

Beratung und Support  
Technische Plattform  
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

# Anleitung

Gesicherter Zugriff von außen  
( meineschule.de anpassen )

Stand 17.01.2017

paedML® Novell

Version: 4+

## **Impressum**

### **Herausgeber**

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

### **Autoren**

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

Hubert Bechthold  
Holger Dzeik  
Stefan Falk  
Ulrich Frei  
Carl-Heinz Gutjahr  
Friedrich Heckmann  
Uwe Labs  
Alfred Wackler

### **Endredaktion**

ZEN-Novell

### **Bildnachweis Titelbilder:**

Thinkstock

### **Weitere Informationen**

[www.support-netz.de](http://www.support-netz.de)  
[www.lmz-bw.de](http://www.lmz-bw.de)

Veröffentlicht: 2017

© Landesmedienzentrum Baden-Württemberg

# Inhaltsverzeichnis

<b>1.</b>	<b>Beschreibung des Verfahrens.....</b>	<b>3</b>
<b>2.</b>	<b>Anleitung .....</b>	<b>4</b>
2.1	Zertifikatsbeschaffung.....	4
2.2	Anpassung der Sophos-Firewall.....	5
2.3	Wildcard-Eintrag beim Provider (Belwü).....	5
2.4	Anpassung auf dem GServer03 .....	6
2.4.1	vhosts-ssl.conf .....	6
2.4.2	Nameserver auf GServer03 anpassen .....	7
2.4.3	webacc.....	8
<b>3.</b>	<b>Erweiterungen.....</b>	<b>9</b>
<b>4.</b>	<b>Anhang .....</b>	<b>9</b>
4.1	Andere Zugriffsmöglichkeiten von außen (schematisch).....	9

# Vorwort

Im August 2015 wurde im Dokument „*Zertifikate-Anleitung*“ ein Weg beschrieben, wie ein gesicherter Zugang auf das Schulnetz mit Groupwise, Filr, Vibe, Intranet usw. mit benutzerfreundlichen URLs über eine öffentliche IP-Adresse und abgesichert mit einem Wildcard-Zertifikat auf dem GServer03 eingerichtet werden kann. Der Zugang erfolgt dabei für alle Dienste über den GServer03. Für jeden Dienst wird dabei für den Apache ein virtueller Host als Proxy eingerichtet.

Dies ermöglicht einerseits den Zugang zu den Diensten mit benutzerfreundlichen URLs, wie z.B. mail.meineschule.de, filr.meineschule.de und so weiter. Andererseits erleichtert es die Einrichtung für die Schule, da nur auf dem GServer03 ein Zertifikat eingerichtet und gepflegt werden muss.

Ab der paedML Novell 4.1 ist nun die für dieses Verfahren erforderliche Einrichtung weitgehend vorkonfiguriert, es muss nur noch der in der Auslieferung verwendete fiktive Domainname *meineschule.de* durch den echten Domainnamen der Schule ausgetauscht und das eigene Zertifikat eingepflegt werden.

Diese Zugriffsart können Sie auch dann nutzen, wenn Sie noch kein eigenes vertrauenswürdiges Zertifikat besitzen. Dann erfolgt die Verschlüsselung mit den vom System generierten selbstsignierten Zertifikaten. Benutzer erhalten dann aber im Browser eine Zertifikatswarnung. Sinnvoller ist es also, dass Sie sich für die Domain Ihrer Schule ein sogenanntes vertrauenswürdiges Zertifikat beschaffen. Dies ist unbedingt erforderlich, wenn Sie über mobile Geräte zugreifen wollen, da diese meist keine selbstsignierten Zertifikate akzeptieren. Außerdem haben wir als Schule auch einen Erziehungsauftrag und sollten insbesondere in dem immer wichtiger werdenden Bereich der Computersicherheit kein schlechtes Vorbild geben.

Im Text wird an einigen Stellen auf bereits veröffentlichte Dokumente verwiesen.  
Hier die Links zu den Seiten mit den angesprochenen Dokumenten:

*Zertifikate-Anleitung*:

<http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/novell/erweiterungen/wildcard-zertifikate-in-der-paedmlr-novell-334.html>

*Zertifikate2-BPZ-Novell-334* und *paedML-Novell-334-Zertifikate*:

<http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/novell/erweiterungen/zertifikate-in-der-paedml-novell-334.html>

Hinweis:

Auszuführende Arbeiten sind im Text durch eine auf der linken Seite angeordnete Linie gekennzeichnet.

Bereiche ohne diese Linie dienen der Erläuterung.

# 1. Beschreibung des Verfahrens

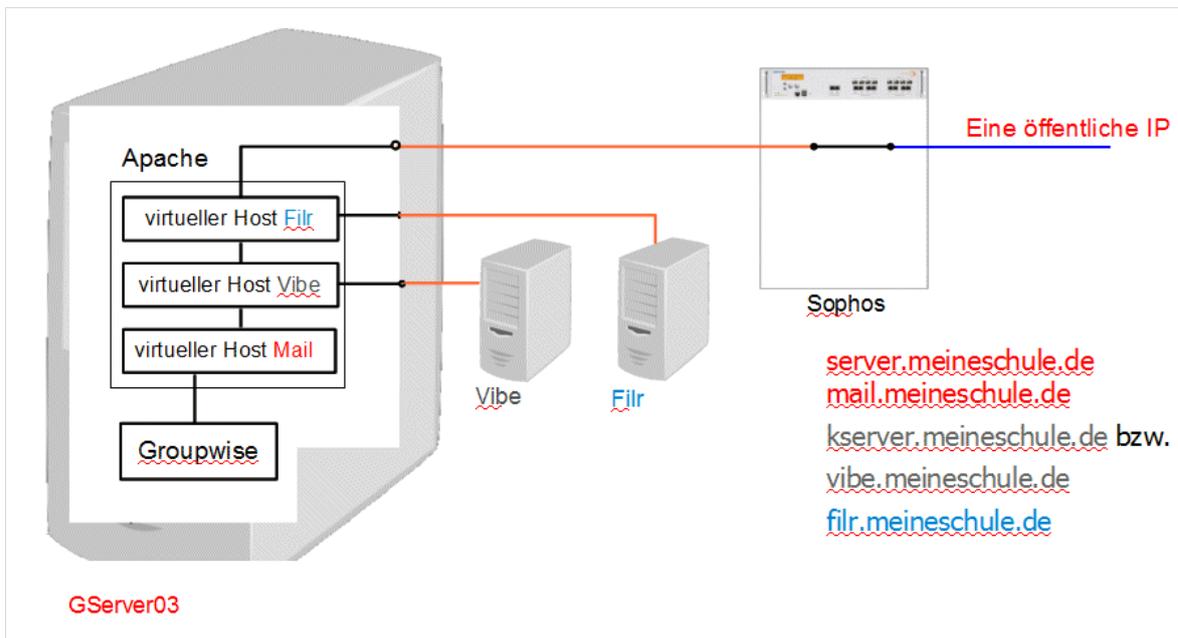


Abb. 1: Zugriffsprinzip über Proxys

Der Zugriff auf die verschiedenen Server und Dienste erfolgt über virtuelle Hosts für Apache auf dem GServer03, die als Proxys dienen. Für eine detaillierte Beschreibung dieses Verfahrens und auch der in der paedML Novell ab Version 4.1 auch weiterhin möglichen anderen Zugriffsmethoden verweisen wir auf das Dokument „Zertifikate-Anleitung.pdf“. Im Anhang finden Sie dazu auch einen kurzen Überblick in Form zweier Diagramme.

Vorteile der Proxy-Methode:

- Zertifikat nur für GServer03 erforderlich (Wildcard-Zertifikat).  
Nur für den GServer03 ist Arbeit bei Einrichtung und Zertifikatsverlängerung erforderlich.
- Beim Provider ist nur ein DNS-Wildcard-Eintrag erforderlich
- Bei Einrichtung zusätzlicher Server oder Dienste keine Änderung an der Firewall und beim Provider erforderlich.
- Nur ein Server ist im Internet exponiert (geschützt durch die Sophos-Firewall):  
Eventuell auftretende Sicherheitslücken können so schneller geschlossen werden.
- HTTPS-Umlenkung einfach umsetzbar. Sicherheits-Zugewinn.

## 2. Anleitung

### 2.1 Zertifikatsbeschaffung

Es ist ein sogenanntes Wildcard-Zertifikat für die schulische Domain erforderlich, im Beispiel \*.meineschule.de. Dieses Zertifikat sichert dann z.B. server.meineschule.de, filr.meineschule.de ab. (Nicht jedoch nocheinserver.subdomain.meineschule.de. „Wildcard“ gilt genau für eine Stufe.)

Zur Zertifikatsbeschaffung verweisen wir auf das Dokument „Zertifikate2-BPZ-Novell-334“.

In der paedML Novell 4.1+ werden die vom System bei der Installation generierten selbstsignierten Zertifikatsdateien *servercert.pem*, *servercabundle.pem* und *serverkey.pem* in *etc/ssl/servercerts* vom System automatisch wieder hergestellt. Wenn Sie also Ihre eigenen Zertifikatsdateien so wie die oben genannten Dateien benennen würden, so wie dies in den älteren Anleitungen beschrieben wurde, dann würden diese Dateien automatisch wieder durch die vom System erzeugten Dateien ersetzt.

**Folgen Sie deshalb bei Pfad- und Dateinamen der Zertifikatsdateien den Angaben in dieser Anleitung.**

Sie erhalten vom Lieferanten Ihr Zertifikat entweder in Form von Dateien oder als Text im Mailanhang. Beachten Sie dazu die Hinweise Ihres Lieferanten.

Im Beispiel erhalten Sie die Dateien ( wobei bei Ihnen statt *mydomain* vermutlich der echte Domainname Ihrer Schule steht).

*\*.mydomain.crt*

Die eigentliche Zertifikatsdatei

*intermediate.crt*

Das Zwischenzertifikat (nicht unbedingt dabei),

außerdem haben Sie noch den privaten Schlüssel, den Sie vor der Zertifikatsbestellung erzeugt haben.

*\*.mydomain.key*

Kopieren Sie die oben genannten Originaldateien auf den Server an einen sicheren Ort.  
Vorschlag */etc/ssl/servercerts/<Schulkürzel>*

Wechseln Sie an der Kommandozeile des GServer03 in den Ordner */etc/ssl/servercerts*  
Erstellen Sie hier einen Ordner mit dem Namen *<Schulkürzel>*

```
md <Schulkürzel>
```

Kopieren Sie die oben genannten Originaldateien in diesen neu erstellten Ordner.

Führen Sie nun am Serverprompt *gserver03:/etc/ssl/servercerts #* die folgenden Kopieraktionen aus:

```
cp <Schulkürzel>/*.mydomain.crt servercert-<Schulkürzel>.pem
cp <Schulkürzel>/intermediate.crt servercabundle-<Schulkürzel>.pem
cp <Schulkürzel>/*.mydomain.key serverkey-<Schulkürzel>.pem
```

Ersetzen Sie dabei die Namen der Quelldateien durch die Namen Ihrer Original-Dateien sowie *<Schulkürzel>* durch Ihr eigenes Schulkürzel (ohne *<>*).

Damit ist die Bereitstellung abgeschlossen.

Für die Verwendung werden die Namen der Kopien in einem späteren Schritt in die *vhost-ssl.conf* eingetragen.

## 2.2 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 virtuellen Hosts als Proxys auf dem Gserver03 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 Proxys auf dem GServer03 erreichen. Eine Anleitung hierfür finden Sie im Dokument „*Zertifikate-Anleitung*“ in Kapitel 5.1.1. *Proxy-Konfiguration/Erweiterungsmöglichkeiten*.

Melden Sie sich an der Sophos-Firewall <https://10.1.1.30:4444> 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 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 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.

## 2.3 Wildcard-Eintrag beim Provider (Belwü)

Lassen Sie bei Ihrem Provider (meist Belwü) einen Wildcard-DNS-Record \*. *meineschule.de* mit der **öffentlichen IP-Adresse Ihrer Firewall** als Zieladresse eintragen.

(Ersetzen Sie auch hier wieder *meineschule.de* durch den echten Domainnamen Ihrer Schule).

Damit werden Anfragen von Außen für *filr, vibe, mail* usw. an Ihren Server weitergeleitet.

Eine Erläuterung zum Thema finden Sie in der Zertifikate-Anleitung „[Gesicherter Zugriff](#)“.

## 2.4 Anpassung auf dem GServer03

### 2.4.1 vhosts-ssl.conf

Wechseln Sie an der Kommandozeile des GServer03 in den Ordner `/etc/apache2/vhosts.d`

Erstellen Sie vor der Bearbeitung eine Sicherheitskopie der Datei `vhost-ssl.conf`.

```
cp -a vhost-ssl.conf vhost-ssl.conf.orig
```

Editieren Sie die Datei `vhost-ssl.conf` mit einem Editor Ihrer Wahl.

Ersetzen Sie in der Datei bei allen virtuellen Hosts im Kommentar und beim Attribut `ServerName` die Domainbezeichnung `meineschule` durch den echten Domainnamen Ihrer Schule.

```
##----- Mail -----  
##----- Aufruf: https://mail.meineschule.de -----  
<VirtualHost *:443>  
    ServerName mail.meineschule.de:443
```

Nun müssen noch die Namen der Zertifikatsdateien angepasst werden.

Suchen Sie in allen virtuellen Hosts (auch in default) die Zeilen

```
SSLCertificateFile /etc/ssl/servercerts/servercert.pem  
SSLCertificateKeyFile /etc/ssl/servercerts/serverkey.pem  
  
#SSLCertificateChainFile /etc/ssl/servercerts/servercabundle.pem
```

ersetzen Sie sie durch

```
SSLCertificateFile /etc/ssl/servercerts/servercert-<Schulkürzel>.pem  
SSLCertificateKeyFile /etc/ssl/servercerts/serverkey-<Schulkürzel>.pem  
  
#SSLCertificateChainFile  
    /etc/ssl/servercerts/servercabundle-<Schulkürzel>.pem
```

Falls Sie von Ihrem Zertifikatslieferanten ein Zwischenzertifikat erhalten haben, so entfernen Sie das Zeichen `#` am Beginn der Zeile `#SSLCertificateChainFile`

Falls Sie noch kein eigenes vertrauenswürdigen Zertifikat besitzen, so belassen sie die Einträge für die Zertifikatsdateien wie sie sind. Sie nutzen dann alle Vorteile der beschriebenen Zugangsweise. Jedoch erhalten Ihre Benutzer im Browser jeweils eine Zertifikatswarnung. Ihr Ziel sollte deshalb unbedingt die Beschaffung eines vertrauenswürdigen Zertifikats für Ihre Schuldomain beschaffen.

Speichern Sie die Datei. Damit sind die Änderungen an der `vhost-ssl.conf` abgeschlossen.

## 2.4.2 Nameserver auf GServer03 anpassen

Um filr, vibe, mail usw. aus dem Intranet mit derselben URL wie von außen aufrufen zu können, müssen im DNS-System des GServer03 Ergänzungen erfolgen.

Editieren Sie die Datei `/etc/named.conf` im abgebildeten Bereich:

```
# Fuer eine Internetanbindung muss meineschule.de durch die echte Domain
# ersetzt werden. Ebenfalls muss dann entsprechend die Datei
# /var/lib/named/master/meineschule.de umbenannt und angepasst werden.

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

Ersetzen Sie hier *meineschule* durch den echten Domainnamen Ihrer Schule.  
Speichern Sie die Datei.

Wechseln Sie an der Serverkonsole in den Ordner `/var/lib/named/master`.  
Benennen Sie die Datei *meineschule.de* um. Ersetzen Sie im Namen wieder *meineschule* durch den echten Domainnamen Ihrer Schule.

```
mv meineschule.de mydomain.de
```

Ersetzen Sie auch hier *meineschule* durch den echten Domainnamen Ihrer Schule.

Editieren Sie die soeben umbenannte Datei:

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

                IN NS      gserver03.oes.ml-bw.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 NS       192.168.1.1 ; Astaro/UTM
```

Ersetzen Sie an den zwei Stellen *meineschule* durch den echten Domainnamen Ihrer Schule.  
Speichern Sie die Datei.

Nun müssen noch die betroffenen Dienste neu gestartet werden:

```
rcnamed restart
rcapache2 restart
```

### 2.4.3 webacc

Editieren Sie die Datei *webacc.cfg* im Verzeichnis */var/opt/novell/groupwise/webaccess*.

Suchen Sie die Zeile

```
#Cookie.domain=.novell.com
```

Tragen Sie darunter die folgende Zeile ein:

```
Cookie.domain=.meineschule.de
```

Ersetzen Sie auch hier wieder *meineschule* durch den echten Domainnamen Ihrer Schule.

Beachten Sie den Punkt vor dem Domainnamen.

Speichern Sie die Datei.

Um den Eintrag zu aktivieren, muss Tomcat neu gestartet werden:

```
rcnovell-tomcat6 restart  
rcapache2 restart
```

**Die Anpassungen am GServer03 sind damit abgeschlossen.**

## 3. Erweiterungen

Wie Sie weitere Server (eigener Webserver in DMZ usw.) bzw. Dienste einbinden können, erfahren Sie im Dokument „Zertifikate-Anleitung“ in Kapitel 5.1.1. *Proxy-Konfiguration/Erweiterungsmöglichkeiten*.

## 4. Anhang

### 4.1 Andere Zugriffsmöglichkeiten von außen (schematisch)

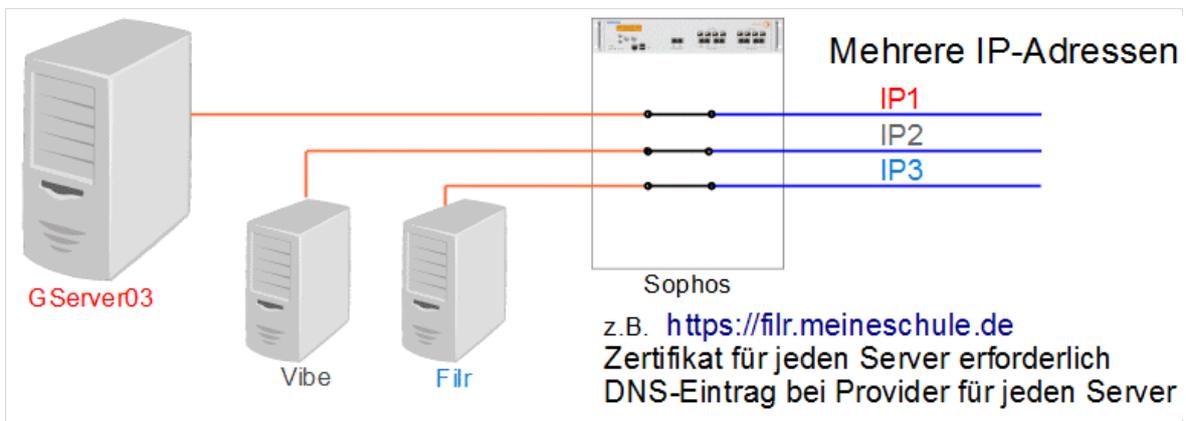


Abb. 2: mehrere IP-Adressen

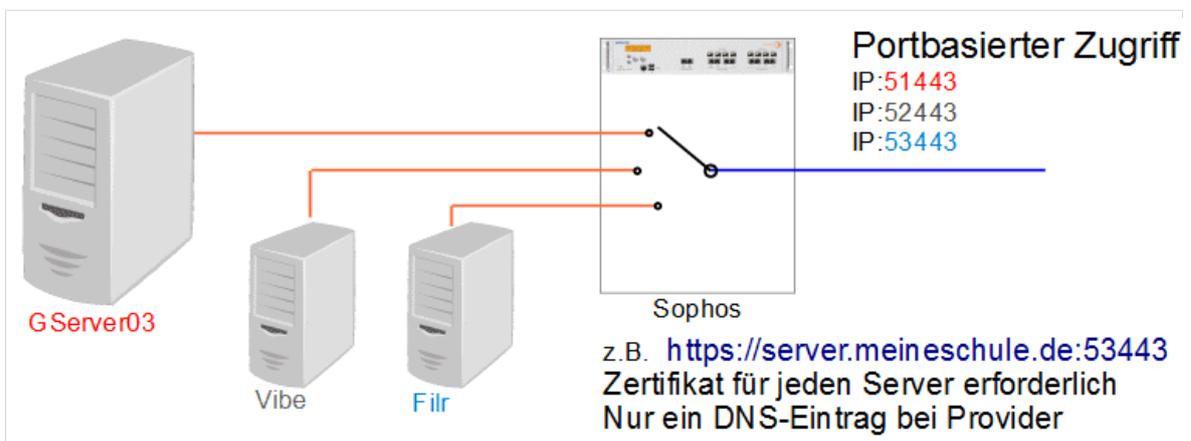


Abb. 3: portbasierter Zugriff

Diese Zugriffsmethoden sind in der paedML Novell auch weiterhin möglich. Es müssen dann in der Sophos-Firewall die entsprechenden Filter und Forwardings eingerichtet werden. Außerdem müssen Sie beim Provider eventuell DNS-Records eintragen lassen.

**Landesmedienzentrum Baden-Württemberg (LMZ)**  
**Support Netz**  
**Rotenbergstraße 111**

**70190 Stuttgart**

© Landesmedienzentrum Baden-Württemberg, 2017