



InteProxy Server Dokumentation

Release 1.0.3

Bjoern Schilberg

03. 11. 2010

Inhaltsverzeichnis

| | | |
|-----------|--|-----------|
| 1 | Eine kurze Einführung | 1 |
| 1.1 | Unterstützte OWS-Absicherungs-Methoden | 1 |
| 2 | Download | 3 |
| 3 | Anforderungen | 5 |
| 4 | Installation von InteProxy Server für Debian Lenny | 7 |
| 4.1 | Installieren des Apache HTTP Server 2 | 7 |
| 4.2 | Herunterladen des InteProxy Servers | 7 |
| 4.3 | Anpassen und Umwandeln der InteProxy Konfigurationsdatei | 7 |
| 4.4 | Einrichten des InteProxy Servers als separaten VirtualHost | 8 |
| 5 | Installation des InteProxy Server für openSuSE 11.3 | 9 |
| 5.1 | Installieren des Apache HTTP Server 2 | 9 |
| 5.2 | Herunterladen des InteProxy Servers | 9 |
| 5.3 | Anpassen und Umwandeln der Rewrite-Rules Konfigurationsdatei | 9 |
| 5.4 | Einrichten des InteProxy Servers als separaten VirtualHost | 10 |
| 5.5 | Hinweise | 10 |
| 6 | Installation des InteProxy Server für Windows Server 2003 (SP2) | 11 |
| 6.1 | Installieren des Apache HTTP Server 2 | 11 |
| 6.2 | Herunterladen des InteProxy Servers | 11 |
| 6.3 | RewriteRule-Konfigurationsdatei | 11 |
| 6.4 | Einrichten des InteProxy Servers als separaten VirtualHost | 12 |
| 7 | VirtualHost Konfigurationsdatei | 13 |
| 8 | Konfigurationsdatei inteproxy.cfg | 15 |
| 9 | ProxyRemote | 17 |
| 10 | URL Rewriting in WMS Capabilites | 19 |
| 10.1 | Vorraussetzungen | 19 |
| 10.2 | Konfiguration | 19 |
| 10.3 | Test | 20 |
| 11 | Erster Test | 21 |
| 11.1 | Nutzerdaten | 21 |

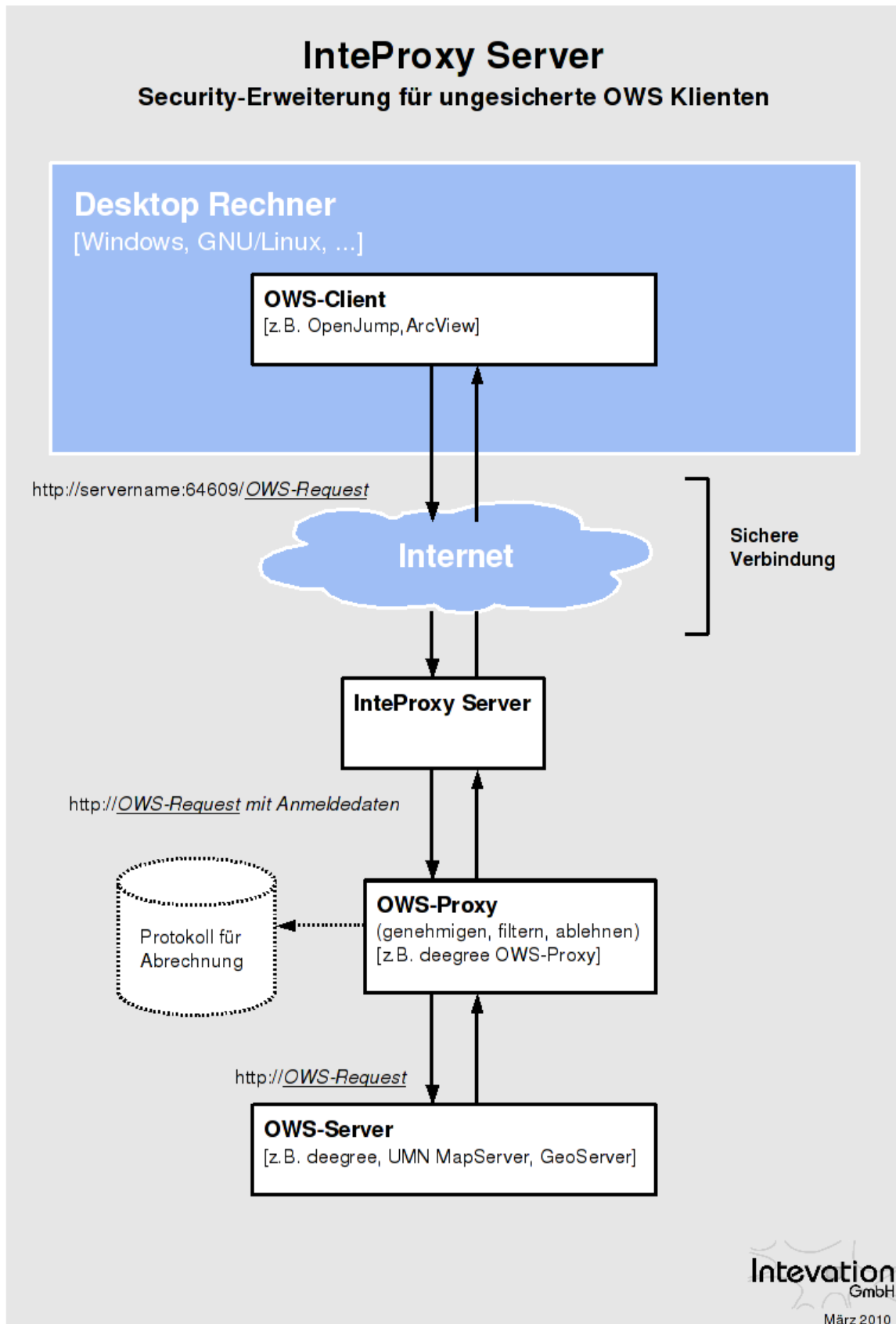
| | | |
|-----------|--|-----------|
| 11.2 | Nutzung von InteProxy Server | 21 |
| 11.3 | Einfacher Funktionstest (über Web-Browser) | 21 |
| 12 | Linkliste | 23 |

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.



Download

Die aktuellsten Versionen des InteProxy Servers befinden sich unter: <http://inteproxy.wald.intevation.org>.

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

Anforderungen

Der InteProxy Server benötigt einen [Apache HTTP Server 2](#) 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](#)
- optional für ProxyRemote:
 - [mod_proxy](#) (Modul erst ab Apache Version 2.2.15 verfügbar)
- optional für URL Rewriting im WMS Capabilities:
 - [mod_substitute](#) (Modul erst ab Apache Version 2.2.7 verfügbar)
 - [mod_filter](#) (Modul erst ab Apache Version 2.1 verfügbar)

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

Installation von InteProxy Server für Debian Lenny

Die folgende Beschreibung der Installation des InteProxy Servers bezieht sich auf eine [Debian Lenny GNU/Linux-Distribution](#).

4.1 Installieren des Apache HTTP Server 2

Installieren Sie den Apache HTTP Server 2 mit Hilfe der Anweisung:

```
apt-get install apache2
```

Die benötigten Apache-Module werden hierbei bereits mit installiert.

4.2 Herunterladen des InteProxy Servers

Laden Sie das InteProxy Server Archive herunter (siehe [Download](#)) und entpacken Sie diese in das Verzeichnis `/opt`.

```
cd /opt
tar xzf InteProxy-SERVER-1.0.3.tar.gz
```

4.3 Anpassen und Umwandeln der InteProxy Konfigurationsdatei

Passen Sie sich die InteProxy Konfigurationdatei `inteproxy.cfg` Ihren Bedürfnissen an. Nach erfolgter Anpassung wandeln Sie die Konfigurationsdatei mit Hilfe des Skripts `create-rewrite-rules.py` aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.3` in [Apache RewriteRule Direktiven](#) um.

```
./create-rewrite-rules.py --config-file=inteproxy.cfg -o \
server/conf/inteproxy-rewrite.conf
```

Sie benötigen zur Ausführung des Skripts `create-rewrite-rules.py` noch das Python-Paket `lxml`, gegebenenfalls müssen Sie es nachinstallieren.

```
apt-get install python-lxml
```

4.4 Einrichten des InteProxy Servers als separaten VirtualHost

Um den InterProxy Server als separaten **VirtualHost** zu betreiben, kopieren Sie hierfür aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.3/server/conf` die Beispiel-Konfigurationsdatei `inteproxy.conf` nach `/etc/apache2/sites-available/`. Sie können die Beispiel-Konfigurationsdatei auch als Vorlage für Ihre eigene Konfiguration verwenden.

Der Standard-Port des Inteproxy Servers ist `64609`. Ergänzen Sie daher in der Datei `/etc/apache2/ports.conf` noch die folgende Zeile:

```
Listen 64609
```

Aktivieren Sie nun den neu hinzugefügten VirtualHost.

```
a2ensite inteproxy.conf
```

Nach erfolgreicher Aktivierung des VirtualHost `inteproxy` laden Sie den Apache HTTP Server neu.

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

Installation des InteProxy Server für openSuSE 11.3

Die folgende Beschreibung der Installation des InteProxy Servers bezieht sich auf eine [openSUSE 11.3-Distribution](#).

5.1 Installieren des Apache HTTP Server 2

Installieren Sie den Apache HTTP Server 2 mit Hilfe der des Kommandozeilenwerkzeugs `zypper` oder über das graphische Werkzeug `Yast`:

```
zypper install apache2
```

Die benötigten Apache-Module werden hierbei bereits mit installiert.

5.2 Herunterladen des InteProxy Servers

Laden Sie das InteProxy Server Archive herunter (siehe [Download](#)) und entpacken Sie diese in das Verzeichnis `/opt`.

```
cd /opt
tar xzf InteProxy-SERVER-1.0.3.tar.gz
```

5.3 Anpassen und Umwandeln der Rewrite-Rules Konfigurationsdatei

Passen Sie sich die InteProxy Rewrite-Rules Konfigurationdatei `inteproxy-rewrite.conf` aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.3/server/conf` manuell Ihren Bedürfnissen an.

Ändern Sie in der Datei `inteproxy-rewrite.conf` die Angaben zum Benutzernamen (`USERNAME`), Passwort (`PASSWORT`) und zum Servernamen (`SERVERNAME`).

Eine detaillierte Beschreibung der Apache Direktiven `RewriteRule` und `Substitute` finden Sie in der Apache Webserver Dokumentation in den jeweiligen Modulen unter:

- [Apache Module mod_rewrite: RewriteRule Directive](#)
- [Apache Module mod_substitute: Substitute Directive](#)

5.4 Einrichten des InteProxy Servers als separaten VirtualHost

Um den InterProxy Server als separaten **VirtualHost** zu betreiben, kopieren Sie hierfür aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.3/server/conf` die Beispiel-Konfigurationsdatei `inteproxy.conf` nach `/etc/apache2/vhosts.d`. Sie können die Beispiel-Konfigurationsdatei auch als Vorlage für Ihre eigene Konfiguration verwenden.

Der Standard-Port des Inteproxy Servers ist `64609`. Ergänzen Sie daher in der Datei `/etc/apache2/listen.conf` noch die folgende Zeile:

```
Listen 64609
```

Wenn Sie sich unsicher sind, wie Apache ihre vhost-Konfiguration interpretiert, nutzen Sie den Befehl:

```
httpd2 -S -DSSL
```

Nach erfolgreichem Test des neu eingerichteten VirtualHost `inteproxy` starten Sie den Apache HTTP Server neu.

```
rcapache2 restart
```

5.5 Hinweise

5.5.1 Warnmeldung beim Starten von apache zu bereits geladenen Modulen

Erscheint beim Starten des Apache Webservers ein Warnhinweis das Apache Module bereits geladen worden sind:

```
module proxy_module is already loaded, skipping
```

Kommentieren Sie ggf. die in der Warnmeldung vorkommenden Module in der Datei `/opt/InteProxy-SERVER-1.0.3/server/conf/platform-suse.conf` aus.

5.5.2 SSL-Fehlermeldung im Klient

Erscheint beispielsweise beim Versuch InteproxyServer mit dem Firefox auf `https://SERVERNAME:64609` anzusprechen folgende Warnmeldung:

```
Secure Connection Failed
An error occurred during a connection to SERVERNAME:64609.
SSL received a record that exceeded the maximum permissible length.
(Error code: ssl_error_rx_record_too_long)
```

Überprüfen Sie die SSL-Konfiguration, ggf. entfernen Sie in der `inteproxy.conf` den Kommentar in folgenden Zeilen:

```
SSL Engine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/apache2/ssl.crt/snakeoil-dsa.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/snakeoil-dsa.key
```

Hinweis

In der Beispiel Konfigurationsdatei `inteproxy.conf` werden Beispiel-Zertifikate der Distribution verwendet. Damit dies funktioniert muss das Paket `apache2-example-certificates` installiert sein. Für einen Produktivbetrieb wird empfohlen die Beispiel-Zertifikate durch eigene Zertifikate zu ersetzen.

Installation des InteProxy Server für Windows Server 2003 (SP2)

Die folgende Beschreibung der Installation des InteProxy Servers bezieht sich auf *Windows Server 2003 (SP2)*.

6.1 Installieren des Apache HTTP Server 2

Laden Sie den Apache HTTP Server 2.0.59 mit SSL-Unterstützung für Windows von <http://archive.apache.org/dist/httpd/binaries/win32/> herunter.

Installieren Sie den Apache HTTP Server 2.0.59 mit Hilfe des Windows Installers. Weitere Informationen zur Installation des Apache HTTP Server 2.0.59 finden Sie in der Apache Dokumentation [Using Apache with Microsoft Windows](#).

Die benötigten Apache-Module werden hierbei bereits mit installiert.

6.2 Herunterladen des InteProxy Servers

Ab Apache 2.2 wird von der Apache Software Foundation empfohlen, nicht mehr eine einzelne Konfigurationsdatei einzusetzen, sondern sie in mehrere kleinere Teile aufzutrennen. Eine Praxis, die bei Linux-Distributionen schon seit Apache 2.0.50 auf unterschiedliche Weise verfolgt wurde. Auf einem Windows-System finden Sie bei einer Standardinstallation jetzt ebenfalls mehrere Unterverzeichnisse im /conf-Verzeichnis.

Die Einrichtung des InteProxy Server erfolgt nach den Empfehlungen der Apache Software Foundation. Laden Sie das InteProxy Server Archive herunter (siehe [Download](#)) und entpacken Sie dieses in das Verzeichnis `C:\Programme\Apache Group\Apache2\conf`.

6.3 RewriteRule-Konfigurationsdatei

Passen Sie sich die InteProxy-RewriteRule-Datei `inteproxy-rewrite.conf` Ihren Bedürfnissen an. Tauschen Sie in der Zeile `mapgate` den USERNAME und das PASSWORT durch das vom LGN übermittelte Passwort und Nutzernamen aus.

Nach erfolgter Anpassung kopieren Sie die Datei nach `C:\Programme\Apache Group\Apache2\conf\InteProxy-SERVER-1.0.3\server\conf\inteproxy-rewrite.conf`

inteproxy-rewrite.conf:

```
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]
```

Bitte beachten Sie: Die Datei `inteproxy-rewrite.conf` darf in der Zeile `RewriteRule` **keine** Zeilenbrüche aufweisen. Die Zeilenbrüche dienen nur zur besseren Lesbarkeit.

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

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](#).

6.4 Einrichten des InteProxy Servers als separaten VirtualHost

Der Standard-Port des InteProxy Servers ist 64609. Ergänzen Sie daher in der Datei `C:\Programme\Apache Group\Apache2\conf\httpd.conf` noch die folgende Zeile:

```
Listen 64609
```

Um den InterProxy Server als separaten **VirtualHost** zu betreiben, ergänzen Sie am Ende der Datei `C:\Programme\Apache Group\Apache2\conf\httpd.conf` noch die folgende Zeile:

```
Include conf/InteProxy-SERVER-1.0.3/server/conf/inteproxy-WindowsServer2003.conf
```

Wenn Sie sich unsicher sind, wie Apache ihre `vhost`-Konfiguration interpretiert, nutzen Sie das Programm `Test Configuration` aus `Programme -> Apache HTTP Server 2.0.59 -> Configure Apache Server`.

Nach erfolgreichem Test des neu eingerichteten `VirtualHost` `inteproxy-WindowsServer2003` starten Sie den Apache HTTP Server zum Beispiel im `Apache Service Monitor` neu.

VirtualHost Konfigurationsdatei

Um den InteProxy Server als Virtuellen Host hinzufügen, kopieren Sie die kommentierte Vorlage `inteproxy.conf` nach `/etc/apache2/sites-available/` für die Debian Distribution und für die openSuSE Distribution nach `/etc/apache2/vhosts.d`. Die VirtualHost Konfigurationsdatei `inteproxy.conf` übernimmt einiges an Automation. So erfolgt das Laden der benötigten Apache-Module plattform-spezifisch durch die Zeile `Include /opt/InteProxy-SERVER-1.0.3/server/conf/platform-debian.conf` für die Debian Distribution **oder** durch die Zeile `Include /opt/InteProxy-SERVER-1.0.3/server/conf/platform-suse.conf` für die openSuSE Distribution. Sollten Sie die Apache-Module bereits geladen haben, können Sie die Zeile einkommentieren.

Die benötigten Apache-Module lassen sich bei Bedarf mit dem Befehl `a2enmod` manuell laden.:

```
a2enmod authz_host proxy proxy_http rewrite ssl
```

Werden die Apache-Module nicht mehr benötigt, können diese manuell mit dem Befehl `a2dismod` entfernt werden.

```
a2dismod authz_host proxy proxy_http rewrite ssl
```

Hinweis: Sollten die oben genannten Apache-Module entfernt werden, läuft der InteProxy Server nicht mehr.

Die VirtualHost Konfigurationsdatei `inteproxy.conf`

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

DocumentRoot /opt/InteProxy-SERVER-1.0.3/server

TransferLog /opt/InteProxy-SERVER-1.0.3/server/logs/access_log

#Include /opt/InteProxy-SERVER-1.0.3/server/conf/platform-suse.conf
Include /opt/InteProxy-SERVER-1.0.3/server/conf/platform-debian.conf
RewriteEngine On
# RewriteLogLevel 0
RewriteLog /opt/InteProxy-SERVER-1.0.3/server/logs/rewrite.log

# Die Datei conf/inteproxy-rewrite.conf beinhaltet die RewriteRules für die
# aktuelle InteProxy Funktionalität. Sollte die Datei nicht existieren, lesen
# Sie im Kapitel 6 wie Sie eine erstellen können.
Include /opt/InteProxy-SERVER-1.0.3/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>
```

Konfigurationsdatei inteproxy.cfg

Die Konfiguration der OWS-Proxydienste erfolgt über eine Konfigurationsdatei. Werden darin keine OWS-Dienste angegeben, verhält sich InteProxy Server wie ein normaler transparenter HTTP-Proxy. Dem Quelltext liegt eine beispielhafte Konfigurationsdatei `inteproxy.cfg` bei. Die Konfigurationsdatei beinhaltet die Services, die als OWS-Proxies fungieren. Bevor der InteProxy Server gestartet wird, muss die Konfigurationsdatei `inteproxy.cfg` mit dem Skript `create-rewrite-rules.py` in [Apache RewriteRule Direktiven](#) umgewandelt werden.

```
./create-rewrite-rules.py --config-file=inteproxy.cfg -o \
server/conf/inteproxy-rewrite.conf
```

Wird beim Starten von InteProxy Server keine Konfigurationsdatei angegeben, wird nach der Datei `inteproxy.cfg` im InteProxy Server-Hauptverzeichnis gesucht. Die Konfigurationsdatei legt darüber hinaus auch fest, ob eine Anmeldung gegen einen Proxy im internen Netzwerk nötig ist, um Dienste zu erreichen. Dazu müssen die Abschnitte `[inteproxy]` und `[http_proxy_authentication]` auskommentiert und angepasst werden. Eine beispielhafte Konfigurationsdatei ist die Datei `inteproxy.cfg`, die den Server `inteproxy-demo.intevation.org` als OWSProxy eingetragen hat.

```
# 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_authentication] aus und passen Sie Ihre
# !! Zugangsdaten entsprechend an.
#
# Anmeldung gegen einen Intranet-Proxy
```

```
# [inteproxy]
# https_proxy=http_proxy_authentication
# http_proxy=http_proxy_authentication
#
# [http_proxy_authentication]
# 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:
#
#   owspoxy   Der gegenüberliegende Rechner ist ein OWSPoxy,
#             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=owspoxy://meier:meier@inteproxy-demo.intevation.org/cgi-bin/frida-wms
      owspoxy://USERNAME:PASSWORT@www.geobasisdaten.niedersachsen.de/mapgate/*
```

ProxyRemote

Sollen Anfragen über einen Apache Proxy Server, welcher sich im Intranet befindet, nach außen durch eine Firewall geleitet werden, kann hier zu die Konfigurationsdirektive `ProxyRemote` verwendet werden. `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.

```

|-----|           |-----|
| InteProxy |       | proxy.remote |
-> | Server   | ->  | :8080         | ->
|-----|           |-----|

```

Im nachfolgenden Beispiel werden alle Proxy-Anfragen an `proxy.remote.com` weitergeleitet:

```
ProxyRemote * http://proxy.remote.com: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 `ProxyRemote` Konfigurationsdirektive sollte in die VirtualHost Konfigurationsdatei `inteproxy.conf` eingetragen. Nach erfolgter Anpassung sollte der Apache HTTP Server neu gestartet werden.

Hinweis: Für eine die `HTTPS_upstream-proxy` Unterstützung benötigen Sie einen Apache Server ab Version 2.2.15! Eine Proxy Authentifizierung wird zur Zeit noch nicht unterstützt.

URL Rewriting in WMS Capabilites

Das URL Rewriting ersetzt die URLs in den ausgelieferten Daten des Inteproxy Servers. So können beispielsweise die URL-Angaben in den OnlineResources des WMS Capabilites umgeschrieben werden.

10.1 Voraussetzungen

Das URL Rewriting benötigt die folgenden Apache-Module:

- `mod_substitute` (Modul erst ab Apache Version 2.2.7 verfügbar)
- `mod_filter` (Modul erst ab Apache Version 2.1 verfügbar)

10.2 Konfiguration

Damit das URL Rewriting angewendet werden kann, müssen zu erst die benötigten Module geladen werden. Bitte stellen Sie sicher das die benötigten Module in der jeweiligen Konfiguration `platform-*.conf` für Ihre Apache-Umgebung korrekt eingetragen sind. Beispielsweise müssen für Windows 2003 in der Datei `platform-WindowsServer2003.conf` folgende Zeilen stehen:

```
LoadModule filter_module modules/mod_filter.so
LoadModule substitute_module modules/mod_substitute.so
```

Zusätzlich müssen in der VirtualHost Konfigurationsdatei ihrer Umgebung die Apache `FilterProvider Direktive` und die Apache `FilterChain Direktive` gesetzt sein. Hier ein Beispiel für Windows 2003 in der Datei `inteproxy-WindowsServer2003.conf`:

```
FilterProvider fixurls SUBSTITUTE \
Content-Type "/(application\057vnd.ogc.wms_xml|text\057xml) ($|;)/"
FilterChain fixurls
```

Bitte beachten Sie: Das die Konfiguration der Direktiven **keine** Zeilenbrüche aufweisen dürfen. Die Zeilenbrüche dienen nur zur besseren Lesbarkeit.

Diese beiden Direktiven definieren eine *filter chain* um die URLs in der WMS Capabilities Antwort um zuschreiben.

Wichtig: Die WMS Capabilities Antworten müssen den MIME-Type/Content-Type `application/vnd.ogc.wms_xml` besitzen.

Für die Aktivierung des URL Rewritings muss mit Hilfe der Konfigurationsdatei `inteproxy.cfg` und mit dem Skript `create-rewrite-rules.py` mit der Option `--server-prefix` zusätzlich eine Apache `Substitute Direktive` in der Datei `inteproxy-rewrite.conf` erstellt werden.

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

Nach erfolgreicher Konfiguration starten Sie den Apache Webserver neu.

10.3 Test

Für einen einfachen Test, 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
```

Nach der erfolgreicher Konfiguration des Inteproxy Servers sollten das WMS Capabilities die geänderten URLs enthalten.

Erster Test

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.

11.1 Nutzerdaten

Um die Anwendungsbeispiele gegen den hier beschriebenen Demoserver zu nutzen, stehen Ihnen die folgenden Nutzerdaten im OWSPoxy 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.

11.2 Nutzung von InteProxy Server

Stellen Sie in Ihrer Anwendung der eigentlichen URL für den WMS Dienst den Text `http://servername:64609/` voran, so wird für den WMS explizit der InteProxy Server angesprochen.

11.3 Einfacher Funktionstest (über Web-Browser)

Mit diesem Test wird geprüft, ob 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 dann die eigentliche nachfolgende WMS-Anfrage 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&password=meier` an die sichere URL an.

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)