

Beratung und Support  
Technische Plattform  
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

# Installationsanleitung

Installation und Konfiguration eines sicheren Lehrernetzes (aktualisierte Fassung)

Stand 28.07.2016

## paedML® Novell

Version: 3.3.x und 4.1

## **Impressum**

### **Herausgeber**

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

### **Autoren**

der Zentralen Expertengruppe Netze (ZEN),  
Support-Netz, LMZ  
  
Carlheinz Gutjahr  
Alfred Wackler

### **Endredaktion**

Doreen Edel

### **Bildnachweis Titelbilder:**

Thinkstock

### **Weitere Informationen**

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

**Änderungen und Irrtümer vorbehalten.**

Veröffentlicht: 2016

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

## Inhaltsverzeichnis

<b>1.</b>	<b>Konfigurationsdateien auf Servern bearbeiten .....</b>	<b>5</b>
1.1	GServer03.....	5
1.1.1	DHCP einrichten .....	5
1.1.2	DNS einrichten .....	5
1.1.2.1	named.conf .....	5
1.1.2.2	DNS-Zonen-Dateien.....	6
1.1.3	Routing einrichten .....	6
1.2	Zugriff auf Apache2-Verwaltungsinstanz erlauben .....	6
1.2.1	Squid.conf modifizieren.....	7
1.3	ZServer .....	7
1.3.1	Routing konfigurieren .....	7
1.3.2	„settings.txt“ konfigurieren.....	8
<b>2.</b>	<b>Einrichten der Lehrernetz-Zone auf der Sophos-UTM.....</b>	<b>8</b>
2.1	Interface konfigurieren .....	8
2.2	DHCP-Relay ggf. aktivieren und für Lehrernetz konfigurieren .....	9
2.3	DNS für das Lehrernetz konfigurieren .....	10
2.4	TFTP-Helper aktivieren .....	11
2.5	Neue Zone bereitstellen.....	12
2.5.1	Netzwerkdefinitionen für interne Server konfigurieren.....	12
2.5.2	Firewallregeln für Lehrernetz konfigurieren .....	13
<b>3.</b>	<b>Änderungshistorie .....</b>	<b>15</b>
<b>4.</b>	<b>Anhang .....</b>	<b>17</b>
4.1	paedML Novell Netzwerkzonen .....	17

## Vorwort

Im Schreiben vom 6. September 2004, Az. 11-0551.0/34 (sogenannter Netzbrief) hat das Kultusministerium die Rahmenbedingungen für die „Gestaltung von Netzen an Schulen“ formuliert. Darin wurde insbesondere festgelegt, dass zum Schutz personenbezogener Daten „lokale Schulverwaltungsnetze“ von „lokalen pädagogischen Netzen“ getrennt sein müssen.

Laut „Netzbrief“ vom Juni 2014 wird nun ein weiteres, optionales Netz, die „Arbeitsumgebung Lehrkräfte“ (das sogenannte Lehrernetz) thematisiert, das „den Lehrkräften zur Unterrichtsvorbereitung oder zum Sammeln und Gestalten von Unterrichtsmaterial dienen [soll]. Ferner erfolgt in diesem Netz die pädagogische Verwaltung: So können Lehrkräfte dort Bewertungen oder Benotungen von Schülerarbeiten verarbeiten und speichern. ... Diese Daten müssen so gespeichert werden, dass nur dazu Befugte auf die zur Aufgabenerfüllung unbedingt erforderlichen Daten zugreifen können ... Ein Zugriff durch Lehrkräfte vom Lehrernetz aus auf die Unterrichtsumgebung ist zulässig. Jeglicher Schülerzugriff auf das Lehrernetz ist unzulässig. Ein Zugriff vom Klassenzimmer aus auf dieses Netz ist zu verhindern...“

In der Praxis wird also gefordert, dass eine Trennung von „Verwaltungsnetz“, dem neu hinzugekommenen „Lehrernetz“ und dem „pädagogischen Netz“ sichergestellt werden muss. Das Lehrernetz kann als ein Sondernetz zwischen pädagogischem Netz und Schulverwaltungsnetz verstanden werden. Vom Lehrernetz aus darf grundsätzlich auf beide anderen Netze zugegriffen werden, um Daten auszutauschen, auf das Verwaltungsnetz aber nur in der Form, dass „ein geregelter Zugriff in Richtung auf das Schulverwaltungsnetz auf ausgewählte Ressourcen zulässig ... ist, dass keine personenbezogenen Daten vom Schulverwaltungsnetz dabei im Lehrernetz physikalisch abgelegt werden können.“

In dieser Anleitung wird beschrieben, wie in der paedML Novell dieses optionale sichere Lehrernetz eingerichtet werden kann, das den Forderungen des Netzbriefes genügt. Wir bilden das „Lehrernetz“ über unsere Sophos-UTM ab, die zwischen den Netzen so vermittelt, dass Lehrkräfte auf Ihre Ressourcen im Schulnetz zugreifen können, zwischen dem pädagogischen Netz und dem Lehrernetz ansonsten aber eine Trennung besteht.

**Hinweis:** Das Lehrernetz mit dem Feature Imaging über PXE lässt sich nur mit neueren Versionen der Sophos UTM realisieren, weil nur in diesen der für das Imaging benötigte *TFTP-Helper-Service* verfügbar ist. Ein Lehrernetz ohne dieses Feature ist auch mit älteren Versionen vor Sophos UTM 9.1 möglich. Bitte beachten Sie: Das Imaging über die Sophos UTM ist sehr ressourcenintensiv und sollte nur auf wenigen Arbeitsstationen gleichzeitig durchgeführt werden. Die erzielbare Performance ist stark von der verwendeten Hardware (Appliance) oder der der virtuellen Maschine zur Verfügung gestellten Ressourcen abhängig! Für komplexere und anspruchsvollere Konfigurationen, in der ganze Netze segmentiert werden, wäre ein Layer-3-Switch besser geeignet.

# 1. Konfigurationsdateien auf Servern bearbeiten

## 1.1 GServer03

### 1.1.1 DHCP einrichten

Damit für Clients im Lehrernetz IP-Adressen verteilt werden können, erweitern Sie die *dhcpd.conf* in */etc/* um mehrere Einträge:

```
subnet 172.18.0.0 netmask 255.255.0.0 {
    option routers 172.18.0.1;
    option subnet-mask 255.255.0.0;
    option broadcast-address 172.18.255.255;
    option domain-name "lehrernetz.oes.ml-bw.de";
    range 172.18.255.1 172.18.255.250;
    next-server 10.1.1.33;
    filename „nvlntp.sys“;
    # folgende Option evtl. für UEFI benötigt
    # option tftp-server-name „zserver“;
    default-lease-time 8640000;
    max-lease-time 8640000;
}
```

Starten Sie den DHCP-Server mit

```
rcdhcpd restart neu.
```

### 1.1.2 DNS einrichten

#### 1.1.2.1 named.conf

Um DNS-Anfragen auch aus dem Lehrernetz zuzulassen, erweitern Sie in der *named.conf* in */etc* folgende Zeile:

```
allow-query { 127/8;10.1/16;172.16/16;192.168.1/24; };
```

um den Eintrag *172.18/16*; sodass die Zeile wie folgt aussieht:

```
allow-query { 127/8;10.1/16;172.16/16;172.18/16;192.168.1/24; };
```

Um die Zonendateien nutzen zu können, braucht es in der *named.conf* Verweise auf die Dateien. Bitte fügen Sie folgende neuen Zonen der *named.conf* hinzu:

```
zone "168.192.in-addr.arpa" in {
    file "master/168.192.in-addr.arpa";
    type master;
};
zone "lehrernetz.oes.ml-bw.de" in {
    file "master/lehrernetz.oes.ml-bw.de";
    type master;
    allow-transfer { any; };
};
zone "18.172.in-addr.arpa" in {
    file "master/18.172.in-addr.arpa";
    type master;
    allow-transfer { any; };
};
```

### 1.1.2.2 DNS-Zonen-Dateien

Kopieren Sie die Dateien *168.192.in-addr.arpa*, *18.172.in-addr.arpa* und *lehrernetz.oes.ml-bw.de* in das Verzeichnis */var/lib/named/master*. Starten Sie den DNS-Server mit

```
rcnamed restart
```

neu.

### 1.1.3 Routing einrichten

Fügen Sie der Datei *routes* in */etc/sysconfig/network* folgenden Eintrag hinzu und speichern Sie sie ab:

```
172.18.0.0 10.1.1.30 255.255.0.0 eth0
```

Führen Sie

```
rcnetwork restart
```

durch. Der Befehl

```
route -n
```

sollte dann die zusätzliche Route ausgeben und ein Ping auf 172.18.0.1 eine Antwort liefern.

## 1.2 Zugriff auf Apache2-Verwaltungsinstanz erlauben

Fügen Sie in der Datei *default-server.conf* in */etc/paedML\_Novell/httpd\_inet* dem ersten Konfigurationsblock ein *Allow-Statement* hinzu:

```
Allow from 172.18.0.0/16
```

Speichern Sie die Datei ab und führen Sie zum Abschluss

```
rchttpd_inet restart
```

durch.

```
<Directory "/var/lib/inet/htdocs">
  Options None
  AllowOverride None
  Order allow,deny
  Allow from 10.1.0.0/16
  Allow from 172.18.0.0/16    <-----
</Directory>
Allow
```

### 1.2.1 Squid.conf modifizieren

Fügen Sie der Datei *squid.conf* im Verzeichnis */etc/squid/* im folgenden Abschnitt zwei Zeilen hinzu, damit die Rechner aus dem Lehrernetz, den Internet-Proxy benutzen dürfen. Der Abschnitt

```
# Clients aus dem Intranet duerfen Proxy benutzen.
# Alle anderen nicht.
acl ML3lokal src 10.1.10.1-10.1.255.254
http_access deny ML3lokal
deny_info http://10.1.1.32:54080/internet_gesperrt.html ML3lokal
```

muss nach der Änderung dann wie folgt aussehen:

```
# Clients aus dem Intranet und dem Lehrernetz duerfen Proxy benutzen.
# Alle anderen nicht.
acl ML3lokal src 10.1.10.1-10.1.255.254
acl Lehrernetz src 172.18.0.0/16
http_access allow Lehrernetz
http_access deny ML3lokal
deny_info http://10.1.1.32:54080/internet_gesperrt.html ML3lokal
```

Starten die den Squid mit

```
rcsquid restart neu.
```

## 1.3 ZServer

### 1.3.1 Routing konfigurieren

Fügen Sie der Datei *routes* in */etc/sysconfig/network* folgenden Eintrag hinzu und speichern Sie sie ab:

```
172.18.0.0 10.1.1.30 255.255.0.0 eth0
```

Führen Sie

```
rcnetwork restart
```

durch. Der Befehl

```
route -n
```

sollte dann die zusätzliche Route ausgeben und ein Ping auf 178.18.0.1 eine Antwort liefern.

### 1.3.2 „settings.txt“ konfigurieren

Die Datei *settings.txt* im TFTP-Verzeichnis des ZServers kontrolliert die Initialisierung der ZENworks Imaging-Umgebung. Diese Datei ist auf dem ZServer insgesamt zwei Mal vorhanden. Sie liegt unter */srv/tftp/boot* für Booten von einem Legacy Client (Standard-BIOS) und unter */srv/tftp/efi* für UEFI-Client. In der *settings.txt* muss die Variable *PROXYADDR* konfiguriert werden. Weisen Sie der Variablen den Wert *10.1.1.33* zu und entfernen Sie jeweils den Gartenzaun vor der Variablen. Mit *rcnovell-pbserv* werden die neuen Einstellungen aktiv.

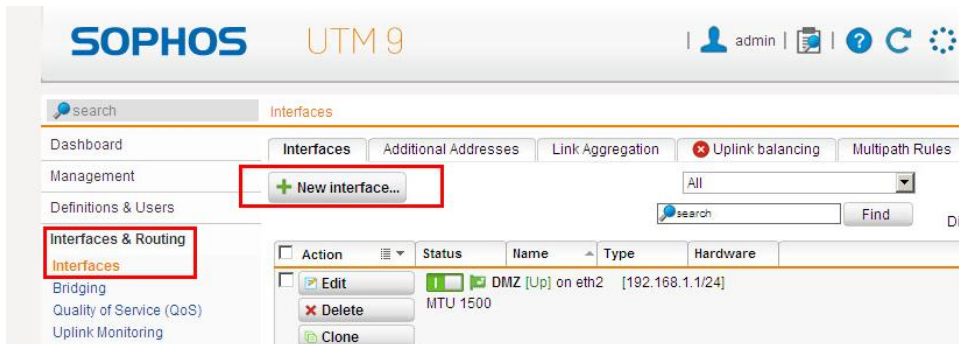
## 2. Einrichten der Lehrernetz-Zone auf der Sophos-UTM

Es gibt die Sophos-UTM in mehreren Ausführungen, als Hardware-Appliance oder als Software-Appliance. Die Umsetzung des Lehrernetzes erfordert mindestens vier Netzwerkkarten, die schon beim kleinsten Sophos-Modell, der SG-105, vorhanden sind. Mit dieser Hardware wäre entweder die vierte Netzwerkkarte für das Lehrernetz vorzusehen, sofern man keine weiteren Netze (Internal-WLAN, Gast-LAN, Gast-WLAN) in Betrieb nehmen möchte oder man behilft sich mit VLANs. Die Belegung der Netzwerk-Interfaces ist im Anhang unter dem Abschnitt „paedML Novell Netzwerkzonen“ dargestellt. Wer die Software-Appliance verwendet, kann sich mit dem „Einbau“ zusätzlicher Netzwerkkarten in die VM und einem dedizierten virtuellen Switch behelfen und diese dann konfigurieren. Im Folgenden wird von einer Software-Appliance ausgegangen. Verfügen Sie über eine Hardware-Appliance mit 8 Netzwerkkarten (Sophos SG 310 und größer), ist die Umsetzung des Lehrernetzes ohne VLANs möglich, bei Hardware-Appliances mit 6 Netzwerkkarten (Sophos SG-210/220) hängt es vom Ausbau der Netzwerkinfrastruktur (Anzahl der zusätzlichen Netze) ab, ob Sie VLANs benötigen. Die Einrichtung von VLANs wird in diesem Dokument nicht beschrieben, wenden Sie sich hierfür an Ihren Händler.

### 2.1 Interface konfigurieren

Loggen Sie sich im Sophos UTM Webinterface als *admin* ein. Wechseln Sie zu *Interfaces & Routing – Interfaces* und klicken Sie auf *New Interface*. In der Maske *Create new interface* geben Sie folgendes ein:





**Create new interface**

Name: Lehrernetz

Type: Ethernet Static

Hardware: eth3 Intel Corporation 825

IPv4 Address: 172.18.0.1

Netmask: /16 (255.255.0.0)

IPv4 Default GW: ☐

Comment: Lehrernetz

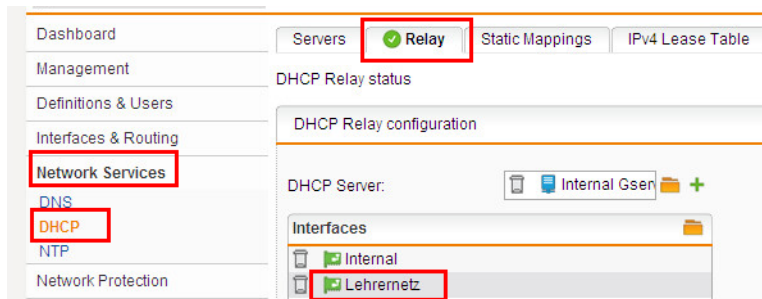
**Advanced**

Speichern Sie die Konfiguration mit **Save** ab und prüfen Sie, ob das Interface *aktiv* ist:

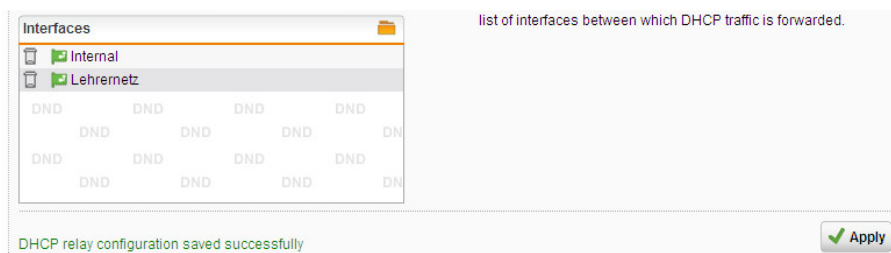


## 2.2 DHCP-Relay ggf. aktivieren und für Lehrernetz konfigurieren

Gehen Sie zu *Network Services – DHCP – Relay* und fügen Sie das *Lehrernetz* dem Relaying hinzu:



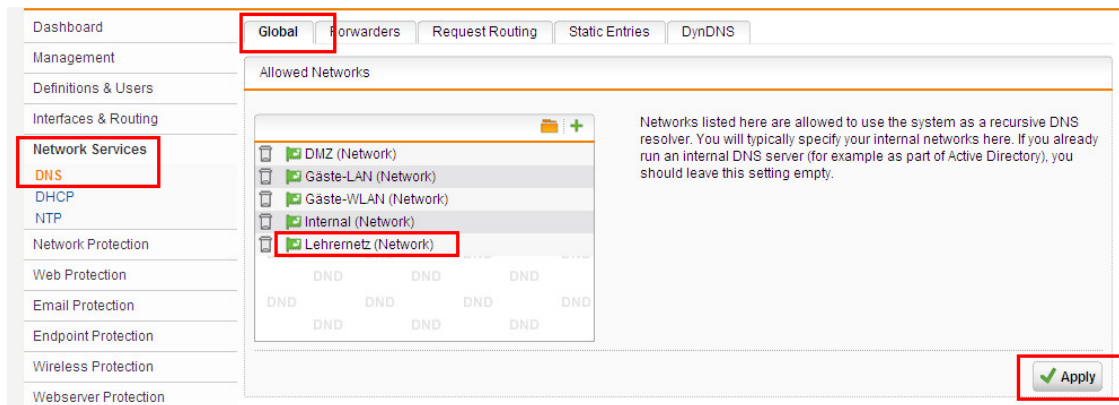
Klicken Sie auf *Apply*, es sollte die Meldung über eine erfolgreiche Speicherung erscheinen.



## 2.3 DNS für das Lehrernetz

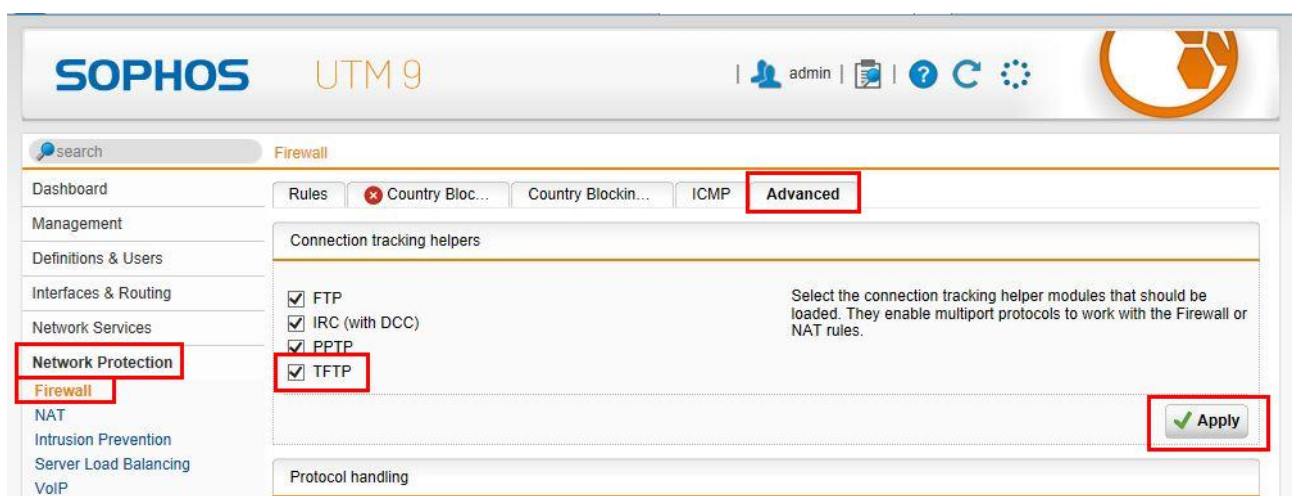
### konfigurieren

Gehen Sie auf *Network Services – DNS – Global* und stellen Sie sicher, dass das Lehrernetz die Sophos als DNS Resolver benutzen darf.



## 2.4 TFTP-Helper aktivieren

Damit im Lehrernetz auch Imaging möglich ist, muss die Unterstützung für TFTP aktiviert werden. Klicken Sie unter *Network Protection – Firewall* auf den Reiter *Advanced* und dann auf *TFTP*. Schließen Sie den Vorgang mit *Apply* ab.



## 2.5 Neue Zone bereitstellen

### 2.5.1 Netzwerkdefinitionen für interne Server konfigurieren

Gehen Sie zu *Definitions & Users – Network Definitions*. Überprüfen Sie, ob es die Netzwerkdefinition *Internal ZServer* gibt. Ggf. müssen Sie die Definition noch anlegen. Klicken Sie auf *New Network*



*Definition* und konfigurieren Sie diese wie folgt: *Type Host, IPv4 Address 10.1.1.33*

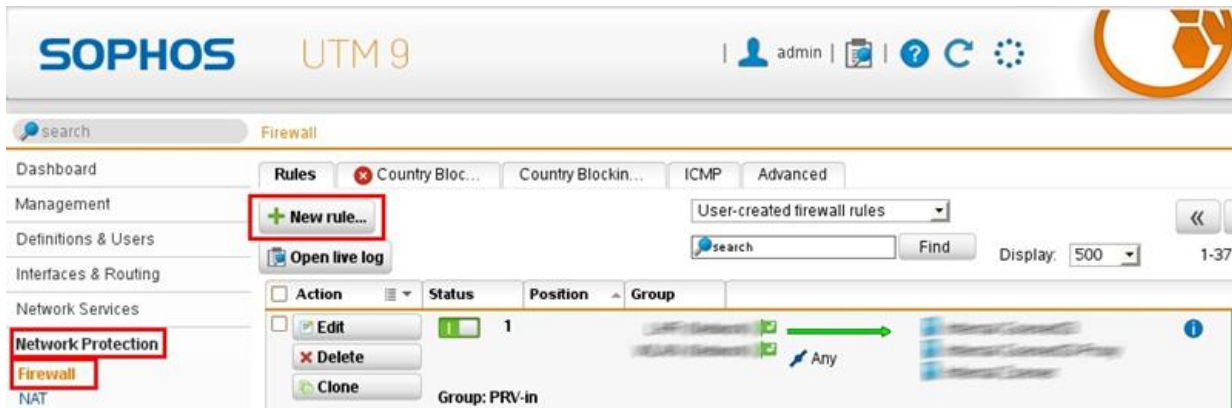
The dialog box 'Create new network definition' contains the following fields and sections:
 

- Name: Internal ZServer
- Type: Host (dropdown menu)
- IPv4 Address: 10.1.1.33
- Expandable sections: DHCP Settings, DNS Settings, and Advanced.
- Comment: Internal ZServer
- Buttons: Save (with a green checkmark) and Cancel (with a red X).

Speichern Sie mit **Save** ab.

## 2.5.2 Firewallregeln für Lehrernetz konfigurieren

Gehen Sie zu *Network Protection – Firewall* und fügen Sie mit *New Rule* eine neue Regel hinzu und



platzieren Sie diese an Position sechs der Regeln:

Konfigurieren Sie die neu erstellte Regel wie folgt: Erstellen Sie eine neue Gruppe *Lehrernetz*, wie im Beispiel ersichtlich, hier auf Position 6. Fügen Sie als *Sourcen* folgende *Hosts* hinzu: *Internal Gserver03*, *Internal-Gserver03-Proxy*, *Internal ZServer*, als *Services* *Any* und als *Action* *Allow*. Als Kommentar können Sie z.B. *access Lehrernetz* hinzufügen. Fügen Sie dann eine weitere Regel hinzu, in der Sie dann *Source* und *Destination* vertauschen. Diese Regel erhält die *Position* 7.



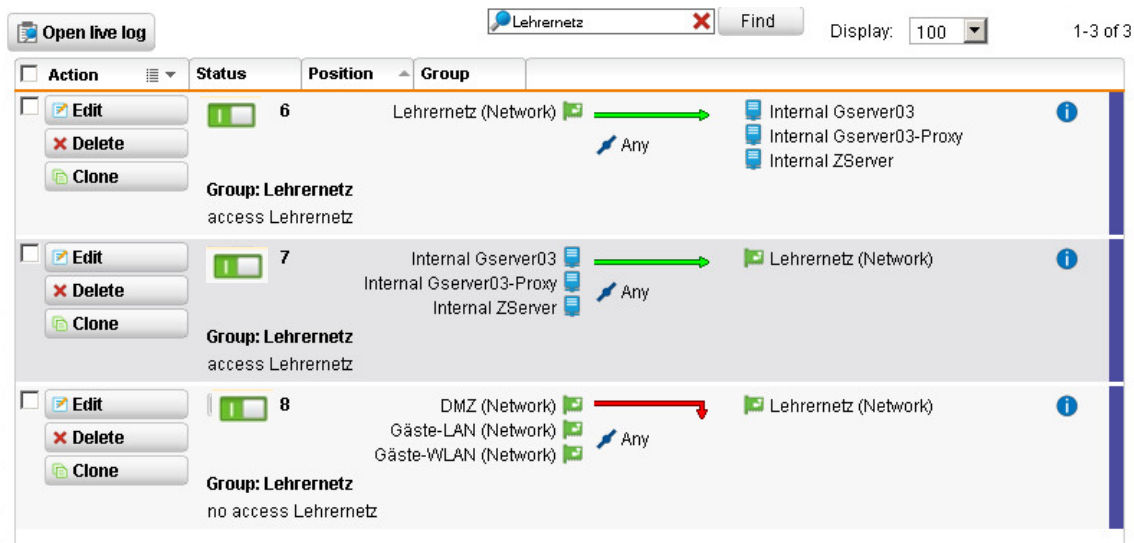
Wollen Sie auch auf *Vibe* und *Filr* vom Lehrernetz aus zugreifen, fügen Sie diese zwei Host-Objekte ebenfalls hinzu. Falls *Vibe* und *Filr* als Host-Objekte noch nicht angelegt sind, gehen Sie so vor, wie bei der Konfiguration einer *Netzwerkdefinition* des ZServers in Kapitel 2.5.1

Allen anderen Netzwerken wird zusätzlich explizit der Zugriff auf das *Lehrernetz* verboten:

Fügen Sie mit *New Rule* eine weitere Firewall-Regel hinzu und konfigurieren Sie diese wie abgebildet:

The screenshot shows the 'Create new rule' dialog box. The 'Group' dropdown is set to 'Lehrernetz'. The 'Position' dropdown is set to '8'. The 'Sources' list contains three items: 'DMZ (Network)', 'Gäste-LAN (Network)', and 'Gäste-WLAN (Network)'. The 'Services' list contains one item: 'Any'. The 'Destinations' list contains one item: 'Lehrernetz (Network)'. The 'Action' dropdown is set to 'Drop'. The 'Comment' field contains the text 'no access Lehrernetz'. At the bottom, there are 'Save' and 'Cancel' buttons. Red boxes highlight the 'Lehrernetz' group, the position '8', the source networks, the 'Any' service, the destination 'Lehrernetz (Network)', the 'Drop' action, and the 'Save' button.

Gibt man unter *Network Protection – Firewall* den Begriff *Lehrernetz* in das Suchfeld ein und klickt auf *Find*, sollten die drei neu erstellten Firewall-Regeln hintereinander, im Beispiel unter den Positionen 6-8, auftauchen:



Um die oben erstellen Regeln zu aktivieren, muss der jeweilige *Status*-Schalter eingeschaltet werden (Status: grüner Schalter).

Damit ist die Konfiguration des Lehrernetzes abgeschlossen. Nun sollten sich Clients im Lehrernetz mit einer IP-Adresse konfigurieren, eine Anmeldung am eDirectory möglich sein sowie eine Anmeldung an der PAEDML\_ZONE des ZServers. Es muss der Zugriff auf die Home-, Tausch- und Projektverzeichnisse möglich sein, wie auch der Internetzugriff.

### 3. Änderungshistorie

Trotz sorgfältiger Überprüfung ist die vorliegende Installationsanleitung zur Inbetriebnahme des Lehrernetzes nicht frei von Fehlern. Auf dieser Seite finden Sie deshalb eine kurze Zusammenfassung aller Korrekturen und inhaltlichen Überarbeitungen, die seit der Veröffentlichung des Dokumentes *paedML-Novell-Lehrernetz.pdf* vorgenommen wurden.

#### Aktualisierung der Anleitung vom 17.7. 2016:

- S. 6: Es wurde das Kapitel 1.2 „Zugriff auf die Apache2-Verwaltungsinstanz erlauben“ hinzugefügt.
- S. 12: Es wurde in Kapitel 2.5.2 die Firewallregel für das Lehrernetz um den Hinweis zu *Vibe* und *Filr* erweitert.

- Das Paket *lehrernetz.zip* wurde aktualisiert, der darin enthaltenen Zonendatei für das Lehrernetz wurden zusätzliche Einträge hinzugefügt (für den Zugriff auf GServer03, ZServer usw.). Es wurde eine weitere Zonendatei für Reverse-Lookup der DMZ-Zone hinzugefügt.



## 4. Anhang

### 4.1 paedML Novell Netzwerkzonen

Netzwerk- zone	Vmware		Firewall		IP-Dienste konfiguriert auf:								IP-Konfiguration			
					Gserver03				Firewall / UTM				IP	Mask	Gateway	
	VMnet	ID	8NIC	4NIC	DNS	DHCP	NAT	DNS	DHCP	NTP	NAT					
		0														
		1														
		2														
		3														
		4														
		5														
		6														
		7														
		8														
External (EXT)	8	9	eth1	eth1	-	-	-	ISP	ISP	ISP	-	(192.168.8.6)	(255.255.255.0)	(192.168.8.1)		
Internal	3	10	eth0	eth0	X	X	DMZ	-	-	X	-	10.1.1.30	255.255.0.0	10.1.1.32		
DMZ	1	11	eth2	eth2.11	-	-	-	X	(X)	X	External	192.168.1.1	255.255.255.0	192.168.1.1		
Internal - WLAN	2	12	eth3	eth3.12	X	X	-	-	Proxy	X	-	172.16.0.1	255.255.0.0	172.16.0.1		
Gast-WLAN	4	13	eth4	eth3.13	-	-	-	X	X	X	External	192.168.13.1	255.255.255.0	192.168.13.1		
Gast-LAN	5	14	eth5	eth3.14	-	-	-	X	X	X	External	192.168.14.1	255.255.255.0	192.168.14.1		
MGT-Netz		15	eth7	eth2.15	-	-	-	X	X	X	-	192.168.15.1	255.255.255.0	192.168.15.1		
		16														
		17														
Internal - LHR	6	18	eth6	eth3.18	X	X	-	-	Proxy	X	-	172.18.0.1	255.255.0.0	172.18.0.1		
		19														
Verwaltung		20	-	eth3.20	-	-	-	-	-	-	-	per DHCP	?	?		
		:														

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

© Landesmedienzentrum Baden-Württemberg, 2015