



LEISTUNGSBESCHREIBUNG SOFTWAREPRODUKT SESAME LOGIN-PORTAL DER PROCONDO GMBH

Stand 08/2007

1 FUNKTIONSÜBERSICHT

Das Softwareprodukt „Sesame Login-Portal“ wird zwischen Web-Browser und Web-Server geschaltet. Es ermöglicht die Authentifikation und Autorisierung von Benutzern zu zentralisieren. Dazu bietet es folgende Funktionen:

- Betrieb als Reverse-Proxy
- Authentifikation
- Unterstützung von Basic Authentication
- Unterstützung von Form-Based Authentication
- Single Sign On
- Anbindung eines LDAP-Server
- Logging
- Sessiontracking
- SSL-Terminierung
- Sitzungsverteilung

2 PRODUKTEINSATZ

Das Login-Portal Sesame ist für Lizenznehmer gedacht, bei denen eine größere Anzahl von Benutzern zentralisiert Zugriff auf eine Reihe von Web-Servern erhalten soll.

3 PRODUKTUMGEBUNG – HARDWARE – SOFTWARE

Voraussetzung für den Betrieb von Sesame Login-Portal sind folgende Komponenten:

- Intel Pentium kompatible CPU
- Linux Betriebssystem ab Version 2.2
- Web-Browser kompatibel zu Internet Explorer 5.5
- Web-Server kompatibel zu Protokoll HTTP/1.0 oder höher
- Web-Browser und Web-Server konform zu RFC2965, RFC2617
- LDAP Schnittstelle kompatibel zu OpenLDAP

4 PRODUKTFUNKTIONEN

4.1 BETRIEB ALS REVERSE-PROXY

Ein von einem Web-Browser eingehender HTTP-Request wird von Sesame Login-Portal abgewandelt und an einen Web-Server weitergeleitet. Die Antwort des Web-Server wird dann vom Reverse-Proxy unverändert an den Web-Browser zurückgeleitet. Für den Web-Browser bleibt die Weiterleitung des Request unsichtbar, wenn der Web-Server mit dem Reverse-Proxy kooperiert. Damit der Web-Server unsichtbar bleibt, darf er insbesondere in der Antwort keine URL der Form „<http://x.y.z/>“ oder „/abc“ aufführen.

4.2 AUTHENTIFIKATION

Sesame Login-Portal kann so konfiguriert werden, dass die Abfrage bestimmter URL-Präfixe eine Authentifikation erfordert. Zur Authentifikation erfragt Sesame einen Benutzernamen und ein Kennwort. Auf Seiten des Browsers ist zwingend das Zulassen von Cookies erforderlich.

4.3 UNTERSTÜTZUNG VON BASIC AUTHENTICATION

Zur Authentifikation kann Sesame Login-Portal eine Antwort gemäß Basic Authentication übermitteln.

4.4 UNTERSTÜTZUNG VON FORM-BASED AUTHENTICATION

Zur Authentifikation kann Sesame Login-Portal eine vom Lizenznehmer konfigurierbare HTML-Seite übermitteln, die Formularfelder zur Angabe von Benutzername und Kennwort enthält.

4.5 SINGLE SIGN ON

Sesame Login-Portal übermittelt die Authentifikation eines Benutzers an die Web-Server mittels Basic Authentication. Ein einmal authentifizierter Benutzer wird durch Sesame erst bei Eintreten eines der nachfolgenden Ereignisse erneut zur Angabe von Benutzername und Kennwort aufgefordert:

- Inaktivität des Browsers über eine konfigurierbare Zeitspanne.
- Beenden der aktuellen Session.
- Versuch des Zugriffs auf eine nicht autorisierte URL.

4.6 ANBINDUNG EINES LDAP-SERVER

Sesame Login-Portal bietet eine Anbindung an einen LDAP-Server. Hierüber können die Angaben eines Benutzers bezüglich Benutzername und Kennwort mit denjenigen im LDAP verglichen werden. Sesame kann so konfiguriert werden, dass bei fehlender Berechtigung der Zugriff auf die Seiten des Web-Servers verweigert wird.

4.7 LOGGING

Eingehende HTTP-Requests werden von Sesame Login-Portal protokolliert.

4.8 SESSIONTRACKING

Wenn ein Web-Browser erstmalig einen Request an Sesame Login-Portal leitet, so übermittelt Sesame dem Browser ein Cookie mit einer eindeutigen Kennung. Diese Kennung wird in alle nachfolgenden Requests des Browser übernommen und kann von Sesame protokolliert werden. Auf Seiten des Browsers ist zwingend das Zulassen von Cookies erforderlich.

4.9 SSL-TERMINIERUNG

Sesame Login-Portal kann Requests sowohl über die Protokolle HTTP und HTTPS entgegennehmen und weiterleiten. Das Protokoll, in dem Requests entgegengenommen werden, ist unabhängig vom Protokoll, in dem Requests weitergeleitet werden. Aufgrund der Natur des HTTPS-Protokolls ist zu beachten, dass Sesame nicht dasselbe Zertifikat wie der dahinterliegende Web-Server verwenden kann.

4.10 SITZUNGSVERTEILUNG

Wenn ein Web-Browser erstmalig einen Request an Sesame Login-Portal leitet, so übermittelt Sesame dem Browser ein Cookie mit einer Sitzungskennung. Der Sitzungskennung wird fest eine Menge von Web-Servern zugeordnet. Nachfolgende Requests werden an dieselben Web-Server weitergeleitet. Durch regelmäßige Abfragen der Web-Server können Serverausfälle detektiert werden. Eine Sitzung wird beendet durch Abmeldung an Sesame Login-Portal oder durch Überschreiten einer Zeitspanne, in der keine Browseraktivität stattfand. Die Anzahl nachgelagerter Web-Server ist auf 1000 beschränkt.

5 TYPISCHES EINSATZSZENARIO

