InteProxy Server Dokumentation

Release 1.0.4

Bjoern Schilberg

16. 06. 2011

Inhaltsverzeichnis

Eine kurze Einführung

Der InteProxy Server ist eine Zugangshilfe für Klienten-Anwendungen zu einer sicheren Geodateninfrastruktur. Derartigen Anwendungen ermöglicht der InteProxy Server eine sichere Übertragung per Secure Sockets Layer (SSL) sowie eine Benutzeranmeldung am sicheren OGC Web Service (OWS) zu nutzen, sofern die Klienten-Anwendungen dies nicht selbst vermögen.

1.1 Unterstützte OWS-Absicherungs-Methoden

Zur Absicherung des OGC Web Services wird der deegree OWS-Proxy durch den InteProxy Server unterstützt. Hierbei werden die URL-Parameter `user=` und `password=` gesetzt. In Verbindung mit HTTPS kann jeder OWS Server, der genau diese URL-Parameter verwendet, bedient werden.

Voraussetzungen

Für den Betrieb des InteProxy Servers benötigen Sie,

- einen aktuellen Apache HTTP Server (mindestens Version 2.2.15),
- eine Python-Umgebung (optional),
- das *lxml XML toolkit* für Python.

Schnelleinstieg

Dieses Tutorial führt Sie schrittweise durch den InteProxy Server Installationsprozess.

Die grünen Pfeile verweisen auf Kapitel, zu denen Sie detailierter Informationen erhalten.

Bemerkung: Es ist erforderlich, dass Sie die nachfolgenden Schritte als *root*-Benutzer bzw. als Administrator ausführen.

3.1 Schritt 1: Installation Apache HTTP Server

Für den Einsatz des InteProxy Servers benötigen Sie einen **aktuellen** Apache HTTP Server (**mindestens Version 2.2.15**).

Weitere Informationen zur Installation finden Sie im Kapitel *Installation Apache HTTP Server*.

3.2 Schritt 2: Installation InteProxy Server

Laden Sie den aktuellen InteProxy Server herunter und entpacken Sie das Installationspaket.

Weitere Informationen zu der Installation erhalten Sie im Kapitel *Installation InteProxy Server*.

3.3 Schritt 3: Konfiguration InteProxy Server

Der InterProxy Server wird als separater VirtualHost betrieben. Hierzu konfigurieren Sie den InteProxy Server im Kontext der Apache HTTP Server Konfiguration.

Informationen zur Konfiguration unter Linux finden Sie im Kapitel *Konfiguration des Inteproxy Servers unter Linux*. Informationen zur Konfiguration unter Windows finden Sie im Kapitel *Konfiguration des Inteproxy Servers unter Windows*.

3.4 Schritt 4: InteProxy Server starten

3.4.1 Linux

Bemerkung: Unter Debian muss vor einem Neuladen der Apache Konfiguration der InteProxy Server VirtualHost aktiviert werden.

```
a2ensite inteproxy.conf
```

Laden Sie die Konfigurationen des Apache HTTP Server neu, damit Sie den InteProxy Server verwenden können.

```
/etc/init.d/apache2 reload
```

3.4.2 Windows

Unter Windows müssen Sie den Apache HTTP Server über das Programm `Apache Service Monitor` neustarten, damit Sie den InteProxy Server verwenden können.

3.5 Schritt 5: InteProxy Server testen

Mit diesem Test wird geprüft, ob der InteProxy Server grundsätzlich bei Ihnen funktioniert und auch nicht durch Firewalls blockiert wird. Stellen Sie sicher, dass InteProxy Server gestartet ist. Um zu testen, ob der InteProxy Server korrekt funktioniert, rufen Sie die folgenden URL (bsp. in einem Browser) auf:

```
http://<servername>:64609/inteproxy-demo.intevation.org/cgi-bin/frida-
wms?Request=GetCapabilities&Service=WMS&Version=1.1.0
```

Erhalten Sie ein Capabilities Dokument des abgesicherten Beispiel WMS Dienstes, haben Sie den InterProxy Server erfolgreich installiert. Herzlichen Glückwunsch! Sie können nun weitere abgesicherte OGC Web Services hinzufügen.


Weitere Erläuterungen zum Testen des InteProxy Servers finden Sie im Kapitel *Testen von InteProxy Server*

3.6 Schritt 6: Einrichtung weiterer abgesicherter OGC Web Services


Wie Sie weitere abgesicherte OGC Web Services hinzufügen können, erfahren Sie im Kapitel *Einrichtung weiterer abgesicherter OGC Web Services*.

Installation Apache HTTP Server

Für den Einsatz des InteProxy Servers wird **mindestens** die Version 2.2.15 des Apache HTTP Servers vorausgesetzt. Für die einzelnen Distributionen wie Debian, SuSE oder Windows Server erhalten Sie in den nachfolgenden Abschnitten detailierter Hinweise zur Installation des Apache HTTP Servers.

4.1 Debian

Für den Einsatz des InteProxy Servers unter Debian wird die Version 6.0 (Debian Squeeze) empfohlen.

Zum Installieren des Apache HTTP Server über die Kommandozeile, führen Sie den folgenden Befehl aus:

```
apt-get install apache2
```

Bemerkung: Für den Einsatz unter Debian Lenny (Version 5.0) ist der Apache HTTP Server aus dem Debian Lenny Backports Repository zu installieren.

4.2 SuSE

4.2.1 SUSE Linux Enterprise Server 11

Für den Einsatz des InteProxy Servers unter SUSE Linux Enterprise Server 11 ist die Installation des aktuellen Apache Paketes aus dem `Up-to-date Apache packages (SLE_11)` Repository erforderlich.

Fügen Sie dazu das `Apache.repo`, mit Hilfe des Kommandozeilenwerkzeuges `zypper` der Paketverwaltung, wie folgt hinzu:

```
zypper ar http://download.opensuse.org/repositories/Apache/SLE_11/ "Apache.repo"
```

Die Pakete des `Apache.repo` sind mit einem Schlüssel signiert. Fügen Sie diesen Schlüssel - nach einer Verifizierung der Korrektheit des Schlüssels - mit folgendem Befehl hinzu:

```
curl -O http://download.opensuse.org/repositories/Apache/SLE_11/repodata/repomd.xml.key
rpm --import repomd.xml.key
```

Installieren Sie nun den Apache HTTP Server:

```
zypper install apache2
```

4.2.2 SUSE Linux Enterprise Server 10

Für den Einsatz des InteProxy Servers unter SUSE Linux Enterprise Server 10 ist die Installation des aktuellen Apache Paketes aus dem `Up-to-date Apache packages (SLE_10)` Repository erforderlich.

Fügen Sie das `Apache.repo`, mit Hilfe des Kommandozeilenwerkzeuges `zypper` der Paketverwaltung wie folgt hinzu:

```
zypper ar http://download.opensuse.org/repositories/Apache/SLE_10/ "Apache.repo"
```

Die Pakete des `Apache.repo` sind mit einem Schlüssel signiert. Fügen Sie diesen Schlüssel - nach einer Verifizierung der Korrektheit des Schlüssels - mit folgendem Befehl hinzu:

```
curl -O http://download.opensuse.org/repositories/Apache/SLE_10/repodata/repomd.xml.key
rpm --import repomd.xml.key
```

Installieren Sie nun den Apache HTTP Server:

```
zypper install apache2
```

4.2.3 OpenSUSE

Für den Einsatz des InteProxy Servers unter OpenSUSE ist mindestens die Version 11.3 erforderlich. Ältere OpenSUSE Versionen werden nicht unterstützt.

Installieren Sie den Apache HTTP Server mit Hilfe des Kommandozeilenwerkzeuges `zypper`:

```
zypper install apache2
```

4.3 Windows Server

Für den Einsatz des InteProxy Servers unter Windows Server wird ein aktueller Apache HTTP Server mit SSL Unterstützung benötigt. Diesen können Sie auf der Seite Downloading the Apache HTTP Server des Apache HTTP Server Projektes herunterladen.

Bemerkung: Es wird das MSI-Paket `Win32 Binary including OpenSSL` benötigt.

Installieren Sie den Apache HTTP Server mit Hilfe des Windows Installers. Weitere Informationen zur Installation des Apache HTTP Server finden Sie in der Apache Dokumentation Using Apache with Microsoft Windows.

KAPITEL 5

Installation InteProxy Server

Die aktuellste Version des InteProxy Servers finden Sie unter: http://inteproxy.wald.intevation.org.

Der InteProxy Server ist Freie Software und unter der GNU GPL (Version 2) lizensiert.

5.1 Installation unter Linux

Laden Sie den aktuellen InteProxy Server herunter und entpacken Sie den InteProxy Server in das Verzeichnis `/opt`.

```
tar zxf InteProxy-SERVER-1.0.4.tar.gz -C /opt
```

5.2 Installation unter Windows

Laden Sie den aktuellen InteProxy Server herunter und entpacken Sie den InteProxy Server in das Verzeichnis `C:\Program Files\Apache Software Foundation\Apache2.2\conf`.

Konfiguration InteProxy Server

6.1 Konfiguration des InteProxy Servers unter Linux

6.1.1 Einrichten des VirtualHosts

Der InterProxy Server wird als separater VirtualHost betrieben, erstellen Sie hierfür eine symbolische Verknüpfung auf die InteProxy Server VHost-Konfigurationsdatei `/opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf` in dem entsprechenden Apache Verzeichnis.

Bemerkung: Das Setzen der symbolischen Verknüpfung ist abhängig von der eingesetzten Distribution.

- **Debian**: `ln -s /opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf /etc/apache2/sites-available/inteproxy.conf`
- **SuSE**: `ln -s /opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf /etc/apache2/vhosts.d/inteproxy.conf`

Eine detailierte Erläuterung der VirtualHost Konfigurationsdatei finden Sie im Kapitel *VirtualHost Konfigurationsdatei*.

6.1.2 Konfigurieren der InteProxy Server Portnummer

Der InteProxy Server nimmt Anfragen auf der Portnummer `64609` entgegen. Ergänzen Sie die InteProxy Server Portnummer, im Kontext der Apache HTTP Server-Konfiguration, in dem Sie die folgende Zeile hinzufügen:

```
Listen 64609
```

Bemerkung: Die Konfigurationsdatei für das Setzen der Portnummer ist abhängig von der eingesetzten Distribution.

- **Debian**: `/etc/apache2/ports.conf`
- **SuSE**: `/etc/apache2/listen.conf`

6.1.3 Einbinden der benötigten Apache Module

Für den Betrieb des InteProxy Servers werden bestimmte Apache Module benötigt. Um diese Module zu laden, entfernen Sie in der InteProxy Server VHost-Konfigurationsdatei `/opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf` den Kommentar vor der `Include`-Zeile, die Ihrer Distribution entspricht. Nachfolgend sehen Sie ein Beispiel für das Einbinden der benötigten Apache Module unter Debian.

```
## Apache Module for SuSE
#Include /opt/InteProxy-SERVER-1.0.4/server/conf/platform-suse.conf

# Apache Module for Debian
Include /opt/InteProxy-SERVER-1.0.4/server/conf/platform-debian.conf
```

Welche konkreten Apache Module benötigt werden, erfahren Sie im Kapitel *Anforderungen*.

6.1.4 Proxy-Umgebung einrichten

Befindet sich der InteProxy Server im Intranet hinter einem Proxy zum Internet, muss dieser eingerichtet werden, damit Anfragen in das Internet weitergeleitet werden können. Das geschieht in der Datei `/opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf`.

```
ProxyRemote * http://intranet.proxy:8080
```

Ersetzen Sie dazu die obige Beispiel URL *http://intranet.proxy:8080* durch die URL Ihres Proxies.

Bemerkung: Müssen Anfragen nicht über einen Proxy nach außen geleitet werden, kommentieren Sie die Zeile mit der Direktive `ProxyRemote` durch das Einfügen einer Raute (#) aus.

Weitere Informationen zur Proxy-Konfiguration erhalten Sie im Kapitel *Nutzung eines Intranet-Proxies*.

6.1.5 Testen der Konfiguration

Testen Sie die Konfiguration auf syntaktische Korrektheit, bevor Sie die Konfigurationsdateien neu laden, mit dem Befehl:

```
apache2ctl -S
```

6.2 Konfiguration des InteProxy Servers unter Windows Server

6.2.1 Einrichten des VirtualHosts

Um den InterProxy Server als seperaten VirtualHost zu betreiben, ergänzen Sie am Ende der Datei `C:\Program Files\Apache Software Foundation\Apache2.2\conf` die folgende Zeile:

```
Include conf/InteProxy-SERVER-1.0.4/server/conf/inteproxy-WindowsServer2003.conf
```

Eine detailierte Erläuterung der VirtualHost Konfigurationsdatei finden Sie im Kapitel *VirtualHost Konfigurationsdatei*.

6.2.2 Konfigurieren der InteProxy Server Portnummer

Der InteProxy Server nimmt Anfragen auf der Portnummer `64609` entgegen. Ergänzen Sie die InteProxy Server Portnummer, im Kontext der Apache HTTP Server-Konfiguration, in dem Sie die folgende Zeile in der Datei `C:\Programme\Apache Group\Apache2\conf\httpd.conf` hinzufügen:

```
Listen 64609
```

6.2.3 Einbinden der benötigten Apache Module

Für den Betrieb von InteProxy Server unter Windows sind die benötigten Module bereits vorkonfiguriert. Diese stehen in der Datei *conf/InteProxy-SERVER-1.0.4/server/conf/platform-WindowsServer2003.conf*.

```
# Apache Module für Windows Server
Include "conf/InteProxy-SERVER-1.0.4/server/conf/platform-WindowsServer2003.conf"
```

Welche konkreten Apache Module benötigt werden, erfahren Sie im Kapitel *Anforderungen*.

6.2.4 Proxy-Umgebung einrichten

Befindet sich der InteProxy Server im Intranet hinter einem Proxy zum Internet, muss dieser eingerichtet werden, damit Anfragen in das Internet weitergeleitet werden können. Das geschieht in der Datei `inteproxy-WindowsServer2003.cong`:

```
ProxyRemote * http://intranet.proxy:8080
```

Ersetzen Sie dazu die obige Beispiel URL *http://intranet.proxy:8080* durch die URL Ihres Proxies.

Bemerkung: Müssen Anfragen nicht über einen Proxy nach außen geleitet werden, kommentieren Sie die Zeile mit der Direktive `ProxyRemote` durch das Einfügen einer Raute (#) aus.

Weitere Informationen zur Proxy-Konfiguration erhalten Sie im Kapitel *Nutzung eines Intranet-Proxies*.

6.2.5 Testen der Konfiguration

Testen Sie die Konfiguration auf syntaktische Korrektheit, bevor Sie die Konfigurationsdateien neu laden. Verwenden Sie hierzu das Programm `Test Configuration` aus `Programme -> Apache HTTP Server 2.x.x -> Configure Apache Server`.

VirtualHost Konfigurationsdatei

Der InterProxy Server wird als separater VirtualHost betrieben, die Konfiguration des VirtualHost erfolgt in der Datei `/opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy.conf`.

Die Inhalte der Datei `inteproxy.conf` werden in dem folgenden Block erläutert; sie bezieht sich auf GNU/Linux-Systeme. Windows-Benutzer nehmen entsprechend die Datei `inteproxy-WindowsServer2003.conf`

```
<VirtualHost *:64609>
ServerAdmin name@domain.de

DocumentRoot /opt/InteProxy-SERVER-1.0.4/server

TransferLog /opt/InteProxy-SERVER-1.0.4/server/logs/access_log
```

 # ZWINGEND ERFORDERLICH! Benötigte Module laden!
 # Zum Laden der benötigten Apache Module entfernen Sie den Kommentar
 # vor der Include-Zeile welche Ihrer Distribution entspricht.

```
## Apache Module für SuSE
#Include /opt/InteProxy-SERVER-1.0.4/server/conf/platform-suse.conf

## Apache Module für Debian
#Include /opt/InteProxy-SERVER-1.0.4/server/conf/platform-debian.conf

## Apache Module für Windows Server
#Include "conf/InteProxy-SERVER-1.0.4/server/conf/platform-WindowsServer2003.conf"

# Intranet Proxy
ProxyRemote * http://intranet.proxy:8080

RewriteEngine On
# RewriteLogLevel 0
RewriteLog /opt/InteProxy-SERVER-1.0.4/server/logs/rewrite.log

# Die Direktive filter chain definiert eine Filter-Kette zum Umschreiben der
# URLs in einem WMS Capabilities Dokument.  WMS Capabilities Dokumente haben
# den Content-Type type application/vnd.ogc.wms_xml.  Der Schrägstrich in dem
# Content-Type  Feld muss als oktales Maskierungszeichen \057 geschrieben, da
# der Schrägstrich als Trenner im Regulären Ausdruck verwendet wird.
# Achtung: Die Zeilen fixurls und gzdeflate dürfen keine Zeilenümbrüche
# aufweisen, diese dienen nur zur besseren Lesbarkeit.
```

```
FilterProvider gzinflate INFLATE resp=Content-Encoding $gzip
FilterProvider fixurls SUBSTITUTE
                       Content-Type "/(application\057vnd.ogc.wms_xml|text\057xml)($|;)/"
FilterProvider gzdeflate DEFLATE
                       Content-Type "/(application\057vnd.ogc.wms_xml|text\057xml)($|;)/"
FilterChain +gzinflate +fixurls +gzdeflate

# Die Datei conf/inteproxy-rewrite.conf beinhaltet die RewriteRules für die
# aktuelle InteProxy Funktionalität. Sollte die Datei nicht existieren, lesen
# Sie im Kapitel 10 wie Sie diese erstellen können.

Include /opt/InteProxy-SERVER-1.0.4/server/conf/inteproxy-rewrite.conf

# Die Direktive Deny bestimmt, welche Hosts, beziehungsweise Netzwerke, vom
# Zugriff auf eine Server-Ressource ausgeschlossen sind; die gegensätzliche
# Direktive Allow ermöglicht es, bestimmten Hosts den Zugriff ausdrücklich zu
# gestatten.
# Grundsätzlich darf kein Host auf die Inhalte des InteProxy Servers
# Kontextes zugreifen, in dem die Direktive definiert ist. Niemand darf auf
# URLs zugreifen, die mit / beginnen.

<Directory />
 Order Deny,Allow
 Deny from All
</Directory>

# SSL Konfiguration.
# SSLProxyEngine muss eingeschaltet sein, damit https-Verbindungen zu anderen
# Rechner möglich sind.

SSLProxyEngine on
SSLProtocol all -SSLv2
SSLCipherSuite HIGH:MEDIUM:!ADH

</VirtualHost>
```

Nutzung eines Intranet-Proxies

Müssen Anfragen über einen Proxy Server, welcher sich im Intranet befindet, nach außen durch eine Firewall geleitet werden, *muss* hierzu die Direktive ProxyRemote verwendet werden. Die Direktive *ProxyRemote* benötigt das Apache-Module mod_proxy.

Die Direktive *ProxyRemote* leitet Proxy-Anfragen, die der lokale Proxy empfangen hat, an einen anderen Proxy-Server weiter.

```
|---------|     |------------|      |-----------------|     |---------------|
| Klient  |     | InteProxy  |      | intranet.proxy  |     | abgesicherter |
|         | -> |  Server    | ->   |     :8080       | -> |     Dienst    |
|---------|     |------------|      |-----------------|     |---------------|
```

Im nachfolgenden Beispiel werden alle Proxy-Anfragen an `intranet.proxy:8080` weitergeleitet:

```
ProxyRemote * http://intranet.proxy:8080
```

- Der erste Parameter ist das URL-Muster der Proxy-Anfragen: Beginn einer URL oder ein * für beliebige URLs.
- Der zweite Parameter ist die vollständige URL des Remote-Servers.

Die Direktive *ProxyRemote* steht in der Datei `inteproxy.conf` eingetragen. Passen Sie in dieser Datei die URL für Ihren Proxy entsprechend an.

Bemerkung: Wird kein Proxy benötigt, müssen Sie die *ProxyRemote* Direktive mit einer Raute (#) auskommentieren.

Nach erfolgter Anpassung müssen Sie die Apache HTTP Server Konfigurationen neu neu laden!

Bemerkung: Für die `HTTPS_upstream-proxy` Unterstützung benötigen Sie einen Apache HTTP Server ab Version 2.2.15 (vgl. Kapitel *Anforderungen*)! Eine Proxy Authentifizierung wird zur Zeit noch nicht unterstützt.

Testen von InteProxy Server

Der InteProxy Server bietet die Möglichkeit als normaler HTTP-Web-Proxy zu arbeiten. Im Folgenden wird die Betriebsart als HTTP-Web-Proxy an Beispielen inklusive Konfigurationsschritten vorgestellt.

9.1 Nutzerdaten

Um die Anwendungsbeispiele gegen den hier beschriebenen Demoserver zu nutzen, stehen Ihnen die folgenden Nutzerdaten im OWSProxy zur Verfügung. Server-URL:

```
http://inteproxy-demo.intevation.org/cgi-bin/frida-wms
```

Zwei Benutzerkonten stehen bereit:

- User/Passwort = `meier`/`meier`: Darf alle WMS Ebenen anschauen
- User/Passwort = `schmidt`/`schmidt`: Darf alle WMS Ebenen anschauen, außer den Straßen.

Die Nuterdaten für das Benutzerkonto `meier` sind bereits in der Datei `inteproxy.cfg` eingetragen.

9.2 Nutzung von InteProxy Server

Stellen Sie in Ihrer Anwendung der eigentlichen URL Text `http://servername:64609/` voran. Dadurch wird der angefragte WMS-Dienst explizit durch InteProxy Server angesprochen und abgesichert.

9.3 Einfacher Funktionstest (über Web-Browser)

Mit diesem Test wird geprüft, ob der InteProxy Server grundsätzlich bei Ihnen funktioniert und auch nicht durch Firewalls blockiert wird. Stellen Sie sicher, dass InteProxy Server gestartet ist. Um zu testen, ob der InteProxy Server korrekt funktioniert, öffnen Sie einen Web-Browser und geben Sie folgende URL ein:

```
http://servername:64609/inteproxy-demo.intevation.org/cgi-bin/frida-wms?
Request=GetMap
&Version=1.1.1&service=WMS
&layers=strassenall,sehenswuerdigkeiten
&format=image/png&width=200&height=200
&srs=epsg:31467&bbox=3427000,5787590,3444000,5800880
```

Der Browser stellt die Anfrage zunächst an InteProxy Server, welcher auf Port 64609 auf dem Server auf Anfragen wartet. Nach Eingabe sollte im Browser dann eine Karte der Stadt Osnabrück erscheinen, denn der InteProxy Server führt die eigentliche nachfolgende WMS-Anfrage an den abgesicherten Dienst aus:

```
https://inteproxy-demo.intevation.org/cgi-bin/frida-wms?VERSION=1.1.1
&SERVICE=WMS&REQUEST=GetMap&layers=strassenall,sehenswuerdigkeiten
&format=image/png&width=200&height=200
&srs=epsg:31467&bbox=3427000,5787590,3444000,5800880
&user=meier&password=meier
```

Insbesondere wird natürlich nun über das sichere Protokoll „https“ und nicht mehr über„http“ kommuniziert. Darüber hinaus hängt der InteProxy Server die ihm bekannten Credentials `user=meier&passwort=meier` an die sichere URL an.

KAPITEL 10

Einrichtung weiterer abgesicherter OGC Web Services

Die Einrichtung weiterer abgesicherter OGC Web Services kann auf zwei unterschiedlichen Wege durchgeführt werden. **Entweder** automatisiert durch das Python-Skript `create-rewrite-rules.py` und die Verwendung der InteProxy Server Konfigurationsdatei `inteproxy.cfg` **oder** durch die manuelle Erstellung der Datei `inteproxy-rewrite.conf`.

10.1 Automatische Einrichtung

Die automatisierte Einrichtung weiterer abgesicherter OGC Web Services erfolgt über die Konfigurationsdatei `inteproxy.cfg`. Werden darin keine OWS-Dienste angegeben, verhält sich der InteProxy Server wie ein normaler transparenter HTTP-Proxy.

Dem InteProxy Server Installationspaket liegt eine beispielhafte Konfigurationsdatei `inteproxy.cfg` bei. In die Konfigurationsdatei können weitere abgesicherte OGC Web Services eingetragen werden.

Für den Betrieb des InteProxy Servers und der Einrichtung weiterer abgesicherter OGC Web Services muss ausschließlich der Haupt-Abschnitt der Absicherungsregeln `[inteproxy-rules]` angepasst werden.

In dem folgendem Block ist eine beispielhafte Konfigurationsdatei `inteproxy.cfg` beschrieben, in welcher im Haupt-Abschnitt der Absicherungsregeln `[inteproxy-rules]` beispielhaft der abgesicherte OGC Web Service `inteproxy-demo.intevation.org` als OWSProxy eingetragen ist.

```
# Demo configuration inteproxy.cfg for InteProxy Desktop.
#
# Diese Datei definiert, wie unterschiedliche entfernte Rechner
# angesprochen werden sollen.
# Alle Server werden über URLs im inteproxy-rules-Abschnitt
# definiert.
#
# Um abwärtskompatibel zu bleiben, wird das alte Format, wo
# jeder Server durch einen eigenen Abschnitt referenziert wurde,
# weiterhin unterstützt.
# Die Benennung der Abschnitte spielt keine Rolle, sie müssen
# nur eindeutig sein.
# Um diese Eindeutigkeit zu bewahren, bietet es sich an,
# den kompletten Domain-Namen auch als Abschnitts-Namen zu
# verwenden.
# In Zukunft können noch weitere InteProxy-Einstellungen in
# dieser Konfigurationsdatei abgelegt werden.
#
# InteProxy-spezifische Konfigurationseinträge folgen:
```

```
# !! WICHTIG:
# !! Sofern ein Intranet-Proxy mit Benutzer/Passwort-
# !! Authentifizierung verwendet wird, kommentieren Sie bitte
# !! die Abschnitte [inteproxy] und
# !! [http_proxy_authentification] aus und passen Sie Ihre
# !! Zugangsdaten entsprechend an.
#
# Anmeldung gegen einen Intranet-Proxy
# [inteproxy]
# https_proxy=http_proxy_authentification
# http_proxy=http_proxy_authentification
#
# [http_proxy_authentification]
# host=upstream.proxy.url.com
# port=8080
# username=john
# password=secret
#
# Haupt-Abschnitt der Absicherungsregeln.
# Der urls-Abschnitt ist eine Liste von URLs. Jede URL muss in
# einer Zeile stehen. Ab der zweiten Zeile müssen die URLs
# eingerückt werden.
#
# Jede URL folgt diesem Schema:
#    SCHEMA://[BENUTZER:PASSWORT@]RECHNERNAME[:PORT]/PFAD
#
# Die Zugangsdaten (BENUTZER und PASSWORT) sowie der Port (PORT)
# sind optional. Wenn kein Port angegeben wird, wird der
# Standardport angenommen.
#
# Das SCHEMA muss eines der folgenden unterstützten Schemen
# sein:
#
#   owsproxy   Der gegenüberliegende Rechner ist ein OWSProxy,
#              der Authentifizierung und https benötigt.
#
#   basicauth  HTTP Basic Authorization über https
#
# Wenn BENUTZER oder PASSWORT spezielle Zeichen wie '%', ':',
# '@' und Nicht-ASCII Zeichen enthalten, müssen diese mit
# einem "%" gefolgt von 2 hexadezimalen Zeichen maskiert
# werden. Weitere Komplikationen können durch das Prozentzeichen
# entstehen, da es in URLs als Spezialzeichen gilt. Aber auch
# in dieser Konfigurationsdatei muss ein %-Zeichen durch ein
# weiteres Prozentzeichen verdoppelt werden. Ein Prozentzeichen
# müsste wie folgt maskiert werden: „%%25" anstatt „%".
#
# RECHNERNAME und PFAD-Teile der URL können „*"-Zeichen als
# Wildcards eingesetzt werden. Diese Wildcards werden auf 0
# und mehr Zeichen angewandt.
#
# Eine Wildcard im RECHNERNAMEN wird nur auf Diesen angewandt,
# gleiches gilt für den PFAD.
#
[inteproxy-rules]
urls=owsproxy://meier:meier@inteproxy-demo.intevation.org/cgi-bin/frida-wms
     owsproxy://USERNAME:PASSWORT@www.geobasisdaten.niedersachsen.de/mapgate/*
```

10.1.1 Ausführen von create-rewrite-rules.py

Bemerkung: Zur Ausführung des `create-rewrite-rules.py` Skriptes wird eine Python Umgebung und das *lxml XML toolkit* für Python benötigt.

Die Konfigurationsdatei `inteproxy.cfg` muss mit Hilfe des Python-Skriptes `create-rewrite-rules.py` in Apache RewriteRule Direktiven umgewandelt. Ergebnis der Umwandlung ist die Datei `inteproxy-rewrite.conf`.

 Informationen zu der Datei `inteproxy-rewrite.conf` finden Sie im Abschnitt *Manuelle Einrichtung*.

Der folgende Beispielaufruf zeigt die Erstellung der Datei `inteproxy-rewrite.conf`:

```
./create-rewrite-rules.py --config-file=inteproxy.cfg \
--server-prefix=http://<servername>:64609 \
--output-file=server/conf/inteproxy-rewrite.conf
```

Bemerkung: Nach Erstellung der Datei `inteproxy-rewrite.conf` muss der Apache HTTP Server die Konfigurationsdateien neu laden.

```
/etc/init.d/apache2 reload
```

Wird beim Ausführen des Python-Skriptes `create-rewrite-rules.py` keine Konfigurationsdatei angegeben, wird nach der Datei `inteproxy.cfg` im InteProxy Server-Hauptverzeichnis gesucht.

Hilfe zur Ausführung erhalten Sie durch den folgenden Aufruf auf der Kommandozeile:

```
./create-rewrite-rules.py -h
```

10.2 Manuelle Einrichtung

Warnung: Die manuelle Einrichtung der Datei `inteproxy-rewrite.conf` ist nicht trivial.

Im folgenden Block wird beispielhaft die Datei `inteproxy-rewrite.conf` erläutert und Hinweise zur Benutzung der verwendeten Apache Direktiven gegeben.

```
RewriteRule ^/inteproxy\-demo\.intevation\.org\/cgi\-bin\/frida\-wms$
            https:/$0?user=meier&password=meier [QSA,P]
RewriteRule ^/www\.geobasisdaten\.niedersachsen\.de\/mapgate\/.*$
            https:/$0?user=USERNAME&password=PASSWORT [QSA,P]
Substitute s!https?://(inteproxy\055demo\.intevation\.org\/cgi\055bin\/frida\055wms
           |www\.geobasisdaten\.niedersachsen\.de\/mapgate\/)
           !http://SERVERNAME:64609/$1!
```

Warnung: Die Datei `inteproxy-rewrite.conf` darf in den Zeilen RewriteRule und Substitute **keine** Zeilenbrüche aufweisen. Die Zeilenbrüche dienen nur zur besseren Lesbarkeit.

10.2.1 Direktive Rewrite Rule

Die Direktive RewriteRule definiert die eigentliche Umleitung. Die Direktive kann mehrmals vorkommen, dabei ergibt jedes Vorkommnis eine eigene Umleitung. Die Reihenfolge der Umleitungen ist wichtig, da diese in der Reihenfolge des Vorkommens angewendet werden.

Die Direktive RewriteRule erwartet als Parameter:

1. **Ausdruck** - beschreibt die URLs, die umgeleitet werden sollen

2. **Umleitung** - gibt die Umleitung an

Ausdruck beschreibt die URLs, die umgeleitet werden. Es ist ein Perl-kompatibler Regulärer Ausdruck (ohne Begrenzerzeichen, '/'). Vor dem Ausdruck kann zusätzlich ein Ausrufezeichen ('!') stehen, um den Regulären Ausdruck zu negieren.

Umleitung ist die URL, auf die umgeleitet wird, wenn der Ausdruck zutrifft.

Am Ende der RewriteRule können Sie noch optional einige weitere Optionen angeben, welche das Verhalten von mod_rewrite steuern, falls die RewriteRule zutrifft. Diese werden in spitzen Klammern ([bzw.]) notiert. Wenn Sie mehrere angeben, trennen Sie diese durch Kommata. Folgende Optionen werden in der InteProxy-RewriteRule-Datei verwendet:

- **QSA** Diese Option müssen Sie angeben, wenn Sie an die Umleitung manuell einen neuen Query-String hängen und den alten dabei nicht komplett ersetzen wollen.
- **P** Diese Option sorgt dafür, dass ein Zugriff von dem Apache-Modul mod_proxy aus auf die URL erfolgt. Dazu muss mod_proxy aktiviert und die URL muss valide sein (sie muss unter anderem auf jeden Fall mit http://hostname beginnen).

Weitere Informationen finden Sie in der Apache Dokumentation URL Rewriting Guide und in der Dokumentation SELFHTML Umleitungen mit mod_rewrite.

10.2.2 Direktive Subsitute

Die Substitute Direktive definiert ein Such- und ein Ersetzungs-Pattern, welche auf den Response-Body angewendet wird. Die Syntax ist dabei wie folgt:

```
Substitute s!Suchtext!Ersetzungstext!
```

Dabei können sowohl reguläre Ausdrücke als auch einfache Text-Ersetzungen verwendet werden. Der Inteproxy-Server verwendet reguläre Ausdrücke in der Substitute Direktive.

Bemerkung: Nach jeder Änderung an der Datei `inteproxy-rewrite.conf` müssen Sie die Apache HTTP Server Konfigurationen neu laden.

Linkliste

- http://archive.apache.org/dist/httpd/binaries/win32/ (Apache HTTP Server Archive für historische win32 Versionen)
- http://codespeak.net/lxml/
- http://httpd.apache.org (Apache HTTP Server)
- http://httpd.apache.org/docs/2.2/mod/core.html (Apache Core Features)
- http://httpd.apache.org/docs/2.2/mod/mod_auth_basic.html (Apache Module mod_auth_basic)
- http://httpd.apache.org/docs/2.2/mod/mod_authz_host.html (Apache Module mod_authz_host)
- http://httpd.apache.org/docs/2.2/mod/mod_filter.html (Apache Module mod_filter)
- http://httpd.apache.org/docs/2.2/mod/mod_proxy.html (Apache Module mod_proxy)
- http://httpd.apache.org/docs/2.2/mod/mod_proxy_http.html (Apache Module mod_proxy_http)
- http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html (Apache Module mod_rewrite)
- http://httpd.apache.org/docs/2.2/mod/mod_ssl.html (Apache Module mod_ssl)
- http://httpd.apache.org/docs/2.2/mod/mod_substitute.html (Apache Module mod_substitute)
- http://inteproxy.wald.intevation.org (InteProxy - Security extension for unsecure OWS clients to secure spatial data infrastructures)
- http://www.debian.org/ (Debian GNU/Linux)
- http://www.gnu.org/licenses/old-licenses/gpl-2.0.html (GNU General Public License, version 2)
- http://www.python.org/ (Python Programming Language)
- https://wiki.deegree.org/deegreeWiki/iGeoSecurity (iGeoSecurity - short description of iGeoSecurity)

Anforderungen

12.1 Benötigte Apache HTTP Server Module

Der InteProxy Server benötigt einen aktuellen Apache HTTP Server und die folgenden Apache-Module:

- mod_rewrite
- mod_authz_host (Modul erst ab Apache Version 2.1 verfügbar)
- mod_proxy
- mod_proxy_http
- mod_ssl
- mod_proxy (Modul erst ab Apache Version 2.2.15 verfügbar)
- mod_substitute (Modul erst ab Apache Version 2.2.7 verfügbar)
- mod_filter (Modul erst ab Apache Version 2.1 verfügbar)

Bemerkung: In den Versionen größer oder gleich der Version 2.2.15 sind alle benötigten Apache HTTP Server Module bereits vorhanden.

12.2 weitere Anforderungen

- Python
- lxml XML toolkit

Für die Ausführung des `create-rewrite-rules.py` Skripts werden zusätzlich eine Python-Umgebung und das Python-Paket lxml benötigt.

KAPITEL 13

Versionsgeschichte

Aktuell ist Version 1.0.4 vom 16. Juni 2011.

13.1 Neu seit Version 1.0.4 vom 16. Juni 2011

- Erweiterung: Überarbeitung der Dokumentation zu InteProxy Server.
- Erweiterung: URL-Rewriting bei Content-Encoding: gzip,deflate implementiert.
- Verbesserung: [inteproxy-Bugs][1613] Erstellung funktionaler Substitute Direktiven mit create-rewrite-rules.py für "einzeilige" Capabilities Dokumenten.
- Anpassung: Konfigurationsdatei inteproxy-rewrite.conf für das Umschreiben von GetCapabilities Antworten.

13.2 Neu seit Version 1.0.3 vom 3. November 2010

- Anpassung: Konfigurationsdatei inteproxy-rewrite.conf für das Umschreiben von GetCapabilities Antworten.
- Anpassung: Konfigurationsdateien und Dokumentation für den Einsatz des InteproxyServers unter openSUSE 11.3
- Erweiterung: Überarbeitung der Dokumentation zu InteProxy Server.

13.3 Neu seit Version 1.0.2 vom 11. September 2010

- Erweiterung: URL Rewriting in WMS Capabilities Antworten

13.4 Neu seit Version 1.0.1 vom 11. Mai 2010

- Erweiterung: Dokumentation der InteProxy-Server-Variante unter Windows 2003 (SP2)

13.5 Neu seit Version 1.0.0 vom 10.12.2009

- Erweiterung: Die Konfigurationsdatei enthält optionale Proxy-Einstellungen. Die Umgebungsvariablen werden weiterhin genutzt.
- Erweiterung: Upstream-Proxy-Authentifikation
- Erweiterung: Paketierung für OpenSuse 10.x
- Erweiterung: Erstellung und Dokumentation einer InteProxy-Server-Variante
- Erweiterung: Konfigurationsskript für InteProxy-Server
- Verbesserung: Logging zur Fehlerbeseitigung
- Verbesserung: Ergänzungen der Unit-Tests