

Anleitung Schulfilter Plus im Lösungspaket Mobiles Lernen .

Inhaltsverzeichnis

- 1. Einleitung
- 2. Schuleigene Endgeräte zuhause und unterwegs
- 3. Schaubild
- 4. Produktbeschreibung
- 5. Systemvoraussetzungen
- 6. VM erstellen
- 7. Konfiguration der VM
- 8. Netzwerk-Konfiguration für transparente Filterung
- 9. DNS-Konfiguration
- 10. Ersteinrichtung der VM
- 11. Funktions-Test der erfolgreichen Einrichtung

1. Einleitung

Der Schulfilter Plus im Lösungspaket Mobiles Lernen wird Ihnen als virtuelle Maschine bereit gestellt. Hierdurch haben Sie einen Standard für alle Schulnetzwerke. Mit einer OVF-Datei haben Sie die Möglichkeit den Hypervisor Ihrer Wahl zu nutzen. Bitte beachten Sie, dass Sie die virtuelle Maschine mit der richtigen Rechenleistung ausstatten. Grundsätzlich gilt: Die Größe der Hardware richtet sich nach der Anzahl der gleichzeitigen Endgeräte, Höhe der Bandbreite sowie dem Umfang der Internetnutzung. Sie können jederzeit die virtuelle Maschine mit der passenden Hardwaregröße dynamisch ausstatten. So haben Sie immer die richtige Performance für Lehrer und Schüler.

Adressat dieser Anleitung

IT-Administration die für die Installation und Konfiguration der VM Schulrouter Plus mit den Lösungspaketen Netzwerksicherheit und Mobiles Lernen zuständig ist. Bei Fragen wenden Sie sich bitte an unseren [Service und Support](#).

2. Schuleigene Endgeräte zuhause und unterwegs

Wenn Sie schuleigene Endgeräte zuhause und unterwegs einsetzen, bietet Ihnen das [Lösungspaket Corona Hilfe II](#) den Schulfilter Plus aus der Cloud. Sobald das Endgerät das WLAN der Schule betritt wirkt automatisch, ohne Einstellungen der Administration, der Schulfilter Plus im Schulnetzwerk. Schülerinnen und Schüler können so durch die Schule und den Schulträger immer vor verbotenen Inhalten geschützt werden. Lehrkräfte können Schülerinnen und Schülern immer ein Bildungsinternet bieten.

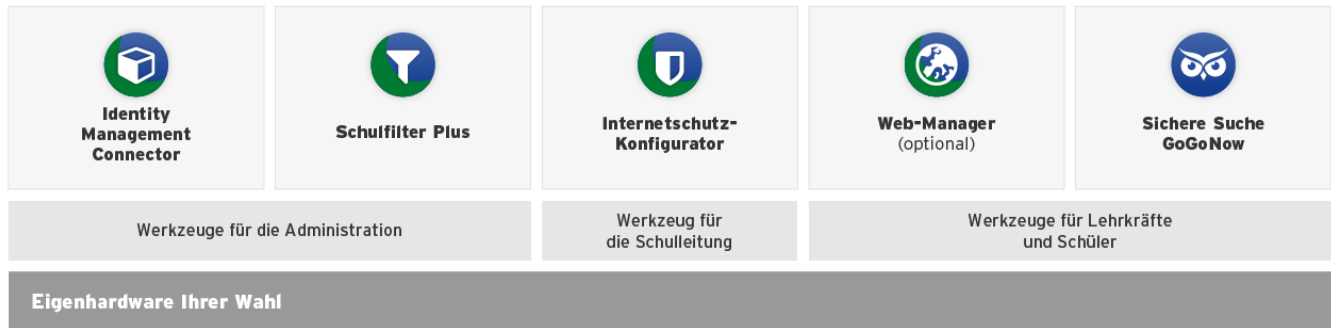
3. Schaubild



Schulfilter Plus im Lösungspaket Mobiles Lernen

Bildungsinternet in der Schule

- Alle Anwendungen in einem Werkzeugkasten als eine virtuelle Maschine (VM) für jede Infrastruktur im OVF-Format
- Für 200, 400, 1000, 1500, 2000 oder mehr Endgeräte
- Für folgende Hypervisoren: VMWare, Microsoft Hyper-V, Citrix Xen, KVM, Oracle Virtual Box
- Kompatibel zu allen vor- und nachgelagerten Produkten wie z.B Firewall, LAN, WLAN Captive Portal



4. Produktbeschreibung

Das **Lösungspaket "Mobiles Lernen"** auf einer virtuellen Maschine enthält unterschiedliche Anwendungen ist im Schuabild (Punkt 2) dargestellt.

[i Weitere Informationen zum Lösungspaket "Mobiles Lernen".](#)

5. Systemvoraussetzungen

- Prozessor
 - Multicore CPU (mindestens 4 Kerne)
 - Hardwarevirtualisierung (Intel VT-x oder AMD RVI)
 - mindestens 2GHz
 - [Benchmark-Wert](#) von mindestens 4000
- Arbeitsspeicher
 - mindestens 8 GB
- Festplattenspeicher
 - mindestens 50 GB
- Netzwerk
 - mindestens eine physische Netzwerkkarte mit 1 Gbit/s
- Internet
 - ein verfügbarer und durch die VM erreichbarer Internetanschluss
- Virtualisierungssoftware
 - VMware
 - KVM
 - Virtual PC
 - Xen
 - Hyper-V
 - VirtualBox

6. VM erstellen

Download

Downloaden Sie zuerst die VM von folgender Adresse: <http://repository.time-for-kids.de/dxvm/ovf/>

Speichern Sie alle im genannten Link enthaltenen Dateien. Die ovf-Datei ist die Steuerungsdatei der virtuellen Maschine und die vmdk-Datei enthält die Dateien der virtuellen Festplatte. Zu beiden Dateien gibt es Prüfsummen-Dateien (*.md5), die Sie ebenfalls herunterladen.

Checksummenprüfung

Prüfen Sie die Checksumme der ovf und vmdk Datei.

Nach dem Download der Dateien können Sie nun Prüfsummentools verwenden und die Prüfsummen der heruntergeladenen Dateien mit den Prüfsummen aus den md5-Dateien vergleichen. Nur wenn die Prüfsummen identisch sind, war der Download fehlerfrei.

Auf Linux-Betriebssystemen steht in der Regel [md5sum](#) hierfür zur Verfügung und für Windows gibt es kostenfreie Programme wie [WinMD5Free](#) oder [MD5 File Hasher](#).

VM-Import

Importieren Sie nun die VM aus dem Image in Ihren Hypervisor.

Ihr Hypervisor unterstützt keine OVF-Dateien?

Es gibt Hypervisoren, die das Standardformat OVF nicht unterstützen. In diesen Fällen besteht aber in der Regel die Möglichkeit die vmdk-Datei umzuwandeln.

Zur Umwandlung (Konvertierung) in die Formate VHD, VHDX (beides HyperV) oder QCOW2 (KVM) bietet beispielsweise [StarWind](#) ein [Konvertierungstool](#) an.

7. Konfiguration der VM

Nachdem die VM erfolgreich importiert wurde, konfigurieren Sie diese entsprechend folgender Informationen:

Eigenschaft	Einrichtung
CPU	mind. 4 Kerne
RAM	mind. 8 GB
Netzwerkkarten	Es werden 2 Karten für die Kommunikation nach Außen (extern) und eine Karte für eine rein interne Kommunikation benötigt.

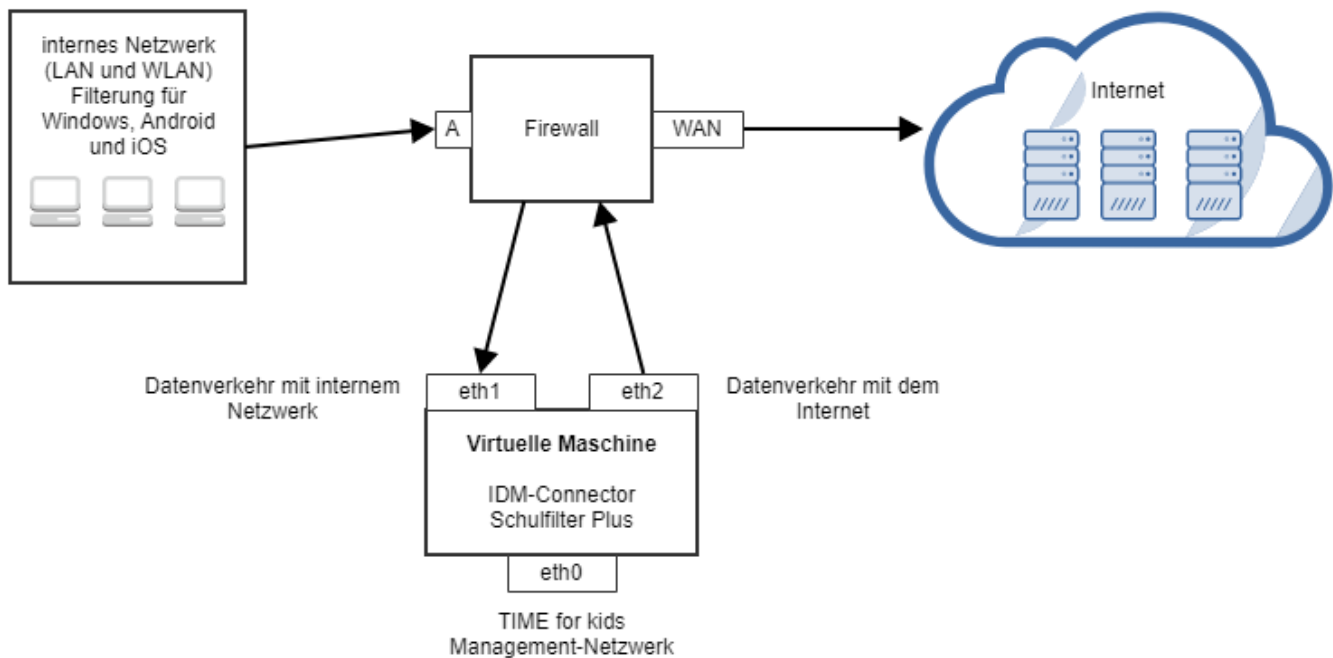
Konfiguration VirtualBox unter Windows

1. Konfigurieren Sie die 3 Netzwerkadapter auf den Typ "Netzwerkbrücke".
2. Aktivieren Sie in den Einstellungen der VM unter "System" die Option "Hardware-Uhr in UTC"

8. Netzwerk-Konfiguration für transparente Filterung

Mit dem Lösungspaket mobiles Lernen bietet TIME for kids den Schulen die Möglichkeit, ohne Einstellungen am Endgerät das WLAN mit einem gefilterten Bildungsinternet zu nutzen. Alle Endgeräte unter Windows, Android und iOS können gefiltert werden. Das nachstehende Schaubild und der darunterliegende Text beschreibt, welche Konfigurationen wo vorgenommen werden müssen.

Geben Sie uns ein Feedback, ob die Darstellung für Sie ausreichend ist oder für Administratoren an Schulen umfangreicher erklärt werden muss.



Anzahl der Netzwerkschnittstellen

⚠ Für den vollen Funktionsumfang, nutzen Sie einen Server, der - wie oben beschrieben - mindestens zwei Netzwerkanlüsse besitzt. Wenn Sie eine einfache und schnelle Lösung mit einem PC suchen, dann prüfen Sie, ob Sie in Ihren PC eine weitere Netzwerkkarte einstecken können.

Wenn Sie den Schulfilter Plus nur via Proxy anbinden möchten, bieten wir alternativ eine Konfigurationsmöglichkeit mit nur einer verbundenen Netzwerkkarte an.

Mit der aktuellen VM-Vorlage können Sie nun auch mit nur einer Netzwerkschnittstelle arbeiten.

Konfigurieren Sie hierfür im unten beschriebenen Schritt "Netzwerkkonfiguration" nur die Schnittstelle eth1. Geben Sie keine IP für Schnittstelle eth2 an!

Im Weiteren folgen Informationen zum Standardprozess für einen Server mit 2 Netzwerkschnittstellen.

Für die transparente Filterung von HTTP und HTTPS, ist dieser Datenverkehr vom Kunden über die SFP-VM zu leiten.

Folgende Schnittstellen werden verwendet:

- eth0 ist für die interne Kommunikation vorgesehen und ist nicht zu konfigurieren
- eth1 ist für die Kommunikation Richtung Schulnetzwerk vorgesehen
- eth2 ist für die Kommunikation Richtung Internet vorgesehen

Routing

Der Schulfilter Plus erhält durch Routing alle Internetanfragen die gefiltert werden sollen. Diese Einstellungen müssen zum Beispiel in der zum Einsatz kommenden Firewall vorgenommen werden. Datenverkehr der nicht gefiltert werden soll, darf nicht über den Schulfilter Plus geroutet werden.

Policy based Routing in der Firewall:

1. Regel: Traffic der gefiltert werden soll vom Typ HTTP und HTTPS vom internen Netzwerk Schnittstelle A mit dem Ziel Internet über Gateway Tfk VM
2. Regel: Traffic der gefiltert werden soll vom Typ HTTP und HTTPS vom Internet Schnittstelle WAN mit dem Ziel internes Netzwerk über Gateway Tfk VM

Firewall-Freigaben für LAN und WLAN

Freigaben aus dem pädagogischen Netz in Richtung TIME for kids Schulfilter Plus-VM

Anwendung	Portnummer
Proxy	3128
HTTP	80
HTTPS	443
Sichere Suche	1910-1917, 50344
Blockpage	83

Freigaben aus der TIME for kids Schulfilter Plus VM in Richtung dem Pädagogisches Netz

Anwendung	Portnummer
Domain Controller - LDAPS	636
Domain Controller - LDAP	389
Domain Controller - Kerberos	88, 464
Domain Controller - DNS	53
Domain Controller - SMB	445
Domain Controller - Remote Procedure Call	135
Domain Controller - Netbios Session Service	139

9. DNS-Konfiguration

Die VM des Lösungspaketes "Mobiles Lernen" enthält einen DNS-Server, welcher alle für das Produkt notwendigen Domain-Name-Einträge bereithält.

Wenn Sie einen eigenen bzw. lokalen DNS-Server für die Endgeräte nutzen, muss für diesen lediglich die VM als Upstream-DNS-Server konfiguriert werden.

Wenn Sie keinen anderen DNS-Server einsetzen, geben Sie bei den Endgeräten als DNS-Server die IP der VM an.


10. Ersteinrichtung der VM

Starten Sie nun die VM.

In der Konsole der VM sehen Sie nach dem Hochfahren die Willkommensmeldung mit dem Hinweis auf das Login:

Nach Login mit den angegebenen Zugangsdaten werden Sie einmalig zum Ändern des Standardpasswortes aufgefordert und befinden sich anschließend in der Ersteinrichtung, in welcher Sie grundlegende Systemkonfigurationen vornehmen können.

Netzwerkkonfiguration

- Richten Sie mit **netconf** die IPs für eth1 und eth2 entsprechend Ihrer Netzwerkumgebung ein.
 - Wenn ihr Host-System nur über eine Schnittstelle verfügt, beachten Sie das obere Kapitel "Anzahl der Netzwerkschnittstellen" !
- Falls gewünscht, können Sie mit **dns** den Nameserver ändern.
- Netzwerk-Konfiguration im Hypervisor
 - Weisen Sie dem Netzwerkadapter für eth0 ein eigenes internes Netzwerk zu.
 - Weisen Sie weiterhin den Netzwerkadaptern für eth1 und eth2 jeweils ein eigenes Netzwerk für die Kommunikation mit der Firewall zu.
 -  Für die Zuweisung von Hypervisor-Netzwerken zu den Netzwerkadaptern, beachten Sie, welcher Adapter im Hypervisor zu welcher Schnittstelle der VM (Linux) zugeordnet wurde. Richten Sie sich nach der Mac-Adresse, welche Sie mit dem Befehl `ip address` ermitteln können.
 - Geben Sie für eth2 ein Gateway an, um die Kommunikation mit dem Internet zu ermöglichen.
- Führen Sie in der VM einen Test durch, ob die Namensauflösung und der Internetzugang funktionieren. Beispielsweise mittels:

```
ping test.de
```

Systemupdate

1. Sobald die Netzwerkanbindung konfiguriert wurde, führen Sie mit dem Befehl **systemupdate** die Paketinstallation und -aktualisierung durch!

Domain-Join (optional)

1. Um den Beitritt in eine Active Directory Domain zu konfigurieren, können Sie den Befehl **domainjoin** nutzen. Folgende Informationen werden dann abgefragt:
 - a. FQDN der Domain
 - b. IP der Domain
 - c. Hostname des AD-Servers
 - d. Userdomain, der beigetreten werden soll
 - e. Realm des AD-Servers
 - f. Nutzername

Übersicht aller Befehle

Bevor Sie das Tool per **exit** beenden, können Sie sich mit dem Befehl **help** weitere zur Verfügung stehende Befehle anzeigen lassen.

Befehl	Kurzbeschreibung
atop	Linux atop Kommando, Analyse der Systemlast/Auslastung der CPU
date	Anzeige und Setzen der Systemzeit
df	Linux df Kommando, zeigt den freien Festplattenspeicher an
dns	Setzen des DNS-Servers
domainjoin	Mit diesem Befehl könnten Sie mit der VM einer Domäne beitreten. Geben Sie dazu alle von diesem Befehl abgefragten Daten an.
firewall	Aktive Firewall-Regeln anzeigen, mit -c werden auch Zählerstände (Pakete, Bytes) ausgegeben
free	Linux free Kommando, zeigt den freien Arbeitsspeicher an
help	Anzeige der zur Verfügung stehenden Befehle und Hilfe zu diesen Befehlen (<i>help befehl</i>)
hostname	Setzen Sie den gewünschten Hostname der VM.
htop	Linux htop Kommando zur Analyse der Systemlast/Auslastung der CPU
ip	Entsprechend des Linux Tools "ip" Nutzen Sie beispielsweise "ip a" um die Aufstellung der Netzwerkschnittstellen, deren MAC, IP und weiteren Informationen zu erhalten.
iptables-save	Linux iptables-save Kommando zur Einsicht der Firewallregeln (alt, ersetzt durch: firewall)
netconf	Einrichtung der Schnittstellen eth1, eth2 Geben Sie dazu alle von diesem Befehl abgefragten Daten an.
netstat	zum Prüfen auf welche Ports das System hört (z.B. zum Prüfen auf welchen Port der Squid hört)

passwd	Setzt das Passwort für den Einrichtungsassistenten
ping	zum Prüfen von Erreichbarkeiten
poweroff	Führt das System herunter
ps	Linux ps Kommando
pstree	Linux pstree Kommando, zeigt die Prozesse des Systems in einer Baumstruktur an
reboot	Startet das System neu
ss	Linux ss Kommando
systemupdate	Mit diesem Kommando können Sie - sobald die Netzwerkconfiguration erfolgte - die Paket-Installation und -Aktualisierung starten.
tcpdump	Linux tcpdump Kommando zum Prüfen des Netzwerkverkehrs
top	Linux top Kommando zur Analyse der Systemlast/Auslastung der CPU
traceroute	Linux traceroute Kommando. Ermittelt, über welche Knoten IP-Datenpakete bis zum angegebenen Ziel gelangen.
versions	Zeigt die Versionsnummern der installierten TIME for kids Software-Komponenten
wbinfo	Mit diesem Systembefehl können Sie den erfolgreichen Domänenbeitritt prüfen. Folgende Parameter stehen zur Verfügung: <ul style="list-style-type: none"> • -t • -u • -g

11. Funktions-Test der erfolgreichen Einrichtung

Prüfen Sie nun die Erreichbarkeit des System und die Filterung.

Produkt aufrufen und lizenzieren

Rufen Sie im Browser eines im Netzwerk befindlichen Endgerätes die von Ihnen festgelegte IP der VM auf.

Anschließend öffnet sich ein Loginfenster.

1. Loggen Sie sich initial mit dem Benutzernamen "tfkadmin" und dem Passwort "tfkadmin" an.
2. Sie werden zum Ändern des Passwortes aufgefordert.
3. Anschließend sehen Sie die Kachelansicht mit allen zur Verfügung stehenden Produkten.
4. Wechseln Sie nun zum Schulfilter Plus über die entsprechende Kachel.
5. Geben Sie unter "Lizenzierung" Ihre Schulfilter Plus Lizenz an und betätigen Sie "Speichern"

Filter-Test

Filterung mit Proxy

Konfigurieren Sie hierfür den Browser und setzen Sie den Proxy auf die von Ihnen festgelegte IP der VM mit dem Port 3128. Vergewissern Sie sich, dass der Proxy für alle Protokolle (HTTP, HTTPS) angegeben wurde.

Rufen Sie nun im Browser Testseiten auf:

1. <http://casino.net>
 - a. diese Seite wird mit einer Blockseite des Schulfilter Plus gesperrt, da sie zu einem standardmäßig gesperrten Themenfeld (Glücksspiel) gehört.
2. <http://time-for-kids.de>

- a. diese Seite ist freigegeben und aufrufbar

Transparente Filterung

Konfigurieren Sie hierfür den Browser und deaktivieren Sie dessen Proxy (kein Proxy). Stellen Sie sicher, dass der Datenverkehr der Endgeräte über die VM geleitet wird!

Rufen Sie nun im Browser Testseiten auf:

1. <http://casino.net>
 - a. diese Seite wird mit einer Blockseite des Schulfilter Plus gesperrt, da diese zu einem standardmäßig gesperrten Themenfeld (Glücksspiel) gehört.
2. <https://casino.com>
 - a. Die Seite kann nicht aufgerufen werden, da diese zu einem standardmäßig gesperrten Themenfeld (Glücksspiel) gehört.
 - b. Aufgrund des Aufrufes über HTTPS, wird die Verbindung unterbrochen. Es kann nicht auf eine Blockseite umgeleitet werden.
3. <http://time-for-kids.de>
 - a. diese Seite ist freigegeben und aufrufbar