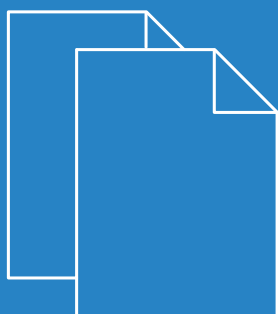


# LCOS FX 10.8

## Addendum



# Inhalt

<b>1 Addendum zur LCOS FX-Version 10.8.....</b>	<b>4</b>
<b>2 Traffic Shaping.....</b>	<b>5</b>
2.1 Shaping-Konfigurationen.....	5
2.2 Traffic-Gruppen.....	7
2.2.1 Traffic-Gruppen-Zuordnung und DSCP-Werte für ausgehenden Datenverkehr.....	7
<b>3 WWAN.....</b>	<b>12</b>
<b>4 BPJM-Modul.....</b>	<b>13</b>

# Copyright

© 2022 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhaltes sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunfts- bezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Bitte senden Sie eine E-Mail an [gpl@lancom.de](mailto:gpl@lancom.de).

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde ([www.openssl.org](http://www.openssl.org)).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

[www.lancom-systems.de](http://www.lancom-systems.de)

# 1 Addendum zur LCOS FX-Version 10.8

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.8 gegenüber der vorherigen Version.

## 2 Traffic Shaping

Der Menüpunkt **Netzwerk > QoS** mit seinen beiden Untermenüpunkten wurde entfernt, bzw. ersetzt durch das neue Menü unter **Netzwerk > Traffic Shaping** und zusätzliche Einstellungen in einzelnen Editoren.

Unter **Netzwerk > Traffic Shaping** können Sie Einstellungen zu Ihrem IP-Traffic vornehmen. Dabei wird ein weitergehenderer Ansatz verfolgt, als nur Quality-of-Service-Werte zuzuweisen. Hier definieren Sie Traffic-Gruppen, über die Regeln für diese Traffic-Gruppe an diversen Stellen in Ihrer LANCOM R&S® Unified Firewall angewendet werden:

- > Über eine Desktop-Verbindung: Dies gilt für den gesamten verschlüsselten Tunnel-Traffic, wobei einzelne Trafficarten innerhalb des Tunnels nicht berücksichtigt werden. Die Zuordnung zu einer Gruppe kann für die ganze Verbindung oder auch nur für einzelne Regeln der Verbindung erfolgen.
- > Über einen IPsec-Tunnel: Dies betrifft den verschlüsselten Datenverkehr über diesen Tunnel, ohne Berücksichtigung evtl. verschiedenartiger unverschlüsselter Daten innerhalb des Tunnels.
- > Über ein App-Routing-Profil: Betrifft den Traffic, der einer der im Profil eingestellten Applikationen und einer Desktop-Verbindung entspricht, auf der dieses Profil verwendet wird.

Die Gruppen können in Regeln verwendet werden, um zu bestimmen, wie ihnen entsprechender Datenverkehr priorisiert werden soll und welche Bandbreiten-Limits und -Garantien gelten. Dazu werden diese Regeln jeweils pro Interface in **Shaping-Konfigurationen** zusammengefasst. Eine solche Shaping-Konfiguration

- > gilt für ein bestimmtes WAN-Interface oder den inneren Traffic zu einem Routen-basierten IPsec-Tunnel,
- > legt fest, welche Bandbreiten (Upload / Download) über das gewählte Interface oder den gewählten Tunnel insgesamt zur Verfügung stehen und
- > hält, separat für Upload und Download, je eine Liste von anzuwendenden Shaping-Regeln. Dies ist für eine Traffic-Gruppe die Priorität, garantierte Bandbreite und maximale Bandbreite.

An allen Stellen, an denen Traffic einer Gruppe zugeordnet werden kann (Desktop-Verbindung, IPsec-Tunnel oder App-Routing-Profil), kann optional auch ein DSCP-Wert (Quality of Service) für ausgehende Pakete festgelegt werden. Damit kann anderen Geräten entlang der Paket-Route innerhalb sowie auch außerhalb des Netzwerks der LANCOM R&S® Unified Firewall ein Anhaltspunkt zur Paket-Priorisierung mitgeteilt werden. Wird keine Angabe gemacht, dann bleibt der entsprechende IP-Paket-Header unberührt und behält seinen alten Wert.







### 2.1 Shaping-Konfigurationen




Navigieren Sie zu **Netzwerk > Traffic Shaping > Shaping-Konfigurationen**, um Ihre Shaping-Konfigurationen zu verwalten. In einer solchen Konfiguration können für ein WAN-Interface oder den Traffic innerhalb eines IPsec-Tunnels die nötigen Rahmenparameter sowie einzelne Shaping-Regeln für eingehenden und ausgehenden Datenverkehr festgelegt werden. Die Shaping-Regeln legen fest, wie der Traffic, der zu den verschiedenen Traffic-Gruppen gehört, für das angegebene Interface bzw. den Tunnel und die jeweilige Richtung priorisiert werden soll.

Traffic, der keiner der eingehenden Regeln entspricht, hat die niedrigste Priorität und es wird keine Bandbreite garantiert. Die Summe der garantierten Bandbreiten aller Regeln einer Übertragungsrichtung darf die maximale Interface-Bandbreite für diese Übertragungsrichtung nicht überschreiten. Dasselbe gilt für die in einer Regel festgelegte maximale Bandbreite.

Im Bearbeitungsfenster **Shaping-Konfiguration** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/O	Ein Schiebeschalter gibt an, ob diese Shaping-Konfiguration derzeit aktiv (I) oder inaktiv (O) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status.


Eingabefeld	Beschreibung
	<p> Pro Interface bzw. Tunnel kann es nur eine aktive Shaping-Konfiguration geben.</p>
<b>Interface</b>	Wählen Sie ein Interface aus.
<b>Maximale Download-Bandbreite</b>	<p>Geben Sie die maximale Download-Bandbreite des gewählten Interfaces an. Diese Angabe wird benötigt, um die Regeln für eingehenden Datenverkehr korrekt anzuwenden.</p> <p> An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.</p>
<b>Maximale Upload-Bandbreite</b>	<p>Geben Sie die maximale Upload-Bandbreite des gewählten Interfaces an. Diese Angabe wird benötigt, um die Regeln für ausgehenden Datenverkehr korrekt anzuwenden.</p> <p> An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.</p>
<b>Eingehende Regeln</b> – Definieren Sie hier den Regelsatz für eingehenden Datenverkehr. Eine einzelne Regel ordnet dem Datenverkehr der ausgewählten Traffic-Gruppe eine Priorität und ein Bandbreiten-Kontingent zu. Dieses besteht aus der einer Traffic-Gruppe garantierten Bandbreite und der Bandbreite, die sie maximal in Anspruch nehmen darf.	
<b>Traffic-Gruppe</b>	Wählen Sie die Traffic-Gruppe aus, für die diese Regel gelten soll.
<b>Priorität</b>	<p>Eine kleine Zahl (1) entspricht einer hohen Priorität, eine hohe Zahl (7) einer niedrigen.</p> <p> Mehrere Regeln können die gleiche Priorität haben. In diesem Fall wird die Übertragungskapazität „fair“ aufgeteilt.</p>
<b>Garantierte Bandbreite</b>	<p>Garantierte Bandbreite für diese Traffic-Gruppe.</p> <p> An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.</p>
<b>Maximale Bandbreite</b>	<p>Maximale Bandbreite für diese Traffic-Gruppe.</p> <p> An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.</p>
<b>Ausgehende Regeln</b> – Definieren Sie hier den Regelsatz für ausgehenden Datenverkehr	
<b>Traffic-Gruppe</b>	Wählen Sie die Traffic-Gruppe aus, für die diese Regel gelten soll.
<b>Priorität</b>	<p>Eine kleine Zahl (1) entspricht einer hohen Priorität, eine hohe Zahl (7) einer niedrigen. Pro Interface kann nur eine Shaping-Konfiguration zur gleichen Zeit aktiv sein. Traffic, der keiner der ausgehenden Regeln entspricht, hat die niedrigste Priorität und es wird keine Bandbreite garantiert. Die Summe der garantierten Bandbreiten aller Regeln einer Übertragungsrichtung darf die maximale Interface-Bandbreite für diese Übertragungsrichtung nicht überschreiten. Dasselbe gilt für die in einer Regel festgelegten maximalen Bandbreite.</p>

Eingabefeld	Beschreibung
	 Mehrere Regeln können die gleiche Priorität haben. In diesem Fall wird die Übertragungskapazität „fair“ aufgeteilt.
<b>Garantierte Bandbreite</b>	Garantierte Bandbreite für diese Traffic-Gruppe.  An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.
<b>Maximale Bandbreite</b>	Maximale Bandbreite für diese Traffic-Gruppe.  An der rechten Seite des Bandbreiten-Eingabefeldes wird die aktuell gültige Einheit bzw. Größenordnung für die Eingabe angezeigt (GBit/s, MBit/s, KBit/s). Mit einem Klick auf die gegenwärtig eingestellte Größenordnung lässt sich ein Menü öffnen, um diese anzupassen. Außerdem wechselt durch Tippen von „g“, „m“ oder „k“ im Eingabefeld die Größenordnung ebenfalls auf Giga, Mega oder Kilo.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

## 2.2 Traffic-Gruppen

Navigieren Sie zu **Netzwerk > Traffic Shaping > Traffic-Gruppen**, um die Liste der derzeit im System angelegten Traffic-Gruppen anzuzeigen und zu verwalten. Diesen Traffic-Gruppen kann Datenverkehr auf unterschiedlichen Wegen zugeordnet werden (Desktop-Verbindung, IPsec-Verbindung, App-Routing-Profil, DSCP-Wert).

Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Traffic-Gruppe ansehen und anpassen oder eine Traffic-Gruppe aus dem System löschen. Klicken Sie auf die Schaltfläche , um eine neue Traffic-Gruppe anzulegen. Es öffnet sich ein Bearbeitungsfenster, in dem Sie die Einstellungen für eine Traffic-Gruppe anpassen können.

Im Bearbeitungsfenster **Traffic-Gruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
<b>Name</b>	Der Name dieser Traffic-Gruppe. Sie können bis zu 7 Traffic-Gruppen anlegen.
<b>DSCP eingehend</b>	Wählen Sie einen optionalen DSCP-Wert für eingehenden Datenverkehr aus der Liste aus. Datenverkehr, der außerhalb der Unified Firewall entsprechend markiert wurde, wird in der Unified Firewall der aktuellen Traffic-Gruppe zugeordnet. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „AF41“) und der Gruppe (z. B. „Multimedia Conferencing“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste können Sie entsprechend dieser Darstellungen durchsuchen, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

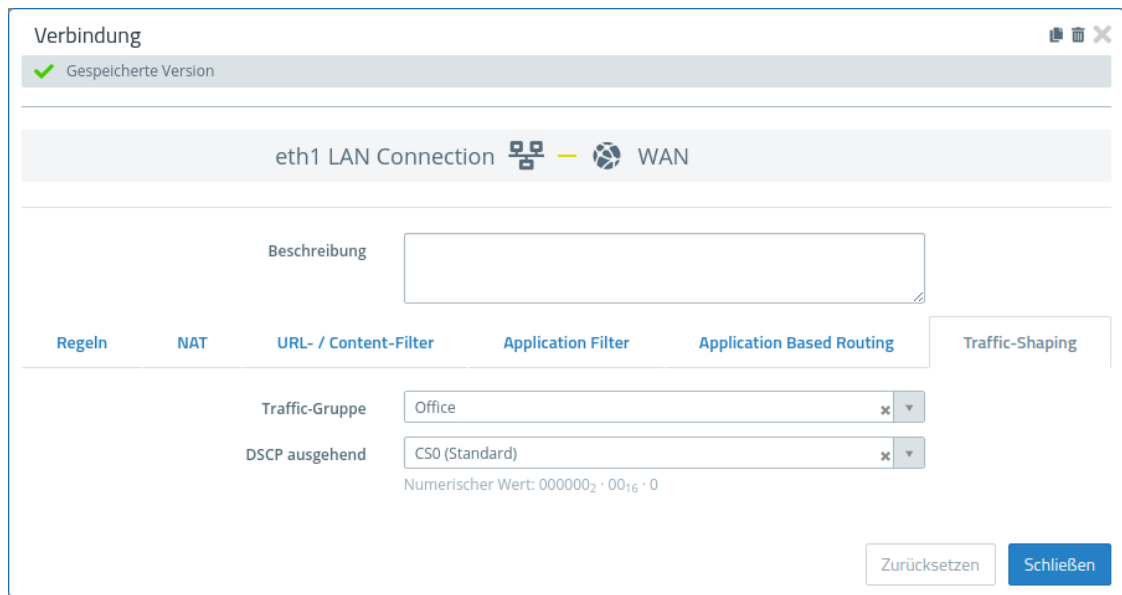
### 2.2.1 Traffic-Gruppen-Zuordnung und DSCP-Werte für ausgehenden Datenverkehr

An unterschiedlichen Stellen lässt sich Datenverkehr einer Traffic-Gruppe zuordnen, sowie ein DSCP-Wert festlegen, mit dem entsprechende Pakete vor dem Weitersenden durch die LANCOM R&S<sup>®</sup> Unified Firewall versehen werden. Beide

Angaben sind stets optional. Die Angabe einer **Traffic-Gruppe** erlaubt es, den entsprechenden Datenverkehr mit Hilfe einer Shaping-Konfiguration zu priorisieren. Der Wert im Feld **DSCP ausgehend** erlaubt es anderen Geräten im Netzwerk, die entsprechenden Pakete ebenfalls zu klassifizieren und – bei entsprechender Konfiguration – wunschgemäß zu behandeln.


**Desktop-Verbindungen**

Die Einstellungen betreffen den Datenverkehr, welcher der bearbeiteten Desktop-Verbindung entspricht. Die Einstellungsmöglichkeiten bei Desktop-Verbindungen verhalten sich wie diejenigen für NAT-Einstellungen: Sie lassen sich sowohl für die gesamte Desktop-Verbindung als auch für einzelne Regeln innerhalb dieser Verbindung vornehmen. In beiden Fällen werden die Einstellungen über den Tab **Traffic-Shaping** (entweder auf Verbindungs- oder auf Regelebene) vorgenommen. In der Regelliste lässt sich in der zweiten Spalte (TS) anhand der Checkboxes sehen und anpassen, ob die Einstellungen auf Verbindungs-Ebene genutzt werden sollen, oder nicht.



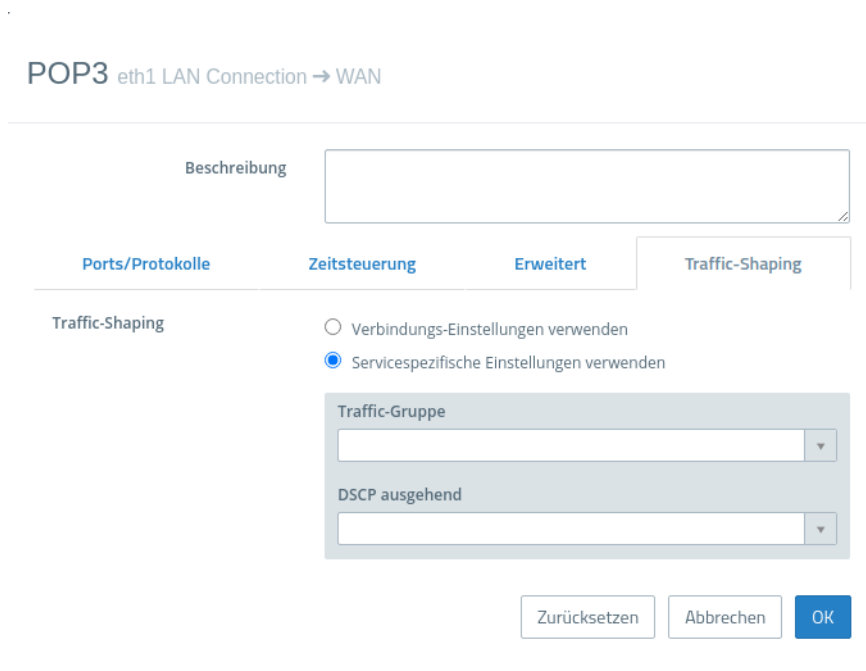
**Abbildung 1: Desktopverbindung > Traffic-Shaping**

Im Tab **Traffic-Shaping** können Sie die Einstellungen des Traffic Shaping für den Datenverkehr auf der gewählten Verbindung konfigurieren:

Eingabefeld	Beschreibung
<b>Traffic-Gruppe</b>	<p>Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch <a href="#">Traffic Shaping</a> auf Seite 5.</p> <p> Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.</p>
<b>DSCP ausgehend</b>	<p>Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.</p>




Diese Einstellungen für die Verbindung lassen sich dann in einer Firewall-Regel verwenden oder dort durch servicespezifische Einstellungen überschreiben.



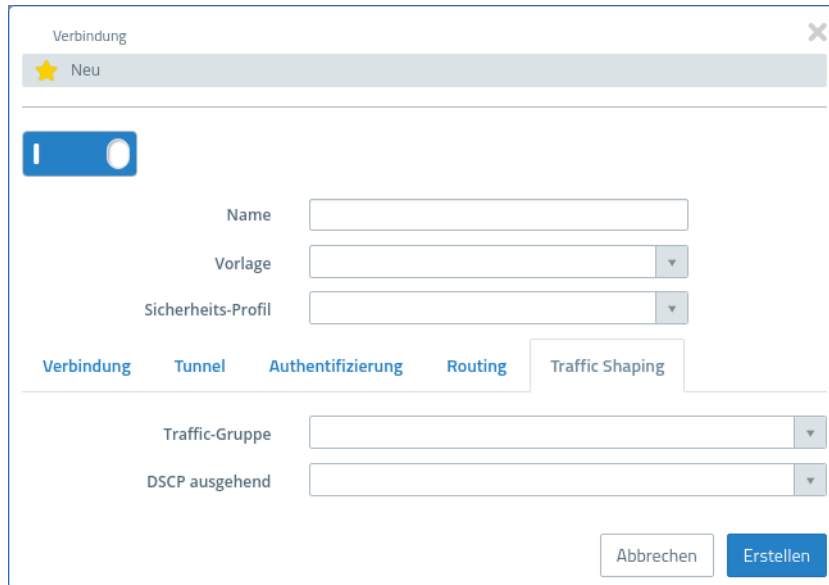
**Abbildung 2: Firewallregel > Traffic-Shaping**

Im Tab zu den Einstellungen unter **Traffic-Shaping** stehen die folgenden Optionen zur Verfügung:

Eingabefeld	Beschreibung
<b>Traffic-Shaping</b>	<p>Wählen Sie aus den folgenden Optionen:</p> <ul style="list-style-type: none"> <li>&gt; <b>Verbindungs-Einstellungen verwenden</b> – Mit dieser Einstellung werden die auf Verbindungsebene vorgenommenen Traffic-Shaping-Einstellungen übernommen. Siehe <a href="#">Einstellungen für Desktopverbindungen</a>.</li> <li>&gt; <b>Servicespezifische-Einstellungen verwenden</b> – Über diese Einstellung können sie die Traffic-Shaping-Einstellungen pro Service einstellen. Dazu werden die im Folgenden beschriebenen Einstellungen eingeblendet.</li> </ul>
<b>Traffic-Gruppe</b>	<p>Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch <a href="#">Traffic Shaping</a> auf Seite 5.</p> <hr/> <p> Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.</p>
<b>DSCP ausgehend</b>	<p>Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.</p>


**IPsec-Verbindungen und -Templates**

Unter **VPN > IPsec > Verbindungen** bzw. **VPN > IPsec > Vorlagen** können Sie die Traffic-Shaping-Regeln für IPsec-Verbindungen bzw. IPsec-Verbindungsvorlagen anwenden.



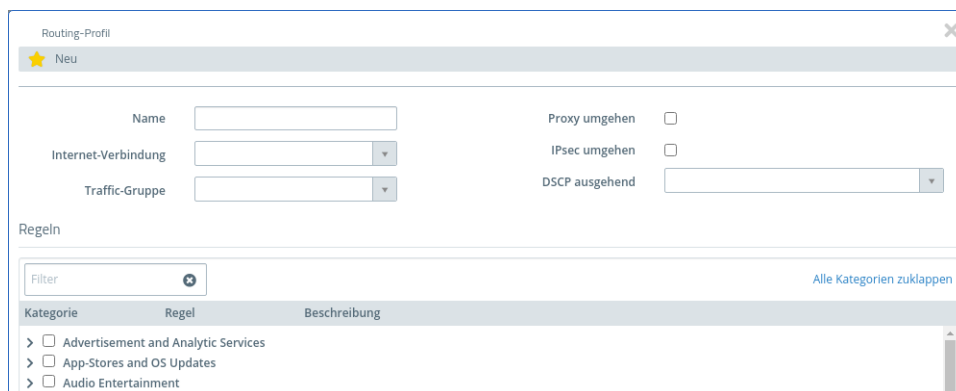
**Abbildung 3: VPN > IPsec > Verbindungen**

Im Tab **Traffic-Shaping** können Sie die folgenden Felder konfigurieren:

Eingabefeld	Beschreibung
<p><b>Traffic-Gruppe</b></p>	<p>Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr auf dieser Verbindung angewendet. Siehe auch <a href="#">Traffic Shaping</a> auf Seite 5.</p> <hr/> <p> Falls es sich um einen Routen-basierten IPsec-Tunnel handelt, kann der Datenverkehr innerhalb eines Tunnels mit Hilfe einer eigenen Shaping-Konfiguration priorisiert werden.</p>
<p><b>DSCP ausgehend</b></p>	<p>Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.</p>

### App-Routing-Profile

Hier finden Sie die Einstellungen nicht in einem eigenen Tab, sondern direkt auf oberster Ebene des Editors eines App-Routing-Profils unter **UTM > Application-Management > Routing-Profile**.



**Abbildung 4: UTM > Application-Management > Routing-Profile**

Eingabefeld	Beschreibung
<b>Traffic-Gruppe</b>	Wählen Sie optional den Namen einer Traffic-Gruppe aus. Dadurch werden die für diese Gruppe definierten Regeln für den Datenverkehr angewendet, der vom Application Filter den im Routing-Profil ausgewählten Regeln zugeordnet wird. Dafür muss der Datenverkehr zunächst auch der Desktop-Verbindung entsprechen, in der das bearbeitete App-Routing-Profil verwendet wird. Siehe auch <a href="#">Traffic Shaping</a> auf Seite 5.
<b>DSCP ausgehend</b>	Wählen Sie einen optionalen DSCP-Wert für ausgehenden Datenverkehr aus der Liste aus. Die Liste enthält die Bezeichnungen aus den relevanten RFCs (z. B. „CS0“) und der Gruppe (z. B. „Standard“). Zusätzlich wird der Wert ebenfalls in seiner numerischen Repräsentation zu verschiedenen Basen (binär, hexadezimal und dezimal) angezeigt. Die Liste kann entsprechend dieser Darstellungen durchsucht werden, so dass Sie unabhängig von der individuell bevorzugten Darstellung schnell den gewünschten Wert finden.

### 3 WWAN

Ab LCOS FX-Version 10.8 wird für WWAN-Verbindungen (**Netzwerk > Verbindungen > WWAN-Verbindungen**) in einer neuen Zeile unterhalb des Status jetzt auch der gegenwärtige Roaming-Status angezeigt, bzw. ob die Verbindung gerade in das Heimat-Netz besteht, oder nicht.

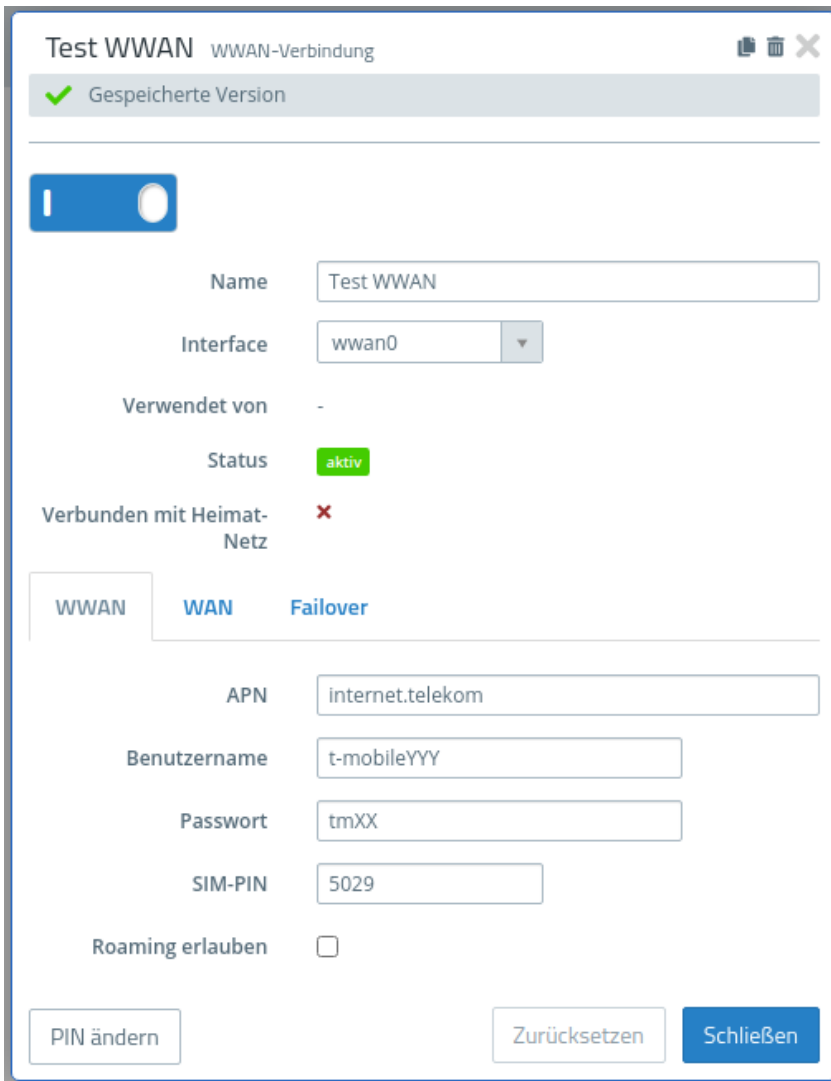


Abbildung 5: Netzwerk > Verbindungen > WWAN-Verbindungen

Eingabefeld	Beschreibung
<b>Verbunden mit Heimat-Netz</b>	Zeigt den Roaming-Status der Verbindung an bzw. ob die Verbindung gerade in das Heimat-Netz besteht, oder nicht.

## 4 BPJM-Modul

Ab LCOS FX-Version 10.8 gibt es über den URL / Contentfilter die Möglichkeit, Webseiten per BPJM-Modul zu sperren. Das BPJM-Modul wird von der Bundeszentrale für Kinder- und Jugendmedienschutz herausgegeben und sperrt Webseiten, die Kindern und Jugendlichen in Deutschland nicht zugänglich gemacht werden dürfen. Das ist vor allem für Schulen wichtig. Dies ist über eine separate Contentfilter-Kategorie realisiert.