The challenge
- AAI implementation for UNIL students

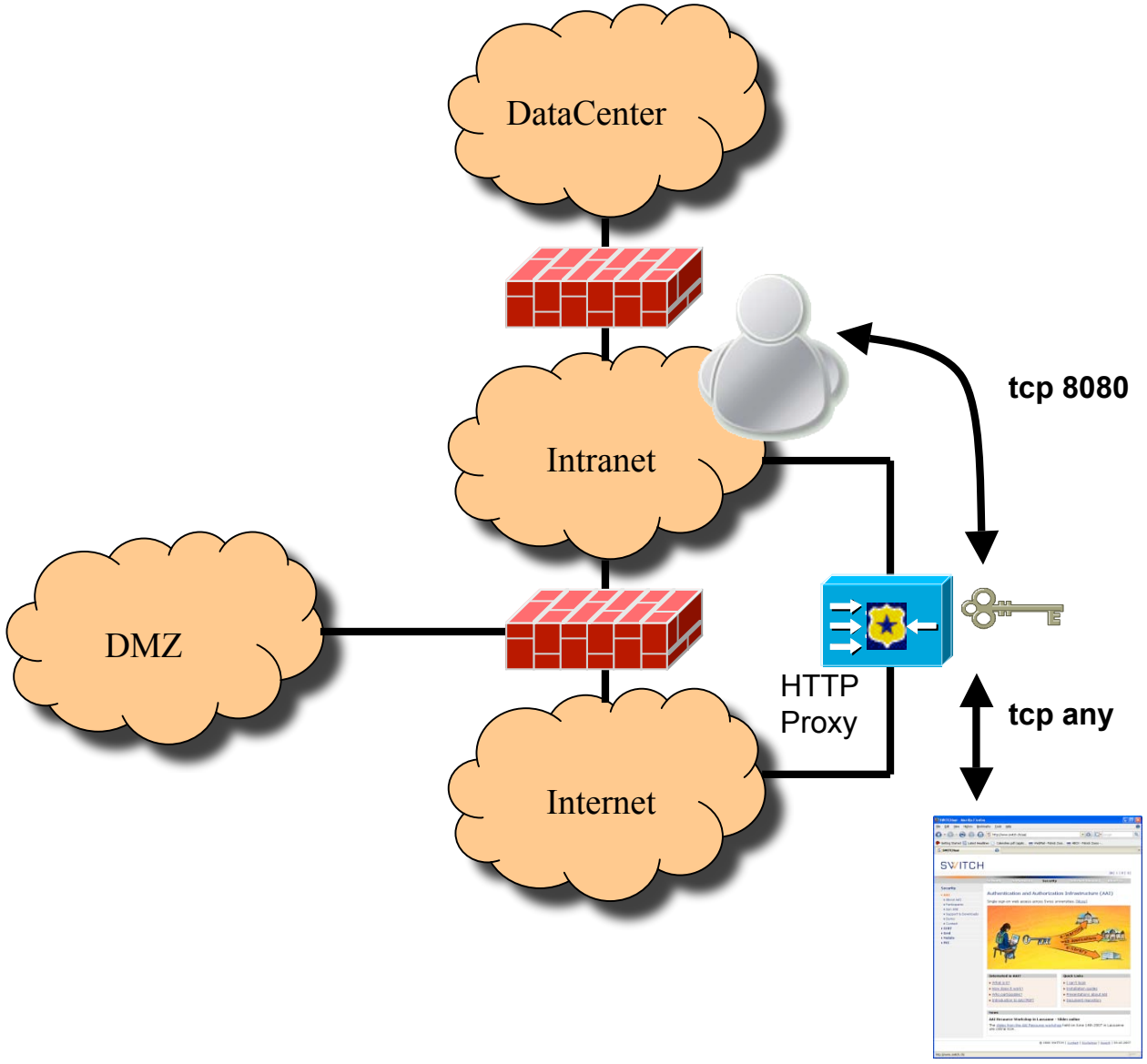
Security concepts at CHUV

O I H Office informatique



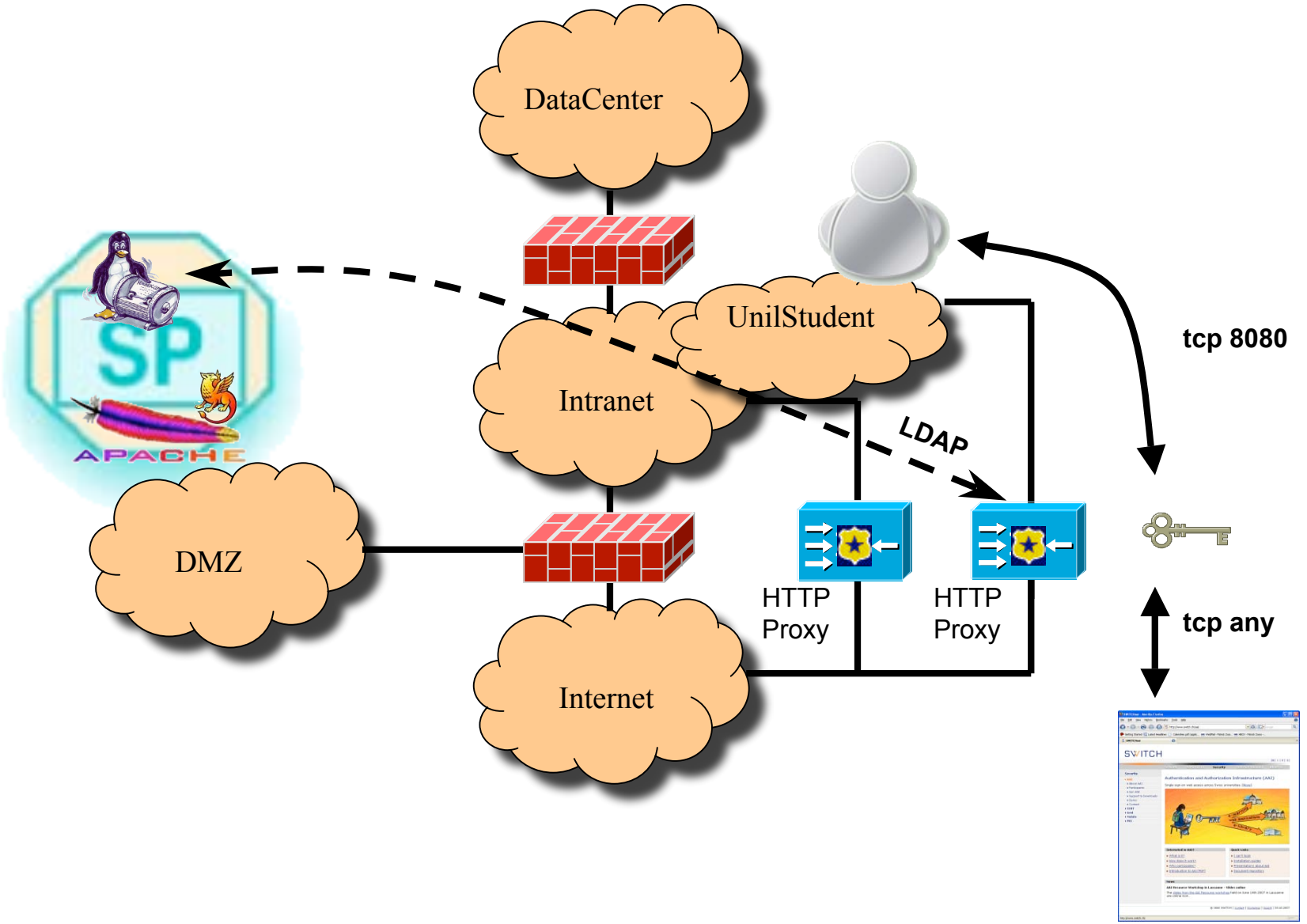
Security concepts at CHUV

O I H Office informatique



Security concepts at CHUV

O I H Office informatique



Agenda

O I H Office informatique

- The challenge
- AAI implementation for UNIL students

The situation:

- Users who are not CHUV employees (UNIL students) need to access internet from our premises
- They use specific PCs from the library
- They use PCs configured to automatically logon with a generic account

The needs:

- We need to identify the users who access internet for policy enforcement purpose

The Challenge

O I H Office informatique

The environment:

- Our proxies are currently BlueCoat appliances
- BlueCoat does not support mod_shib authentication
- Shibboleth is “easy” to implement on IIS or Apache
- We need to force the PCs to use the proxy

The solution:

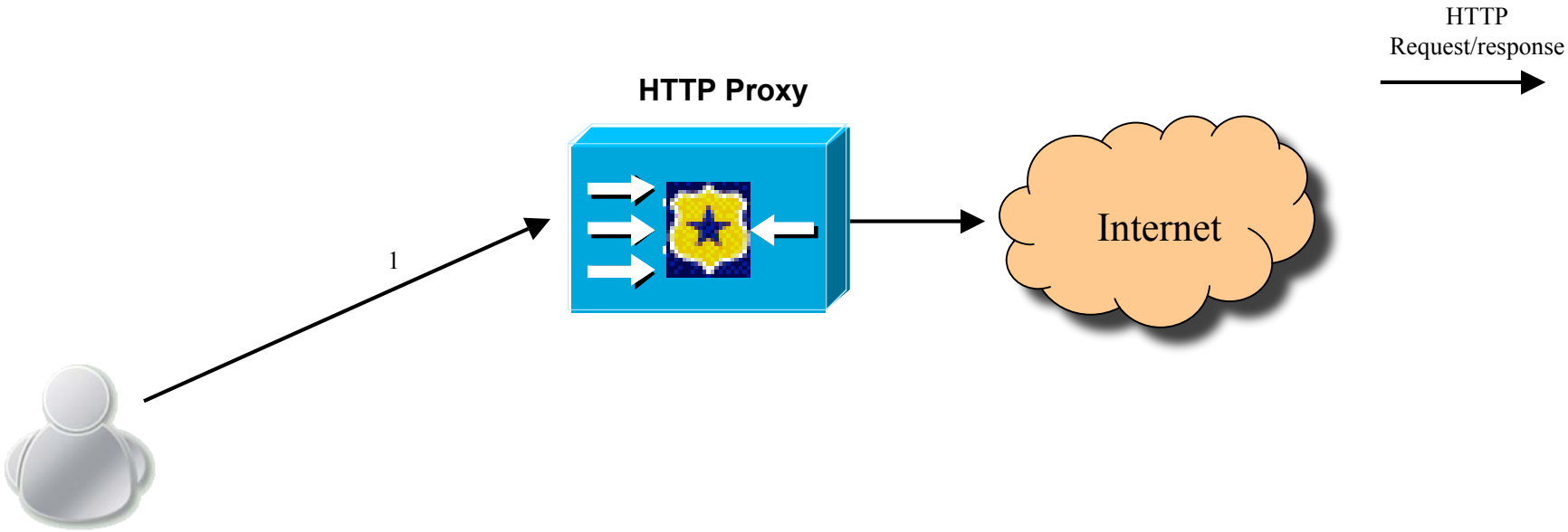
- A dedicated BlueCoat proxy
- A Service Provider on Debian 4.0
- Apache 2.2 with mod_shib enabled
- Open LDAP
- Two CGI scripts
- A GPO to force the user's PCs to use the proxy

Agenda

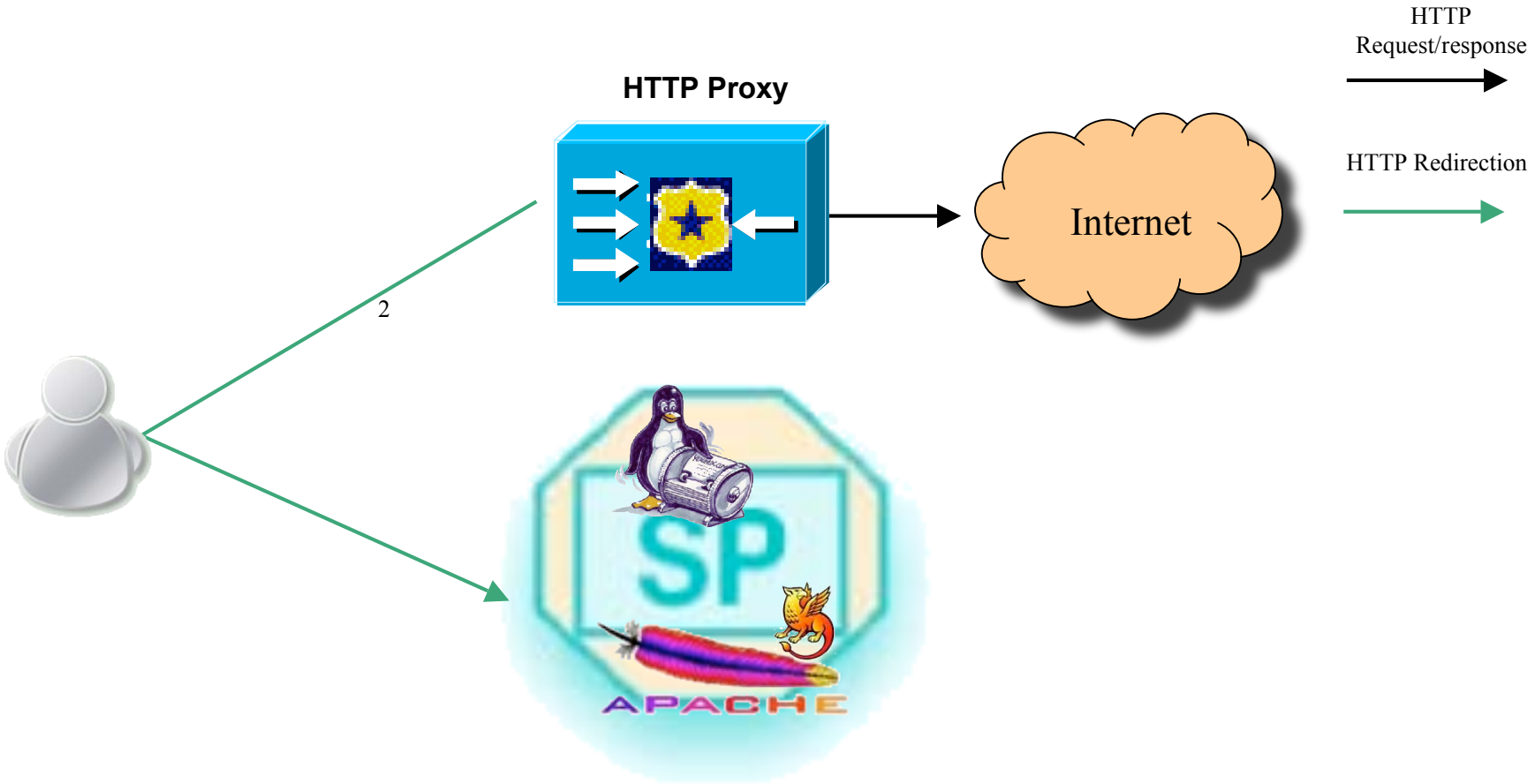
O I H Office informatique

- AAI implementation for UNIL students

1 Internet access request

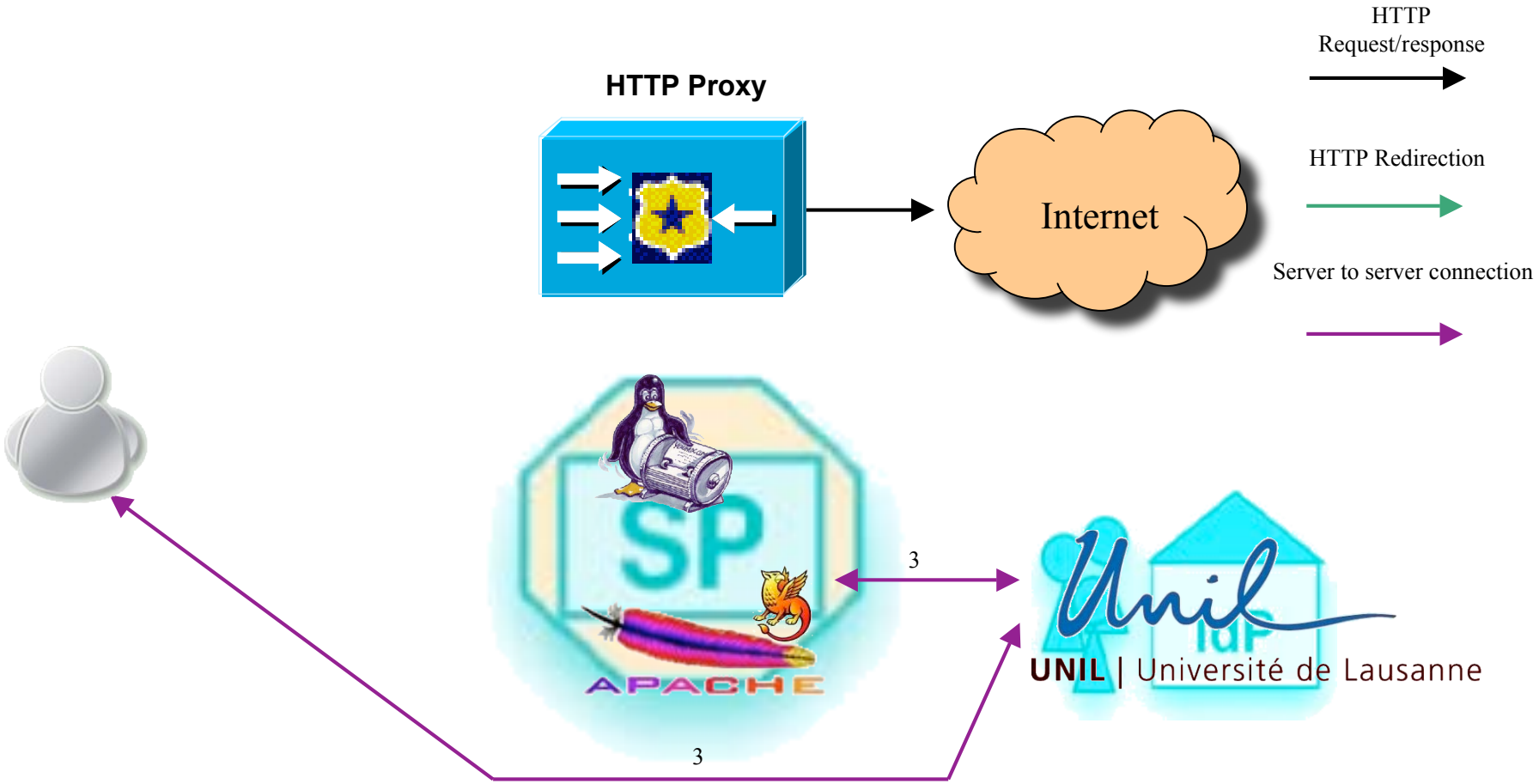


2 Redirection to a perl script protected by Shibboleth



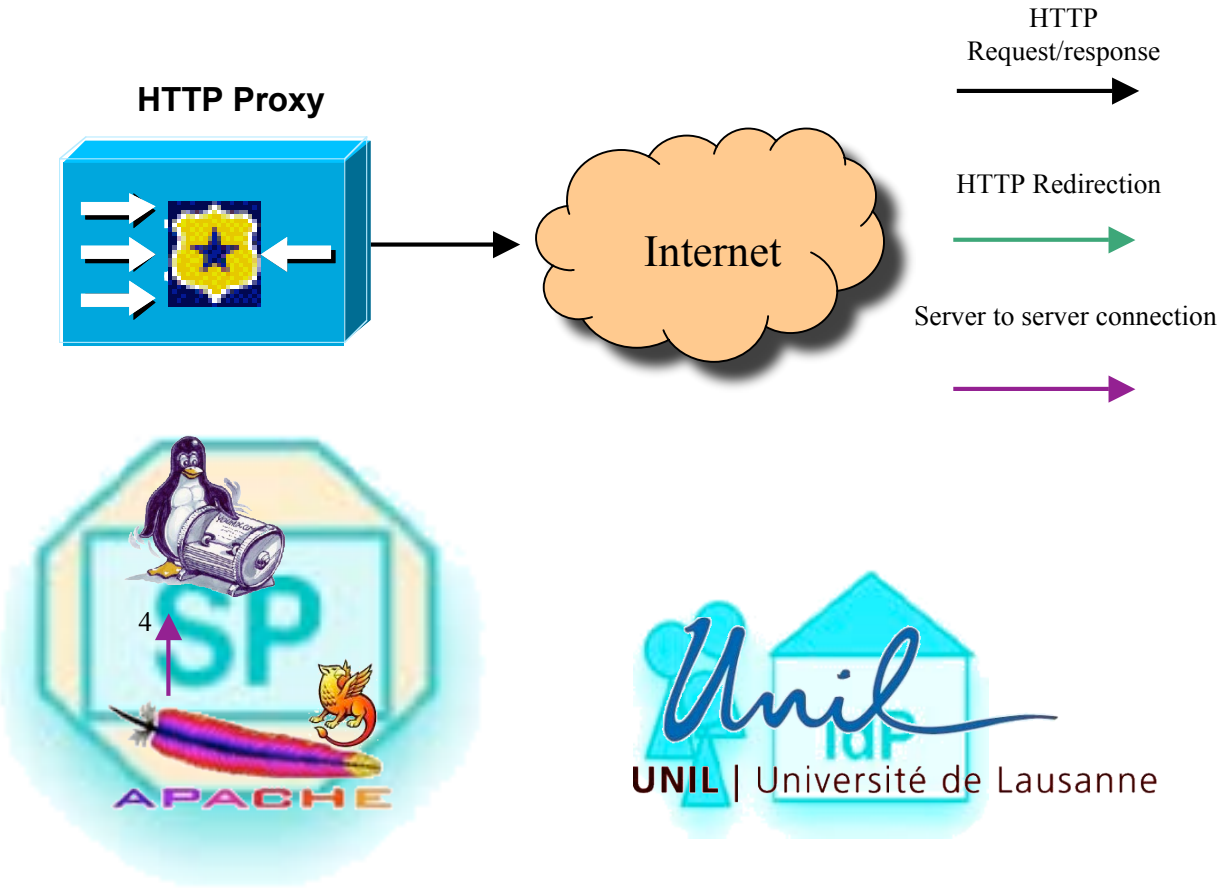
O I H Office informatique

3 AAI authentication



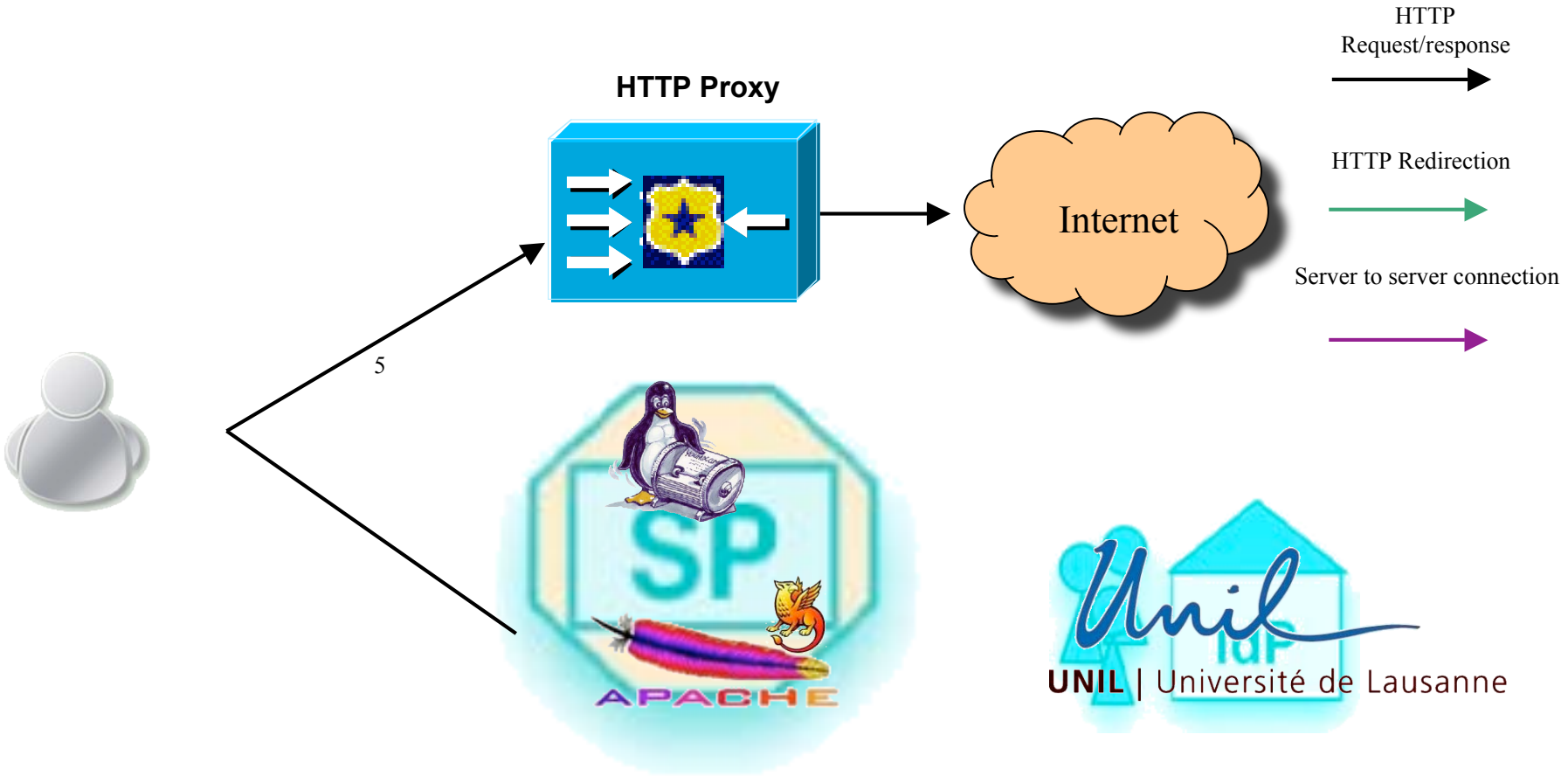
O I H Office informatique

4 Creating the LDAP user



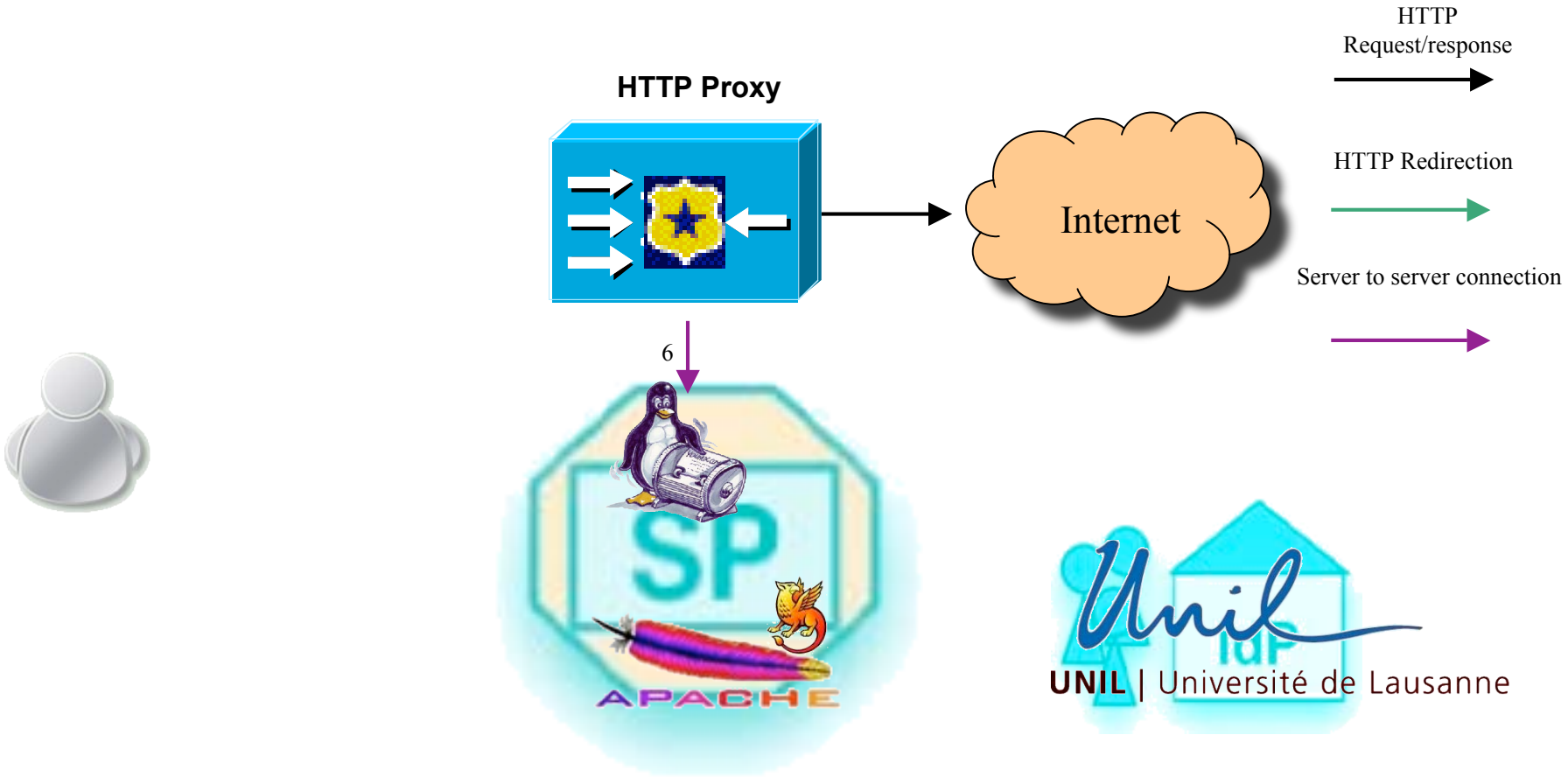
O I H Office informatique

5 Creating and sending the authentication form



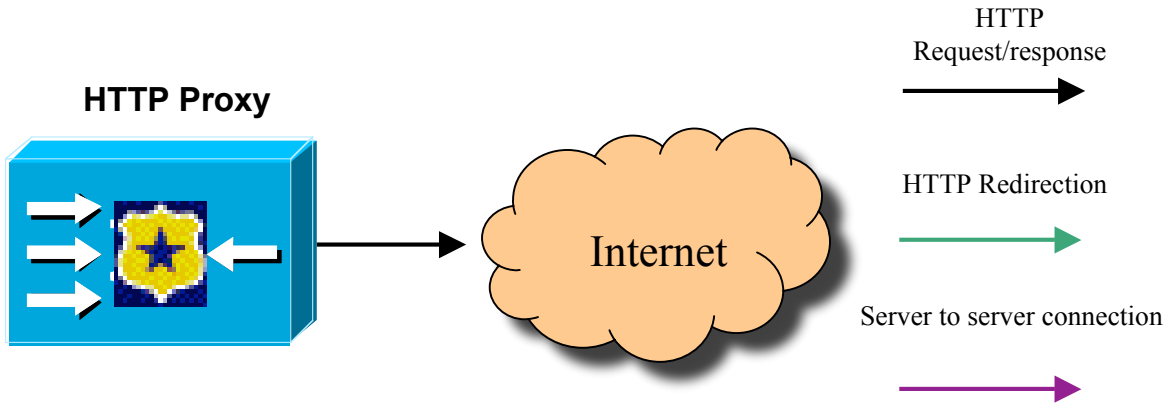
O I H Office informatique

6 The proxy requests authentication to the LDAP server



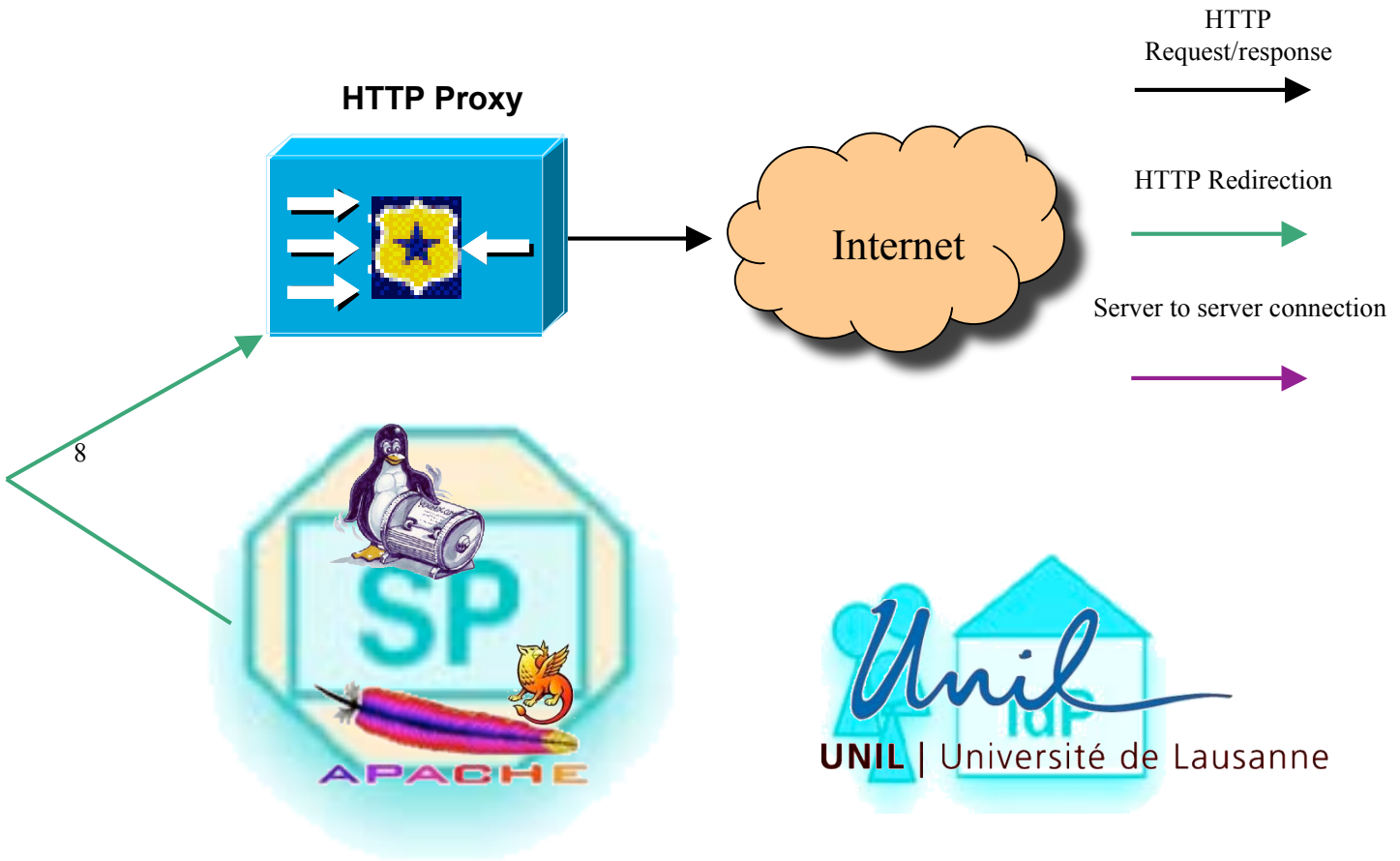
O I H Office informatique

7 LDAP user gets deleted



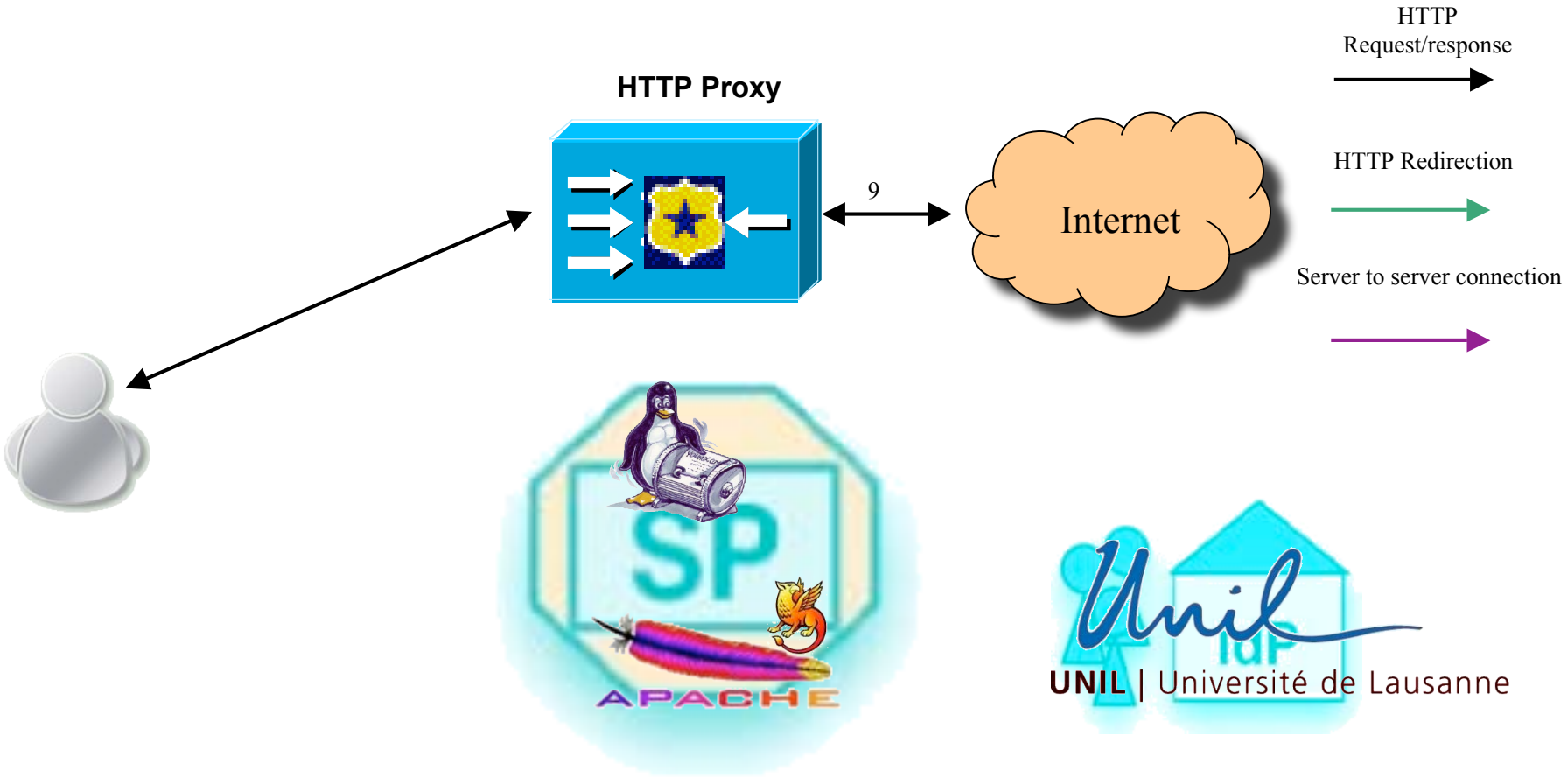
O I H Office informatique

8 Redirection to the requested URL



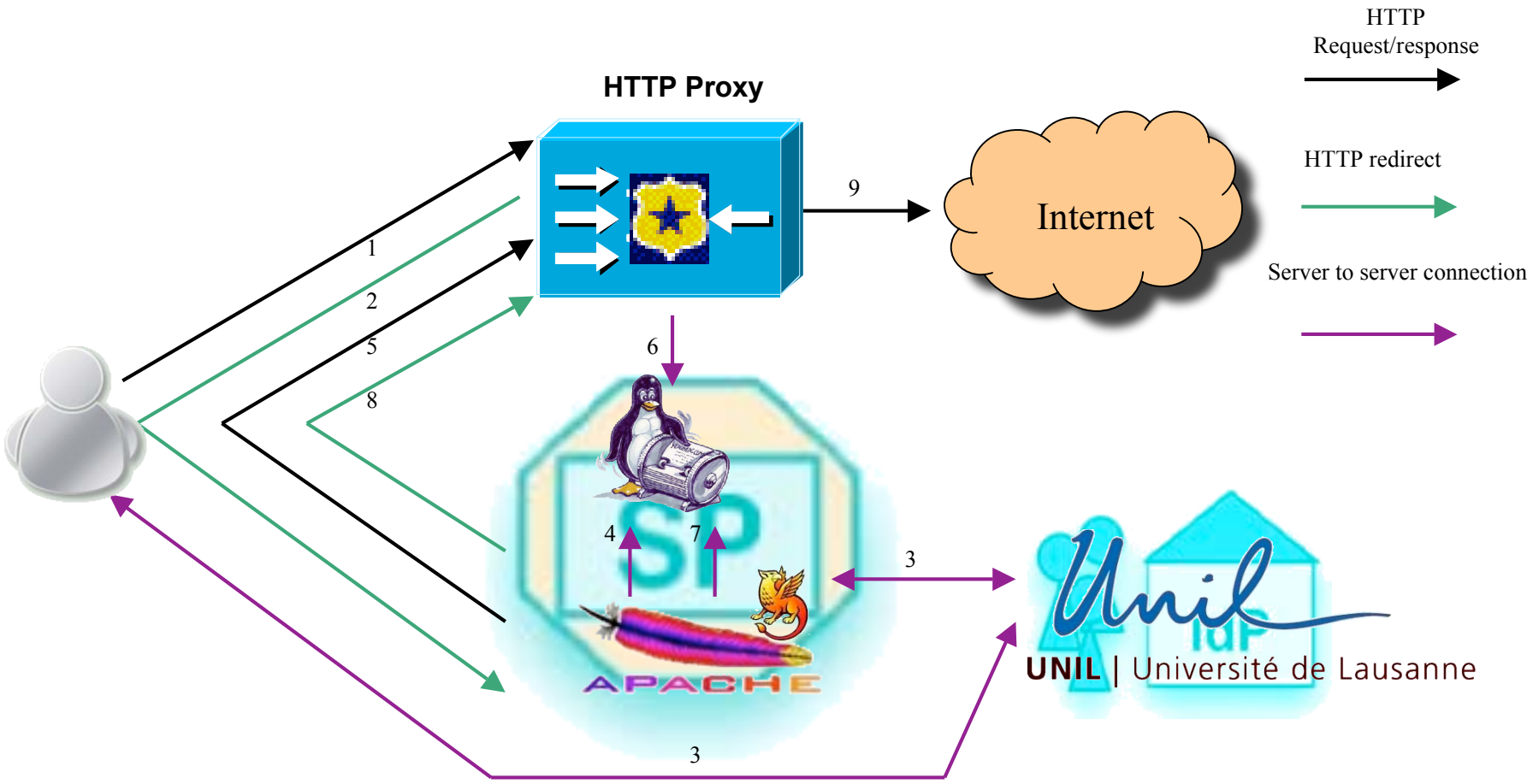
O I H Office informatique

9 Internet access



AAI implementation for UNIL students

O I H Office informatique



1 Internet access request
2 Redirection to a perl script protected by Shibboleth
3 AAI authentication
4 Creating the LDAP user
5 Creating and sending the authentication form
6 The proxy requests authentication to the LDAP server
7 LDAP user gets deleted
8 Redirection to the requested URL
9 Internet access

O I H Office informatique