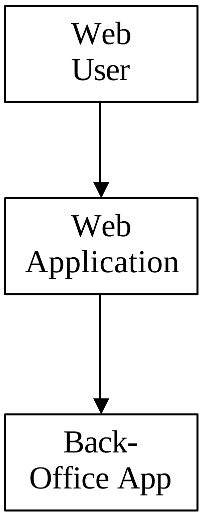
Back-office Scenarios

Back-office scenarios were originally proposed in an attempt to provide better security between security domains WITHIN a particular organization, rather than across them. This scenario was suggested in response to customers who wanted a better solution than using 'proxy' accounts to access back-end and legacy services.

The Problem:
Web-tier applications often need to access back-end applications, such as legacy order processing applications and databases. Authentication and authorization are handled in the web tier, at the 'front door', and so the user accounts are managed and maintained in a repository close to the web tier. The user accounts are NOT, however, replicated into the back-end applications that the web apps are accessing. Instead, a group of proxy accounts are established that the web applications use to access the back-end apps. This creates security problems – particularly related to audit-ability.

What customers require is a way to propagate web-tier authentication/session information to back-end systems. In some scenarios these back-end systems could be web services.


Web
User
Web
Application
Back-
Office App