

Beratung und Support
Technische Plattform
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

Zertifikate-Anleitung

Erweiterung: Gesicherter Zugriff auf die paedML Novell

Stand: 19.08.2015

paedML® Novell

Version: 3.3.4 und 4.1

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Stefan Falk
Ulrich Frei
Carl Heinz Gutjahr
Friedrich Heckmann
Hubert Bechtold
Uwe Labs
Alfred Wackler

Endredaktion

Redaktion Support-Netz (de)

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.lmz-bw.de

Veröffentlicht: 2015

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

0.	Inhaltsverzeichnis	1
1.	HTTPS-gesicherter Zugriff auf die paedML® Novell	2
1.1.	Einleitung	2
1.2.	Der Zugriff von außen	3
2.	Anpassung der Sophos-Firewall *	6
3.	Konfiguration und Einrichtung auf dem GServer03 *	6
3.1.	Zugriff von innen über die gleichen URLs *	6
3.2.	DNS-Eintrag beim Provider *	8
4.	Wildcard-Zertifikat einrichten *	8
5.	Apache2 Konfiguration	10
5.1.	Proxy-Konfiguration *	10
5.1.1.	Erweiterungsmöglichkeit	17
5.1.2.	Hintergrund-Informationen	21
5.2.	HTTPS-Umlenkung einrichten *	21
6.	Fazit	23
7.	Anhang	24
7.1.	Einsatzmöglichkeit der neuen vhost-ssl.conf	24
7.2.	Selbstsigniertes Wildcard-Zertifikat erstellen	24
8.	Änderungen gegenüber der Anleitung vom 17.06.2014	26

1. HTTPS-gesicherter Zugriff auf die paedML® Novell

Anmerkung:

In diesem Dokument sind neben der eigentlichen Anleitung ausführliche Erläuterungen und Erklärungen enthalten, die zum Verständnis des Verfahrens beitragen sollen. Die Kapitel bzw. Abschnitte, die die Installationsanleitung mit von Ihnen durchzuführenden Schritten enthalten, sind durch eine vertikale Linie am linken Rand gekennzeichnet. Kapitel bzw. Abschnitte, die Tätigkeiten erfordern, sind außerdem in der Überschrift durch * gekennzeichnet.

Änderungen gegenüber der Anleitung vom 17.06.2014

Wenn Sie die Anleitung vom 17.06.2014 bereits umgesetzt haben, so müssen Sie in Ihrer *vhost-ssl.conf* und in *userdir.conf* aus Sicherheitsgründen einige Änderungen vornehmen. Diese Änderungen sind auch erforderlich, um die Kommunikation mit dem neuen *Vibe 4.0* und *Filr 1.2* zu ermöglichen.

Lesen Sie hierzu Kapitel 8

Standard-Kommunikations-Verfahren ab der kommenden Version 4.1 der paedML Novell

Das in dieser Anleitung beschriebene Verfahren wird ab der kommenden Version 4 der paedML Novell bereits eingerichtet sein und dort als Standard-Kommunikations-Verfahren empfohlen.

(Sie müssen dort dann lediglich noch das eigene Zertifikat einrichten.)

1.1. Einleitung

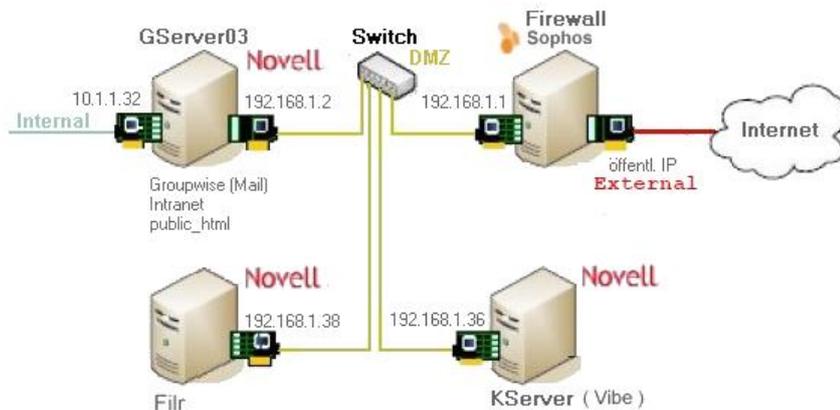
Die paedML Novell bietet vielfältige Webdienste und Möglichkeiten zur Kommunikation, den Zugriff auf persönliche Daten, die Veröffentlichung von Webseiten und vieles mehr. Dabei soll der Zugang sowohl intern als auch extern möglich sein. Auch ein externer Zugriff über Mobilgeräte ist erwünscht.

Wenn Sie diese Möglichkeiten nutzen möchten, so ist dafür ein gesicherter verschlüsselter Zugang über HTTPS erforderlich. Die Absicherung erfolgt dabei über Zertifikate. In der Auslieferungsversion der paedML Novell sind sowohl im GServer03 als auch im KServer nur sogenannte selbstsignierte Zertifikate enthalten. Dies hat bei Zugriffen über einen Browser, beispielsweise auf das Intranet, auf GroupWise-Webaccess oder auch Vibe und Filr den Nachteil, dass im Browser eine Warnung wegen eines nicht-vertrauenswürdigen Zertifikats erscheint, das dann manuell akzeptiert werden muss. Dies ist einerseits lästig und andererseits nicht im Sinne einer sicherheitsbewussten Handhabung des Internets.

Sinnvoller ist es also, dass Sie sich für die Domain Ihrer Schule ein sogenanntes vertrauenswürdiges Zertifikat beschaffen. Dies ist auch unbedingt erforderlich, wenn Sie über mobile Geräte zugreifen wollen, da diese meist keine selbstsignierten Zertifikate akzeptieren.

1.2. Der Zugriff von außen

Der Zugriff von außen auf die Webdienste der paedML Novell ist auf mehrere Arten möglich. Die folgende Abbildung zeigt zunächst die technische Struktur der paedML Novell.



Die verschiedenen Webdienste werden teils vom GServer03, teils von separaten Servern in der DMZ bereitgestellt. *Groupwise (Mail)*, *Intranet* und *public_html* (persönliche Webseiten) werden auf dem *Gserver03* bereitgestellt. Die Kommunikationsplattform *Vibe* läuft auf dem *KServer* und *Filtr* auf einem eigenen Server. Bei einem Zugriff von außen muss die Verbindung in geeigneter Weise auf den jeweiligen Server geleitet werden. Dafür gibt es verschiedene Möglichkeiten. Der Zugang erfolgt dabei in jedem Fall über die Sophos-Firewall der paedML Novell.

Möglichkeit 1:

Zugang über eine einzige öffentliche IP-Adresse.

Der Zugriff auf die verschiedenen Server wird über zugeordnete Portnummern geregelt.

z.B. `https://server.<Ihre schuldomain>:52443` für Zugriff auf *Vibe*
`https://server.<Ihre schuldomain>:53443` für Zugriff auf *Filtr*

- + Nur eine öffentliche IP-Adresse erforderlich
- Sehr unkomfortabler, kryptischer Zugang für die Nutzer
- Portfreigabe im Router (Belwü) erforderlich
- Konfiguration der Firewall (Sophos) erforderlich

Details können Sie in der Anleitung zur Installation von *Vibe* und von *Filtr* nachlesen.

Möglichkeit 2:

Mit Belwü als Provider stehen der Schule normalerweise mehrere öffentliche IP-Adressen zur Verfügung. Damit ist es möglich, jedem Server eine eigene IP-Adresse zuzuordnen. Für die Namensauflösung müssen Sie bei Belwü für jeden Server einen DNS-Eintrag einrichten lassen und für jede gewählte IP-Adresse die Freigabe von Port 443 im Router veranlassen.

Normalerweise ist bei Belwü bereits der DNS-Eintrag `server.<Ihre Schuldomain>` vorhanden. Dieser Eintrag verweist in der paedML-Konfiguration der Sophos-Firewall auf den *GServer03*. Für jeden weiteren Server müssen Sie beim Provider einen DNS-Eintrag (A-Record auf die jeweilige dem Server zugeordnete IP) einrichten lassen.

z.B. `kserver.<Ihre Schuldomain>` oder `vibe.<Ihre Schuldomain>`
`filtr.<Ihre Schuldomain>`

Nutzer können mit dieser Konfiguration die Dienste bequem aufrufen:

z.B. <https://vibe.<Ihre schuldomain>> und <https://filr.<Ihre schuldomain>>

- + Nutzerfreundlicher Zugang
- Portfreigabe im Router (Belwü) erforderlich
- Konfiguration der Firewall (Sophos) erforderlich
- Für jeden Server ist ein eigenes Zertifikat erforderlich

Details für diese Variante können Sie in der Anleitung zur Installation von *Vibe* und von *Filr* nachlesen.

Möglichkeit 3:

Für die paedML Novell wurde nun eine weitere Variante entwickelt, die einen geringeren Einrichtungsaufwand erfordert, nutzerfreundlich und außerdem flexibel erweiterbar ist. Die Einrichtung wird in diesem Dokument beschrieben.

Zunächst aber kurz die zugrundeliegende Funktionsweise:

Der Zugang erfolgt wieder über eine einzige öffentliche IP-Adresse. Alle Anfragen werden zunächst an den GServer03 gerichtet. Dort wird Apache als Proxy eingerichtet und leitet die Anfragen an den jeweiligen Server weiter. Außerdem wird in der beschriebenen Konfiguration dafür gesorgt, dass Anfragen auf <https://> umgelenkt werden, wenn sie über eine ungesicherte [http](http://)-Anfrage erfolgen.

Hinweis: Browser ergänzen in der Regel [http](http://) als Protokoll, wenn in der URL kein Protokoll angegeben wird. So wird vom Browser bei der URL *server.meineschule.de* automatisch die Anfrage <http://server.meineschule.de> gesendet. Für den Nutzer stellt sich der Zugang dann wie folgt dar (im Folgenden wird als Beispiel die Domain *meineschule.de* verwendet. Diese ist natürlich durch Ihre eigene Schuldomain zu ersetzen).

Zugriff auf Vibe: *vibe.meineschule.de* oder auch <https://vibe.meineschule.de> beziehungsweise *kserver.meineschule.de* oder auch <https://kserver.meineschule.de>

Zugriff auf Filr: *filr.meineschule.de* oder auch <https://filr.meineschule.de>

GW-Webaccess: *mail.meineschule.de* oder auch <https://mail.meineschule.de>
Dies ist äquivalent zu <https://server.meineschule.de/gw/webacc>

Intranet: *server.meineschule.de* oder auch <https://server.meineschule.de>

Kollegium: *kollegium.meineschule.de* oder auch <https://kollegium.meineschule.de>
Dies ist äquivalent zu <https://server.meineschule.de/intranet/schulweb/>
Hier entsteht durch die Umlenkung auf den [https](https://)-Zugang ein großer Sicherheitszugewinn. Beim Zugang zum Kollegiums-Webbereich ist ja eine Anmeldung mit Benutzernamen und Passwort erforderlich.
In der beschriebenen Konfiguration erfolgt nun bereits diese Anmeldung [https](https://)-gesichert bzw. verschlüsselt.

public_html: Auch der public_html-Zugang (persönliche Webseiten) erfolgt nun gesichert über https. Dies erlaubt dort auch die Einrichtung von geschützten Bereichen, die nur mit Anmeldung erreichbar sind und bei denen die Anmeldung https-gesichert erfolgt.

Für diese Möglichkeit wird eine separate Anleitung veröffentlicht.

Optional: Webserver in der DMZ mit IP 192.168.1.3
web.meineschule.de oder auch <https://kollegium.meineschule.de>
Beschreibung siehe Kapitel *Proxy-Konfiguration/Erweiterungsmöglichkeiten*.

- + Sehr nutzerfreundlicher Zugang
Für alle Bereiche gesicherter Zugang (https wird erzwungen)
Einrichtung:
Nur Änderungen am GServer03 und eine einmalige Umstellung an der Sophos Firewall.
Nur auf einem Server, dem GServer03 muss ein Zertifikat (Wildcard-Zertifikat) eingerichtet werden.
Bei Belwü nur Wildcard-DNS-Eintrag erforderlich.
- Die Kosten für ein Wildcard-Zertifikat sind in der Regel etwas höher als die Kosten für die Einzelzertifikate für die verschiedenen Server. Diese Kosten relativieren sich aber, wenn man die Dienstleistungskosten für Einrichtung und spätere Zertifikatserneuerung einbezieht.

In den folgenden Kapiteln werden nun die erforderlichen Anpassungen und die Konfiguration dieser 3. Möglichkeit beschrieben.

2. Anpassung der Sophos-Firewall *

In der Auslieferungsversion der Sophos-Firewall erreicht man den Gserver03 von außen über die Ports 51080 bzw. 51443. Die Ports 80 und 443 zeigen auf einen optionalen Webserver in der DMZ (IP 192.168.1.3). Bei der in diesem Dokument beschriebenen Zugangsart soll über die Proxies auf dem Gserver03 aber über die Standardports 80 und 443 (keine Portangabe im Browser erforderlich) zugegriffen werden. Dafür muss in der Sophos-Firewall eine Anpassung erfolgen, falls dies nicht bereits geschehen ist.

Hinweis:

Ein eventuell vorhandener Webserver in der DMZ ist nun nicht mehr direkt über Port 80 bzw. 443 von außen erreichbar. Sie können diesen aber über die in diesem Dokument beschriebene Zugangsmöglichkeit über Proxies auf dem GServer03 erreichen. Die Anleitung hierfür finden Sie im Kapitel *Proxy-Konfiguration/Erweiterungsmöglichkeiten*.

Melden Sie sich an der Sophos-Firewall an.

Wählen Sie nun unter *Network Security/NAT* den Reiter *DSNAT/SNAT* bzw. unter *Network Protection/NAT* den Reiter *NAT* bei Sophos 9.

Editieren Sie die DNAT-Regel [ASG-80] bzw. die Regel *Regel Any-->HTTP 80-->External (Address)*.

Ersetzen Sie im Eingabefeld *Destination* den Eintrag *DMZ Web-Server (WEB)* durch *DMZ Gserver03 (SRV)* und übernehmen Sie die Änderung mit *Save*.

Editieren Sie die DNAT-Regel [ASG-443] bzw. die Regel *Regel Any-->HTTPS 443-->External (Address)*.

Ersetzen Sie hier ebenso im Eingabefeld *Destination* den Eintrag *DMZ Web-Server (WEB)* durch *DMZ Gserver03 (SRV)* und übernehmen Sie die Änderung mit *Save*.

Hiermit ist die Anpassung der Sophos-Firewall abgeschlossen.

3. Konfiguration und Einrichtung auf dem GServer03 *

3.1. Zugriff von innen über die gleichen URLs *

Damit die Anfragen (server, mail, vibe, filr usw.) auch aus dem Intranet über dieselben URLs wie von außen erreichbar sind, sind Einträge im DNS-System auf dem GServer03 erforderlich. Die Anfragen erfolgen dann ebenfalls über https mit dem echten Zertifikat und somit entfallen auch im Intranet die Browserwarnungen.

Anpassung der Bind-Konfiguration

Es muss im internen DNS-Server eine Zone für die externe Domain der Schule angelegt werden, damit die Namensauflösung intern direkt auf die Intranet-Adresse 10.1.1.32 des GServer03 verweist und Anfragen aus dem Intranet direkt dorthin gelangen.

Editieren Sie hierzu die Datei `/etc/named.conf`, z.B. über WinSCP.

Fügen Sie am Ende der Datei folgende Zeilen ein (falls dieser Eintrag nicht bereits vorhanden ist):

```
zone "meineschule.de" in {
    file "master/meineschule.de";
    type master;
};
```

Ersetzen Sie wieder `meineschule.de` durch den echten Domainnamen Ihrer Schule.

Zonendatei

Es muss nun in `/var/lib/named/master` eine Zonendatei für diese Domain angelegt werden.

Editieren Sie die Datei `meineschule.de` aus dem Download. Ersetzen Sie wieder `meineschule.de` durch den echten Domainnamen Ihrer Schule. Achten Sie unbedingt darauf, dass der jeweils den Domainnamen abschließende Punkt nicht verloren geht. Speichern Sie die Datei mit dem Domainnamen als Dateinamen. Kopieren Sie die Datei, z.B. mit WinSCP, nach `/var/lib/named/master`.

```
$TTL 2D
@      IN SOA      meineschule.de.    root.meineschule.de.    (
                2013031900    ; serial
                3H           ; refresh
                1H           ; retry
                1W           ; expiry
                1D )         ; minimum

                IN NS      gserver03.meineschule.de.

server      IN A      10.1.1.32
mail        IN CNAME   server
kserver     IN CNAME   server
vibe        IN CNAME   server
filr        IN CNAME   server
kollegium   IN CNAME   server

;www        IN CNAME   server
www         IN NS      192.168.1.1 ; Astaro
```

Da der Zugang immer über die Proxies auf dem GServer03 über 10.1.1.32 erfolgt, verweisen die Einträge tatsächlich alle auf `server` bzw. `10.1.1.32` und nicht mehr auf die tatsächlichen Adressen der Server in der DMZ.

Hinweis: Wenn Sie eine Webseite bei einem Hoster (z.B. Belwü) betreiben, die mit beginnendem `www` aufgerufen wird, so bewirkt die obige letzte `www`-Zeile, dass die Namensauflösung für `www` an den übergeordneten DNS-Server (hier Astaro bzw. Sophos) weitergeleitet wird. Die auskommentierte `www`-Zeile müsste benutzt werden, wenn die `www`-Seite auf dem GServer03 liegt.

Starten Sie zum Abschluss den Nameserver neu an der Konsole des GServer03 mit
`gserver03:~ # rncamed restart`

3.2. DNS-Eintrag beim Provider *

Bei den meisten Schulen erfolgt der Internetzugang über Belwü als Provider. Die Schule bekommt dabei einige feste, öffentliche IP-Adressen. In der paedML Novell wird dann das External-Interface der Sophos-Firewall an den Belwü-Router angeschlossen.

Belwü richtet auf Ihrem DNS-Server in der Regel einen DNS A-Record ein, *server.meineschule.de*, der auf die von Belwü zugeteilte öffentliche IP-Adresse verweist, auf die wir bei der Installation das External-Interface der Sophos-Firewall eingerichtet haben.

Nun sollen aber auch *vibe.meineschule.de*, *filr.meineschule.de*, *mail.meineschule.de*, *kollegium.meineschule.de* auf die oben genannte Adresse aufgelöst werden. Nun könnte man für jeden dieser Zugänge einen entsprechenden A-Record einrichten lassen. Wenn wir dann noch *wetter.meineschule.de* hinzunehmen wollten, müssten wir wieder bei Belwü vorstellig werden und dafür einen weiteren A-Record einrichten lassen.

Hier gibt es nun die Möglichkeit, vom Provider einen Wildcard-DNS-Record **.meineschule.de* eintragen zu lassen. Stern * steht dabei für jeden beliebigen Namen. Wir können also ohne weiteres später auf unserem GServer03 weitere Proxies bzw. Ziele einrichten, ohne dass hierfür bei Belwü noch Änderungen erforderlich wären. So verweist dann z.B. *smv.meineschule.de* genauso auf die o.g. öffentliche IP-Adresse und die Anfrage wird somit zu unserem GServer03 geleitet.

Anmerkung: Da für *smv.meineschule.de* zunächst noch kein Proxy eingerichtet ist, landet eine solche Anfrage beim Default-Proxy, der *vhost-ssl.conf*, und wird somit genau so behandelt, wie die Anfrage *server.meineschule.de*.

Hinweis: Viele Schulen haben Ihre Webseiten bei Belwü gehostet und sind über *www.meineschule.de* erreichbar. Dafür ist auf dem Nameserver bei Belwü ein A-Record eingerichtet, *www.meineschule.de*, der auf die IP des Belwü-Webserver verweist. Die A-Records für eine Domain haben Vorrang vor dem Wildcard-Record dieser Domain. Damit werden alle Namen, für die ein A-Record besteht auf die jeweils im A-Record eingetragene Ziel-IP aufgelöst. Alle Namen für die kein A-Record besteht werden dann über den Wildcard-Record aufgelöst.

Nehmen Sie mit Belwü Kontakt auf, um einen Wildcard-DNS-Record für Ihre Domain einrichten zu lassen. Dies ist in der Regel von Belwü in einem Tag umgesetzt. Halten Sie beim Anruf Ihre Belwü-Kundennummer bereit.

4. Wildcard-Zertifikat einrichten *

Mit einem Wildcard-Zertifikat können beliebig viele Server zu einer Domain abgesichert werden. So werden mit einem Wildcard-Zertifikat, das für **.meineschule.de* eingerichtet wurde, die Server *server.meineschule.de*, *vibe.meineschule.de*, *mail.meineschule.de* usw. abgesichert. Dabei kann an der Stelle von * ein beliebiger Servername stehen. Damit sind Sie auch für eventuelle Erweiterungen zertifikatsseitig gerüstet.

Das Wildcard-Zertifikat wird auf dem GServer03 genauso eingerichtet wie das Zertifikat für einen einzelnen Server. Deshalb wird dies hier nicht gesondert beschrieben, sondern wir verweisen auf Kapitel 3 der Anleitung [Zertifikate2-BPZ-Novell-334.pdf](#). Die in der *vhost-ssl.conf* notwendigen Änderungen sind im Kapitel *Apache/Proxy Konfiguration* in der vorliegenden Anweisung separat beschrieben. Die Anweisungen

bezüglich iprint und der Anwendungsobjekte müssen Sie jedoch nach der genannten Anleitung durchführen, falls Sie nicht bereits gültige Zertifikat einsetzen.

Sie müssen in der *Zertifikate2-BPZ-Novell-334-Anleitung* in Kapitel 3.1 *Erzeugung des Zertifikats* lediglich jeweils **server.meineschule.de** bzw. **gserver03.meineschule.de** durch ***.meineschule.de** ersetzen. Wenn Sie keine eigene Firstlevel-Domain besitzen, sondern für Ihre Schule nur eine Subdomain bei Belwü eingerichtet ist, wie beispielsweise *meineschule.meinort.schule.de* so müssen Sie **server.meineschule.de** bzw. **gserver03.meineschule.de** ersetzen durch ***.meineschule.meinort.schule.de**.

Bei der Bestellung müssen Sie nun ein Wildcard-Zertifikat auswählen. Eine Auswahl steht Ihnen über denselben Link zur Verfügung, wie im *Kapitel 3.2* der o.g. Anleitung beschrieben. Die Zertifikate werden von Lieferanten in verschiedener Form bereitgestellt, z.B. wie beschrieben als zip-Datei, aber auch als Textanhang in einer E-Mail oder zum Download. Halten Sie sich hier an die Anleitung Ihres Lieferanten. Das Zertifikat wurde beim Autor unter dem Namen **.meineschule.crt* geliefert und musste dann auf dem Server nach *servercert.pem* kopiert werden. Das Zwischenzertifikat wurde mit dem Namen *intermediate.crt* geliefert und ist auf dem Server nach *servercabundle.pem* zu kopieren.

Achtung:

Wenn Sie mit Ihrem Zertifikat ein Zwischenzertifikat erhalten haben, so müssen Sie die in Kapitel 5 beschriebenen *vhost-ssl.conf* auskommentierten Zeilen

```
#SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
```

durch Entfernen des Kommentarzeichens # aktivieren.

Hinweis:

Wenn Sie im Moment noch kein vertrauenswürdige Wildcard-Zertifikat besitzen oder beschaffen können, so können Sie die in diesem Dokument beschriebene Zugangsweise trotzdem realisieren. Dazu können Sie ein selbstsigniertes Wildcard-Zertifikat erstellen und ebenso wie ein gekauftes vertrauenswürdige Zertifikat einbinden. Die Nutzer Ihrer Seiten erhalten dann natürlich im Browser weiterhin eine Zertifikatswarnung. Ziel sollte aber auf jeden Fall die Beschaffung eines vertrauenswürdigen Zertifikats sein. Sie müssen dann nur noch das selbstsignierte Zertifikat gegen das vertrauenswürdige Zertifikat austauschen. Nur mit einem vertrauenswürdigen Zertifikat kommt aus datenschutzrechtlicher Seite eine sichere Kommunikation zustande (siehe http://lehrerfortbildung-bw.de/netz/it-infrastruktur/3_dienste/).

Auch wenn Sie für GServer03, Vibe und Filr bereits Einzelzertifikate erworben haben, können Sie den in diesem Dokument beschriebenen Zugang umsetzen.

In der *vhost-ssl.conf* (siehe die Virtual-Host-Abschnitte für die jeweiligen Server/Dienste mit den dazugehörigen **SSLCertificateFile**-Einträgen) verweisen Sie dann nicht bei jeder Rewrite-Rule auf das Wildcard-Zertifikat, sondern in der Regel für den Vibe auf das Vibe-Zertifikat, für den Filr auf das Filr-Zertifikat, für den GServer03 auf das GServer-Zertifikat (die Zertifikate müssen dann lokal auf dem GServer vorliegen, */etc/ssl/servercerts/gserver03*, */etc/ssl/servercerts/vibe* ...).

Anmerkung:

Der beschriebene Zugang über Apache Proxies auf dem GServer03 mit Wildcard-Zertifikat erspart die doch teilweise aufwändige Einrichtung von separaten Zertifikaten auf den einzelnen Servern. Bei der nach einigen Jahren erforderlichen Zertifikatserneuerung muss man sich nur um ein Zertifikat auf einem Server kümmern. Deshalb empfohlen.

5. Apache2 Konfiguration

5.1. Proxy-Konfiguration *

Wie beschrieben sollen alle Anfragen beim Apache2 des GServer03 auflaufen und über die Proxy-Funktionalität an die entsprechenden Server oder auch an die entsprechenden Seiten auf dem GServer03 weitergeleitet werden.

Dazu muss auf dem GServer03 die Datei `/etc/apache2/vhosts.d/vhost-ssl.conf` angepasst und erweitert werden. Für jeden Proxy wird ein virtueller Host mit entsprechenden Rewrite-Regeln erstellt. Erstellen Sie zunächst von der Originaldatei eine Sicherungskopie.

An der Serverkonsole: Wechseln Sie zunächst in das Verzeichnis `/etc/apache2/vhosts.d`
gserver03:/etc/apache2/vhosts.d #cp -a vhost-ssl.conf vhost-ssl.conf.original

Ersetzen Sie in der heruntergeladenen Datei `vhost-ssl.conf` die Einträge `meineschule.de` jeweils durch den echten Domainnamen Ihrer Schule. Wenn Sie den Kserver einsetzen und Sie als Hostnamen statt `vibe kserver` benutzen wollen, ändern Sie dies in der `vhost-ssl.conf` im Abschnitt Vibe ab. Kopieren Sie die Datei dann nach `/etc/apache2/vhost-ssl.conf`. **Wenn zu Ihrem Zertifikat kein Zwischenzertifikat geliefert wird, kommentieren Sie die Zeilen mit `servercabundle.pem` aus.**

Falls Sie in Ihrer ursprünglichen `vhost-ssl.conf` bereits eigene Änderungen vorgenommen haben, so müssen Sie diese noch von der gesicherten Originaldatei in die neue Datei übertragen. Prüfen Sie, ob Ihre früheren Änderungen mit den Änderungen dieser Anleitung verträglich sind.

Im Folgenden wird der Inhalt der Datei abgebildet (nur zur Information, falls Sie den Download verwenden).

- Vorhandene Zeilen, die nicht mehr gebraucht bzw. durch andere Einträge ersetzt werden, sind durch ein `-` gekennzeichnet und werden mit `###` auskommentiert (das `-` ist natürlich nicht mit einzugeben). Diese Zeilen können auch gelöscht werden.
- Neu hinzugekommene Zeilen werden durch `+` gekennzeichnet (das `+` ist natürlich nicht mit einzugeben).
- Kommentierungen der Änderungen erfolgen durch `##`
- Geänderte Zeilen erscheinen im Fettdruck

Hinweis: Mit der neuen `vhost-ssl.conf` wurde auch die SSL-Konfiguration des Apache verändert. Das SSL-Protokoll schränkt die Kommunikation zwischen Server und Clients nicht auf eine Verschlüsselungsmethode für den Datenaustausch ein. Es gibt eine Vielzahl an möglichen Verfahren, die Server und Client aushandeln können. Die Ciphersuite des Apache gibt dabei die erlaubten Verfahren vor, die für eine Verbindung zugelassen werden. Die neue Sicherheitskonfiguration des Apache des GServers trägt dem Umstand Rechnung, dass inzwischen beispielsweise das Protokoll SSLv2 als nicht mehr sicher angesehen wird und deshalb deaktiviert werden sollte. Der dafür zuständige Abschnitt der `vhost-ssl.conf`:

```
+ SSLProtocol all -SSLv2 -SSLv3
+ SSLHonorCipherOrder on
+ SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES: \
                  !MD5:!EXP:!kEDH:!PSK:!SRP:!kECDH' (eine Zeile)
```



Der Backslash in der dritten Zeile deutet nur den Zeilenumbruch an und ist nicht Teil der CipherSuite-Konfiguration, darf also nicht eingegeben werden. Hier und in allen weiteren Auszügen aus der *vhost-ssl.conf* deutet der Backslash und der Hinweis (*eine Zeile*) auf diesen Zeilenumbruch hin.

Da inzwischen auch an die Kommunikation mit den Proxies, wie z.B. von Vibe und von Filr 1.2 höhere Sicherheits-Anforderungen bestehen und die Kommunikation sonst geblockt wird, müssen entsprechende Einträge auch bei allen Proxies erfolgen.

```
+ SSLProtocol all -SSLv2 -SSLv3
+ SSLHonorCipherOrder on
+ SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES: \
                  !MD5:!EXP:!kEDH:!PSK:!SRP:!kECDH' (eine Zeile)
+ SSLProxyProtocol all -SSLv2 -SSLv3
+ SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
                       !EXP:!kEDH:!PSK:!SRP:!kECDH' (eine Zeile)
```

Und hier nun im Zusammenhang die komplette *vhost-ssl.conf* zum Überblick.

```
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs-2.0/mod/mod_ssl.html>
#
# For the moment, see <URL:http://www.modssl.org/docs/> for this info.
# The documents are still being prepared from material donated by the
# modssl project.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Until documentation is completed, please check http://www.modssl.org/
# for additional config examples and module documentation. Directives
# and features of mod_ssl are largely unchanged from the mod_ssl project
# for Apache 1.3.

+ ## Modifikationen ZEN-Novell Landesmedienzentrum Baden-Wuerttemberg
+ ## 22.02.2014 / Ulrich Frei
+ ## 12.12.2014: Aenderung wegen Poodle-Vulnerability
```

```

+ ## Zeile "SSLProtocol all -SSLv2" geaendert in "SSLProtocol all -SSLv2 -SSLv3"
+ ## 25.04.2015 Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+ ##           Sicherheitseinstellungen
<IfDefine SSL>

<IfDefine !NOSSL>

#
# SSL Virtual Host Context
#

+ <Proxy *>
+   Order deny,allow
+   Allow from all
+ </Proxy>

+ NameVirtualHost *:443

- ### <VirtualHost _default_:443>
+ <VirtualHost *:443>
    # General setup for the virtual host
    DocumentRoot "/srv/www/htdocs"
    #ServerName www.example.com:443
    #ServerAdmin webmaster@example.com
+   ServerName default.meineschule.de:443
+   ServerAlias gserver03.oes.ml-bw.de:443
    ErrorLog /var/log/apache2/error_log
    TransferLog /var/log/apache2/access_log

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on
+   SSLProxyEngine on

    # SSL Cipher Suite:
    # List the ciphers that the client is permitted to negotiate.
    # See the mod_ssl documentation for a complete list.
    # Die Original-Cipher-Suite wurde nach Security-Audit im Mai 2014 durch unten
    # folgende drei Zeilen ersetzt (A. Wackler), 25.04.2015:
-   # SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
+   SSLProtocol all -SSLv2 -SSLv3
+   SSLHonorCipherOrder on
+   SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
                    !EXP:!kEDH:!PSK:!SRP:!kECDH'          (eine Zeile)
+   SSLProxyProtocol all -SSLv2 -SSLv3
+   SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
                        !EXP:!kEDH:!PSK:!SRP:!kECDH'+      (eine Zeile)

```

```

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)

- ### SSLCertificateFile /etc/ssl/servercerts/servercert.pem
  ## verlegt nach unten zu Wildcard-Zertifikat *.meineschule.de
  #SSLCertificateFile /etc/apache2/ssl.crt/server-dsa.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)

- ### SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
  ## verlegt nach unten zu Wildcard-Zertifikat *.meineschule.de
  #SSLCertificateKeyFile /etc/apache2/ssl.key/server-dsa.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.

#SSLCertificateChainFile /etc/apache2/ssl.crt/ca.crt

+ #####
+ ## Wildcard-Zertifikat *.meineschule.de ##
+ ## CA ..... ##
+ ## ausgestellt am ..... ##
+ ## gültig bis ..... ##
+ ## gekauft bei ..... ##
+ ## http://..... ##
+ ## installiert am 28.01.2014 / Vorname Name ##
+ #####
+ SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+ SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+ #SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem

## Hinweis Zertifikate
## =====
    
```

```

## Die ursprünglichen selfsigned Zertifikate wurden mit Zusatz .original gesichert
## Die gekauften Wildcardzertifikat-Dateien wurden kopiert (Anleitung LMZ)
## *.meineschule.crt --> servercert.pem
## *.meineschule.key --> serverkey.pem
## intermediate.crt --> servercabundle.pem

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
...
!!! hier wird aus Platzgründen eine größere Anzahl von Zeilen
!!! ausgeblendet, bei denen keine Änderungen erforderlich sind.
...
# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog /var/log/apache2/ssl_request_log ssl_combined

+ RewriteEngine On
+ ## zur Fehlersuche aktivieren, falls Probleme auftauchen sollten
+ ## RewriteLog /var/log/apache2/rewrite.log
+ ## RewriteLogLevel 2

+ ## Redirect zur Benutzung von public_html
+ ## In /etc/apache2/conf.d/userdir.conf nicht mehr erforderlich
+ RewriteMap MapHome txt:/srv/www/htdocs/userdir/redirect_map.txt
+ RewriteRule ~([^\/]*) (.*) ${MapHome:$1}$2
+ ## die RewriteRule wurde gegenüber der Version in /etc/apache2/conf.d/userdir.conf
+ ## verändert. Durch den Wegfall von \ / ist nun der abschließende / nicht mehr
+ ## erforderlich
+ ## z.B. server.meineschule.de/~SpechtB-LFB
+ ## statt server.meineschule.de/~SpechtB-LFB/

+ ## Groupwise Webaccess über https://server.meineschule.de/mail (optional)
+ RewriteRule ([^\/]*)\mail(.*) https://server.meineschule.de/gw/webacc$2
</VirtualHost>

## Für jeden Proxy wird nun ein virtueller host eingerichtet:

+ ##----- Mail -----
+ ##----- Aufruf: https://mail.meineschule.de -----
+ <VirtualHost *:443>
+   ServerName mail.meineschule.de:443
+
+   SSLEngine on
+   SSLProxyEngine on
+

```

```

+ # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+ # Sicherheitseinstellungen, 25.04.2015
+ SSLProtocol all -SSLv2 -SSLv3
+ SSLHonorCipherOrder on
+ SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+             !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+ SSLProxyProtocol all -SSLv2 -SSLv3
+ SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+             !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+
+ CustomLog /var/log/apache2/ssl_request_log  ssl_combined
+
+ ## Wildcard-Zertifikat *.meineschule.de
+ SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+ SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+ #SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
+
+ RewriteEngine On
+ ## RewriteLog /var/log/apache2/rewrite.log
+ ## RewriteLogLevel 2
+
+ RewriteRule ([^/]*) (.*) https://server.meineschule.de/gw/webacc$2
+ </VirtualHost>
+
+ ##----- Vibe -----
+ ##----- Aufruf: https://vibe.meineschule.de -----
+ ## Falls Sie hier lieber kserver.meineschule.de verwenden wollen,
+ ## ersetzen Sie vibe jeweils durch kserver
+ ## Es ist auch möglich für vibe und für kserver einen virtuellen host anzulegen.
+ <VirtualHost *:443>
+     ServerName vibe.meineschule.de:443
+
+     SSLEngine on
+     SSLProxyEngine on
+
+     # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+     # Sicherheitseinstellungen, 25.04.2015
+     SSLProtocol all -SSLv2 -SSLv3
+     SSLHonorCipherOrder on
+     SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+             !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+     SSLProxyProtocol all -SSLv2 -SSLv3
+     SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+             !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+
+     CustomLog /var/log/apache2/ssl_request_log  ssl_combined
+
+     ## Wildcard-Zertifikat *.meineschule.de
  
```

```

+ SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+ SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+ #SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
+
+ ProxyPreserveHost on
+ RewriteEngine On
+ # RewriteLog /var/log/apache2/rewrite.log
+ # RewriteLogLevel 2
+
+ RewriteRule ^(.*)$ https://192.168.1.36$1 [P]
+ # Alternativ kann auch verwendet werden:
+ # RewriteRule ^(.*)$ https://192.168.1.36:8443$1 [P]
+ </VirtualHost>
+
+ ##----- Filr -----
+ ##----- Aufruf: https://filr.meineschule.de
+ <VirtualHost *:443>
+   ServerName filr.meineschule.de:443
+
+   SSLEngine on
+   SSLProxyEngine on
+
+   # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+   # Sicherheitseinstellungen, 25.04.2015
+   SSLProtocol all -SSLv2 -SSLv3
+   SSLHonorCipherOrder on
+   SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                   !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+   SSLProxyProtocol all -SSLv2 -SSLv3
+   SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                       !EXP:!kEDH:!PSK:!SRP:!kECDH'       (eine Zeile)
+
+   CustomLog /var/log/apache2/ssl_request_log    ssl_combined
+
+   ## Wildcard-Zertifikat *.meineschule.de
+   SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+   SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+   #SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
+
+   ProxyPreserveHost on
+   RewriteEngine On
+   # RewriteLog /var/log/apache2/rewrite.log
+   # RewriteLogLevel 2
+
+   RewriteRule ^(.*)$ https://192.168.1.38$1 [P]
+   # Alternativ kann auch verwendet werden:
+   # RewriteRule ^(.*)$ https://192.168.1.38:8443$1 [P]
+ </VirtualHost>

```

```

+  ##----- Kollegium -----
+  ##----- Aufruf: https://kollegium.meineschule.de
+  <VirtualHost *:443>
+    ServerName kollegium.meineschule.de:443
+
+    SSLEngine on
+    SSLProxyEngine on
+
+    # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+    # Sicherheitseinstellungen, 25.04.2015
+    SSLProtocol all -SSLv2 -SSLv3
+    SSLHonorCipherOrder on
+    SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                  !EXP:!kEDH:!PSK:!SRP:!kECDH'          (eine Zeile)
+    SSLProxyProtocol all -SSLv2 -SSLv3
+    SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                       !EXP:!kEDH:!PSK:!SRP:!kECDH'    (eine Zeile)
+
+    CustomLog /var/log/apache2/ssl_request_log    ssl_combined
+
+    ## Wildcard-Zertifikat *.meineschule.de
+    SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+    SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+    #SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
+
+    RewriteEngine On
+    ## RewriteLog /var/log/apache2/rewrite.log
+    ## RewriteLogLevel 2
+
+    RewriteRule ([^/]*)(.*) https://server.meineschule.de/intranet/kollegium$2
+  </VirtualHost>
+</IfDefine>
+</IfDefine>

```

Falls *vhost-ssl.conf* auf einem Windows-System editiert wurde, so müssen Sie an der Serverkonsole noch den folgenden Befehl ausführen: `dos2unix /etc/apache2/vhosts.d/vhost-ssl.conf`

Um die Weiterleitung auf die weiteren Server (vibe, filr usw.) zu ermöglichen, müssen Sie noch in */etc/sysconfig/apache2* in der Zeile *APACHE_MODULES* den Eintrag *proxy_http* am Zeilenende einfügen und über *rcapache2 restart* den Dienst neu starten.

Die erscheinenden Warnungen „module rewrite_module is already loaded“ können vernachlässigt werden.

5.1.1. Erweiterungsmöglichkeit

Der in dieser Anleitung beschriebene Zugangsweg über den Proxy des Apache auf dem GServer03 erlaubt einfach zu realisierende Erweiterungen. Dies soll an einem Beispiel erläutert werden.

Ersetzen Sie *meineschule.de* jeweils wieder durch den echten Domainnamen Ihrer Schule.

Nehmen wir an, Sie haben eine Wetterstation auf Basis von Raspberry Pi entwickelt und möchten diese natürlich komfortabel aus dem Internet erreichen, am besten über *wetter.meineschule.de*.

Lösung: Plazieren Sie den Raspberry Pi in der DMZ und geben ihm eine Adresse aus dem DMZ-Bereich, z.B. 192.168.1.241. Nun müssen Sie noch in *vhost-ssl.conf* einen neuen virtuellen Host eintragen:

```
+ ##----- wetter -----
+ ##----- Aufruf: https://wetter.meineschule.de
+ <VirtualHost *:443>
+   ServerName wetter.meineschule.de:443
+
+   SSLEngine on
+   SSLProxyEngine on
+
+   # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+   # Sicherheitseinstellungen, 25.04.2015
+   SSLProtocol all -SSLv2 -SSLv3
+   SSLHonorCipherOrder on
+   SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                   !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+   SSLProxyProtocol all -SSLv2 -SSLv3
+   SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                       !EXP:!kEDH:!PSK:!SRP:!kECDH'       (eine Zeile)
+
+   CustomLog /var/log/apache2/ssl_request_log    ssl_combined
+
+   ## Wildcard-Zertifikat *.meineschule.de
+   SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+   SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+
+   ProxyPreserveHost on
+   RewriteEngine On
+   # RewriteLog /var/log/apache2/rewrite.log
+   # RewriteLogLevel 2
+
+   RewriteRule ^(.*)$ http://192.168.1.241$1 [P]
+ </VirtualHost>
```

Beachten Sie, dass hier bei der Rewrite-Regel die Weiterleitung mit http und nicht mit https erfolgt. Details hierzu finden Sie bei den Hintergrund-Informationen.

Wenn Sie die Wetterstation auch aus dem Intranet mit *wetter.meineschule.de* erreichen möchten, so müssen Sie für Wetter noch einen Eintrag in der DNS-Zonendatei machen, so wie dies im Kapitel 3.1 beschrieben ist.

Wenn für Ihre Domain beim Provider ein Wildcard-DNS-Rekord eingerichtet ist (siehe Kapitel 3), dann ist nach dem Neustart des Apache *wetter.meineschule.de* ohne Änderung beim Provider weltweit erreichbar.

Wenn Sie in der DMZ einen eigenen Webserver betreiben, so können Sie diesen ebenso einrichten. Im Beispiel soll der Webserver mit der IP 192.168.1.3 über *web.meineschule.de* erreicht werden. Sie müssen hierfür in *vhost-ssl.conf* einen weiteren virtuellen Host eintragen:

```
+ ##----- webserver -----
+ ##----- Aufruf: https://web.meineschule.de
+ <VirtualHost *:443>
+   ServerName web.meineschule.de:443
+
+   SSLEngine on
+   SSLProxyEngine on
+
+   # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+   # Sicherheitseinstellungen, 25.04.2015
+   SSLProtocol all -SSLv2 -SSLv3
+   SSLHonorCipherOrder on
+   SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                   !EXP:!kEDH:!PSK:!SRP:!kECDH'           (eine Zeile)
+   SSLProxyProtocol all -SSLv2 -SSLv3
+   SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
+                       !EXP:!kEDH:!PSK:!SRP:!kECDH'       (eine Zeile)
+
+   CustomLog /var/log/apache2/ssl_request_log    ssl_combined
+
+   ## Wildcard-Zertifikat *.meineschule.de
+   SSLCertificateFile /etc/ssl/servercerts/servercert.pem
+   SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem
+
+   ProxyPreserveHost on
+   RewriteEngine On
+   # RewriteLog /var/log/apache2/rewrite.log
+   # RewriteLogLevel 2
+
+   RewriteRule ^(.*)$ https://192.168.1.3$1 [P]
+ </VirtualHost>
```

Für den Zugriff von innen ist noch ein Eintrag in der DNS-Zonendatei erforderlich.

5.1.2. Hintergrund-Informationen

Bei der in der Anleitung beschriebenen Methode mit Apache Proxies kommunizieren Nutzer ausschließlich mit dem GServer03. Die tatsächliche Adresse des über den Proxy angesprochenen Servers bleibt dem Nutzer verborgen. Anders als bei einer Weiterleitung, bei der dem Browser des Nutzers die Weiterleitungsadresse bekannt gegeben wird und die Kommunikation anschließend über diese Adresse erfolgt.

Die Verschlüsselung der Daten erfolgt auf dem Gserver03 mit dem eingerichteten Wildcard-Zertifikat. Dieses Zertifikat bekommen die Nutzer zu sehen. Es besteht also eine https-gesicherte Verbindung zwischen dem Nutzer und dem Gserver03.

Wie geht es mit den Daten nun weiter zu den vom Proxy angesprochenen Servern?

Dies soll am Beispiel von *vibe* erläutert werden.

Fragt ein Nutzer *vibe.meineschule.de* an, so werden die ein- und ausgehenden Daten am Gserver03 ent- bzw. verschlüsselt. Mit der Rewrite-Regel `RewriteRule ^(.*)$ https://192.168.1.36/$1 [P]` werden vom Proxy Daten zu 192.168.1.36 geleitet oder von dort geholt. Die Verbindung vom GServer03 zum KServer erfolgt wieder verschlüsselt, wie man am *https* in der Rewrite-Regel erkennen kann. Für die Kommunikation zwischen den beiden Servern werden die Daten nun mit dem selbstsignierten Zertifikat im KServer verschlüsselt. Da diese Kommunikation nur über die DMZ zwischen den Servern abläuft, ist dies sicherheitstechnisch unkritisch.

Betrachten wir nun den im vorigen Kapitel *Erweiterungsmöglichkeiten* beschriebenen Proxy für *wetter.meinschule.de*.

Hier lautet die Rewrite-Regel `RewriteRule ^(.*)$ http://192.168.1.241$1 [P]`

Wieder wird der Datenverkehr mit dem Nutzer am GServer03 ver- bzw. entschlüsselt. Vom Gserver03 zum Raspberry Pi auf 192.168.1.241 erfolgt die Kommunikation unverschlüsselt über *http*, was wiederum kein Risiko darstellt, da die Kommunikation zwischen den Servern intern über die DMZ erfolgt.

Der Vorteil ist nun, dass der Raspberry Pi mit seinen beschränkten Ressourcen keine https-Verschlüsselung ausführen muss und keine Zertifikatsinfrastruktur benötigt. Trotzdem erfolgt die Kommunikation mit dem Nutzer abgesichert über *https*.

5.2. HTTPS-Umlenkung einrichten *

Wie an der Einrichtung der virtuellen Hosts (Proxies) am Port 443 zu erkennen ist, wirken diese zunächst nur bei einem Aufruf über *https*, z.B. *https://filr.meineschule.de*. Der Aufruf *http://filr.meineschule.de* würde fehlschlagen.

Nun kann aber über eine Rewrite-Regel in der Datei */etc/apache2/conf.d/userdir.conf* eine Umlenkung eingerichtet werden, die *http*-Anfragen automatisch in *https*-Anfragen umwandelt.

Beispielsweise *http://filr.meineschule.de* in *https://filr.meineschule.de* usw.

Die so umgewandelten Anfragen werden nun von den Proxies weiterverarbeitet. Ein zusätzlicher Vorteil ist der Komfort für den Nutzer. Da Browser in der Regel automatisch *http* als Protokoll anfügen, wenn in der URL kein Protokoll angegeben wird, kann z.B. Filr nun besonders bequem aufgerufen werden mit *filr.meineschule.de* usw.

Erstellen Sie zunächst von der Originaldatei eine Sicherungskopie.

An der Serverkonsole: Wechseln Sie zunächst in das Verzeichnis */etc/apache2/conf.d*
`gserver03:/etc/apache2/conf.d #cp -a userdir.conf userdir.conf.original`

Kopieren Sie die Datei *userdir.conf* aus dem Download nach *etc/apache2/conf.d/userdir.conf*. Anpassungen in dieser Datei sind nicht erforderlich. Falls Sie in Ihrer ursprünglichen *userdir.conf* bereits eigene Änderungen vorgenommen haben, so müssen Sie diese noch von der gesicherten Originaldatei in die neue Datei übertragen. Prüfen Sie, ob Ihre früheren Änderungen mit den Änderungen dieser Anleitung verträglich sind.

Im Folgenden wird der Inhalt der Datei abgebildet.

- Vorhandene Zeilen, die nicht mehr gebraucht bzw. durch andere Einträge ersetzt werden, sind durch ein - gekennzeichnet und werden mit ### auskommentiert (das - ist natürlich nicht mit einzugeben). Diese Zeilen können auch gelöscht werden.
- Neu hinzugekommene Zeilen werden durch + gekennzeichnet (das + ist natürlich nicht mit einzugeben).
- Kommentierungen der Änderungen erfolgen durch ##.
- Geänderte Zeilen erscheinen im Fettdruck.

```
# Die naechsten 3 Abschnitte ermoeeglichen die Benutzung des public_html
# Verzeichnisses (Tool: userDir (Uli Frei)). 19/23.7.2006
# (aus httpd.conf nachhier verlagert; 5.5.2010)
<Directory "/media/nss/DOCS/">
    Options Indexes MultiViews
    AllowOverride All
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>

# Die folgenden beiden Moduln sind bereits ueber Yast/Network Services/HTTP Server
# eingeschaltet. Andernfalls muessen die Komentarzeichen entfernt werden. 26.04.2015
# LoadModule proxy_connect_module /usr/lib64/apache2/mod_proxy_connect.so
# LoadModule rewrite_module /usr/lib64/apache2/mod_rewrite.so

RewriteEngine on
SSLProxyEngine on

#RewriteLog /home/wwwrun/debug.log
#RewriteLogLevel 2

<Proxy *>
    AddDefaultCharset off
    Order deny,allow
    #Deny from all
    Allow from all
</Proxy>

+ ## Modifikations ZEN-Novell Landesmedienzentrum Baden-Wuerttemberg
+ ## 22.02.2014 / Ulrich Frei

+ ### NSS-Pfade koennen nicht als Pfad zur Redirect-Datei verwendet werden,
```

```
+ ### da NSS-Volumes zur Startzeit von apache2 nicht bereit stehen.  
+ ### RewriteMap MapHome txt:/srv/www/htdocs/userdir/redirect_map.txt  
+ ### RewriteRule ~(?:/*)\/(.*) ${MapHome:$1}$2  
+ ## Hier nicht mehr erforderlich, da HTTPS-Umlenkung erfolgt und die  
+ ## Regel nun in vhost-ssl.conf eingetragen ist.  
  
+ ## Keine Umlenkung auf https fuer WPAD (3.5.2015)  
+ RewriteCond %{REQUEST_URI} !wpad\.dat$  
+ ## gesamten Verkehr auf https umlenken  
+ RewriteCond %{HTTPS} !=on  
+ ## aber nur, wenn es sich nicht bereits um eine HTTPS-Anfrage handelt  
+ RewriteRule ^/?(.*?) https://%{SERVER_NAME}/$1 [R,L]
```

Falls *userdir.conf* auf einem Windows-System editiert wurde, so müssen Sie an der Serverkonsole noch den folgenden Befehl ausführen: `dos2unix /etc/apache2/conf.d/userdir.conf`
Starten Sie nach Abschluss Apache neu mit `rcapache2 restart` an der Konsole des GServer03.

6. Fazit

Mit dem hier beschriebenen Verfahren über Apache Proxies auf dem GServer03 steht für die paedML Novell ein zeitgemäßer, sicherer und nutzerfreundlicher Zugang für Webdienste zur Verfügung. Der erforderliche Einrichtungsaufwand ist vergleichsweise gering und außerdem sehr einfach erweiterbar, wenn weitere Webdienste hinzugenommen werden sollen.

Dieses Verfahren wird ab der kommenden Version 4 der paedML Novell bereits eingerichtet sein und dort als Standardkommunikations-Verfahren empfohlen.

(Sie müssen dort dann lediglich noch das eigene Zertifikat einrichten.)

7. Anhang

7.1. Einsatzmöglichkeit der neuen vhost-ssl.conf

Auch wenn Sie Filr und Vibe über separate öffentliche IP-Adressen betreiben und dafür eventuell auch schon Einzelzertifikate erworben haben, können Sie die geänderte vhost-ssl.conf auf dem GServer03 einsetzen. Sie haben dann auf jeden Fall für die Kommunikation mit dem GServer03 die aktuellen Sicherheits-Einstellungen eingerichtet. Die eingerichteten Proxies werden dann eben nicht genutzt.

Wenn Sie die neue vhost-ssl.conf nicht einsetzen wollen, so empfehlen wir aus Sicherheitsgründen auf jeden Fall im default-host die Protokoll- und Ciphersuite-Zeilen anzupassen.

7.2. Selbstsigniertes Wildcard-Zertifikat erstellen

Hinweis:

Wenn Sie im Moment noch kein vertrauenswürdiges Wildcard-Zertifikat besitzen oder beschaffen können, so können Sie die in diesem Dokument beschriebene Zugangsweise trotzdem realisieren. Dazu können Sie ein selbstsigniertes Wildcard-Zertifikat erstellen und ebenso wie ein gekauftes vertrauenswürdigen Zertifikat einbinden. Die Nutzer Ihrer Seiten erhalten dann im Browser weiterhin eine Zertifikatswarnung. Das ist nicht nur unbequem, sondern auch unsicher. **Ziel sollte deshalb auf jeden Fall die Beschaffung eines vertrauenswürdigen Zertifikats sein.** Sie müssen dann nur noch das selbstsignierte Zertifikat gegen das vertrauenswürdige Zertifikat austauschen. Nur mit einem vertrauenswürdigen Zertifikat kommt aus datenschutzrechtlicher Sicht eine sichere Kommunikation zustande (siehe http://lehrerfortbildung-bw.de/netz/it-infrastruktur/3_dienste/).

Hier wird nun beschrieben, wie Sie ein selbstzertifiziertes Zertifikat erstellen können. Wir arbeiten an der Konsole oder in einem Terminalfenster (z.B. PuTTY). Wechseln Sie in das Verzeichnis `/root` und legen Sie dort ein Unterverzeichnis namens `selfsigned` an.

An der Serverkonsole:

Prüfen Sie mit `date` zunächst das Datum Ihres Servers und stellen Sie es gegebenenfalls korrekt ein. Das augenblickliche Serverdatum wird nämlich das Datum für den Gültigkeitsbeginn des Zertifikats.

```
cd /root
mkdir selfsigned
cd selfsigned

openssl req -nodes -x509 -days 1095 -newkey rsa:2048 -out /
selfsigned.cert -keyout selfsigned.key
```

(alles eine Zeile, ohne den Backslash!)

Es erscheint eine Ausgabe, in der Sie nun eine Menge eingeben müssen:

```
Country Name          DE
State orProvince Name Baden-Wuerttemberg
Locality Name         <MeineStadt>
Organization Name     <Meine-Schule>
```

Organizational Unit Name	< z.B. EDV >
Common Name	*.meineschule.de
Email Address	<edv>@meineschule.de

Hinweis: keine Umlaute, keine Sonderzeichen.

Im Feld *Common Name* wird der Domainname eingetragen, für den das Zertifikat erstellt werden soll.

Ersetzen Sie alle Angaben jeweils durch die für Ihre Schuldmain gültigen Bezeichnungen.

Wenn Sie keine eigene Firstlevel-Domain besitzen, sondern für Ihre Schule nur eine Subdomain bei Belwü eingerichtet ist, wie z.B. *meineschule.meinort.schule.de*, so müssen Sie ***.meineschule.de** durch ***.meineschule.meinort.schule.de** ersetzen.

Im Ordner *selfsigned* werden die beiden Dateien *selfsigned.key* und *selfsigned.cert* erzeugt.

Wechseln Sie nun in das Zertifikatsverzeichnis des Servers:

```
cd /etc/ssl/servercerts
```

Erstellen Sie eine Sicherungskopie der aktuellen Zertifikate:

```
cp serverkey.pem serverkey.pem.original  
cp servercert.pem servercert.pem.original
```

Kopieren Sie nun die zuvor erzeugten Dateien:

```
cp /root/selfsigned/selfsigned.key serverkey.pem  
cp /root/selfsigned/selfsigned.cert servercert.pem
```

Beachten Sie bitte, dass hier kein Zwischenzertifikat erstellt wird und die Zeilen mit *servercabundle.pem* in *vhost-ssl.conf* auskommentiert werden müssen.

Starten Sie Apache neu:

```
rcapache2 restart
```

Sie können die anderen Schritte der Anleitung genauso umsetzen, wie wenn Sie ein vertrauenswürdigen Zertifikat erworben hätten.

8. Änderungen gegenüber der Anleitung vom 17.06.2014

Wenn Sie die Anleitung vom 17.06.2014 bereits umgesetzt haben, so müssen Sie in Ihrer `vhost-ssl.conf` und in `userdir.conf` aus Sicherheitsgründen einige Änderungen vornehmen. Diese Änderungen sind auch erforderlich, um die Kommunikation mit dem neuen *Vibe 4.0* und *Filr 1.2* zu ermöglichen.

Editieren Sie die Datei `/etc/apache2/vhost.d/vhost-ssl.conf`.

Führen Sie im Abschnitt `<VirtualHost *:443>` folgende Änderungen durch.

Kommentieren Sie die mit – gekennzeichnete Zeile aus und fügen Sie die mit + gekennzeichneten Zeilen ein.

```

...
# folgende drei Zeilen ersetzt (A. Wackler), 25.04.2015:
- # SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
+ SSLProtocol all -SSLv2 -SSLv3
+ SSLHonorCipherOrder on
+ SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: /
                    !EXP:!kEDH:!PSK:!SRP:!kECDH'          (eine Zeile)
+ SSLProxyProtocol all -SSLv2 -SSLv3
+ SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: /
                    !EXP:!kEDH:!PSK:!SRP:!kECDH'+        (eine Zeile)
...

```

Tragen Sie in allen virtuellen Hosts die mit + gekennzeichneten Zeilen ein:

```

...
SSLProxyEngine on

+ # Geaenderte Ciphersuite wegen erhoelter Anforderungen an
+ # Sicherheitseinstellungen, 25.04.2015
+ SSLProtocol all -SSLv2 -SSLv3
+ SSLHonorCipherOrder on
+ SSLCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
                    !EXP:!kEDH:!PSK:!SRP:!kECDH'          (eine Zeile)
+ SSLProxyProtocol all -SSLv2 -SSLv3
+ SSLProxyCipherSuite 'AESGCM:RC4:SHA384:SHA256:AES!aNULL:!eNULL:!LOW:!3DES:!MD5: \
                    !EXP:!kEDH:!PSK:!SRP:!kECDH'          (eine Zeile)

CustomLog /var/log/apache2/ssl_request_log    ssl_combined
...

```

Sie können die genannten Zeilen auch durch Kopie aus der zum Download bereitgestellten `vhost-ssl.conf` übernehmen.

Auch in der Datei `/etc/apache2/conf.d/userdir.conf` wurden Änderungen vorgenommen.

*Führen Sie die Änderungen durch, wie in Kapitel 5.2 *HTTPS-Umlenkung einrichten* beschrieben oder verwenden Sie die zum Download bereitgestellte Datei `userdir.conf`.*

Starten Sie Apache neu:

```
rcapache2 restart
```

Viel Erfolg wünscht Ihnen
Ihre ZEN-Novell.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2015