SECURE. **NETWORKS.**

LCOS FX 10.8

Addendum

04/2022

LANCOM
Systems

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). If the respective license demands, the source files for the corresponding software components will be provided on request. Please send an e-mail to *gpl@lancom.de*.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from LANCOM Systems include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 10.8

This document describes the changes and enhancements in LCOS FX version 10.8 since the previous version.

2 Traffic shaping

The menu item **Network** > **QoS** with its two sub-menu items has been removed or replaced by the new menu under **Network** > **Traffic Shaping** and additional settings in individual editors.

Under **Network** > **Traffic Shaping** you can adjust the settings for your IP traffic. This approach involves more than just assigning Quality-of-Service values. Here you define traffic groups that are used to apply rules in various ways in your LANCOM R&S®Unified Firewall:

- Via a desktop connection: This applies to all of the encrypted tunnel traffic, not taking into account any individual types of traffic on the inside of the tunnel. The assignment to a group may be for the entire connection or only for individual rules of the connection.
- Via an IPsec tunnel: This concerns the encrypted data traffic sent through the tunnel, without accounting for the different types of unencrypted data in the tunnel.
- Via an app routing profile: This concerns the traffic for one of the applications set in the profile and for a desktop connection using this profile.

The groups can be used in rules to determine how the matching traffic should be prioritized, and what bandwidth limits and guarantees apply. For this purpose, these rules are collected for each interface in **Shaping Configurations**. A shaping configuration

- applies to a specific WAN interface or the internal traffic to a route-based IPsec tunnel,
- determines which bandwidths (upload/download) are available on the selected interface or the selected tunnel, and
- maintains a separate list of applicable shaping rules for uploads and downloads. For a traffic group, this is the priority, guaranteed bandwidth, and maximum bandwidth.

Wherever traffic can be assigned to a group (desktop connection, IPsec tunnel, or app routing profile), a DSCP value (Quality of Service) can optionally be specified for outbound packets. This gives an indication to other devices along the packet route (both inside and outside the LANCOM R&S®Unified Firewall network) how they should prioritize packets. If nothing is specified, the corresponding IP packet header with its original value remains unchanged.

2.1 Shaping configurations

Navigate to **Network** > **Traffic Shaping** > **Shaping Configurations** to manage your shaping configurations. A shaping configuration is used to specify the necessary framework parameters and individual shaping rules for inbound and outbound data traffic on a WAN interface or for the traffic in an IPsec tunnel. The shaping rules define how traffic belonging to the different traffic groups should be prioritized for the specified interface or tunnel and the respective direction.

Traffic that does not match any of the inbound rules has the lowest priority, and bandwidth is not guaranteed. The sum of the guaranteed bandwidths of all rules in any transmission direction must not exceed the maximum interface bandwidth for this transmission direction. The same applies to the maximum bandwidth specified in a rule.

In the **Shaping Configuration** editing window you can modify the following parameters:

Input box	Description
I/0	A slider button indicates whether this shaping configuration is currently enabled (**I**) or disabled (**0**). Click on the slider button to change this. ⓘ There can be only one active shaping configuration per interface or tunnel.
Interface	Choose an interface.

Input box	Description
Maximum Download Bandwidth	Enter the maximum download bandwidth for the selected interface. This information is required to correctly apply the rules for inbound traffic. ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on “g”, “m” or “k” in the input box sets the size to giga, mega or kilo.
Maximum Upload Bandwidth	Enter the maximum upload bandwidth for the selected interface. This information is required to correctly apply the rules for outbound traffic. ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on “g”, “m” or “k” in the input box sets the size to giga, mega or kilo.
Inbound Rules – Define the rule set for inbound data traffic here. A single rule assigns a priority and bandwidth quota to the data traffic of the selected traffic group. This consists of the bandwidth guaranteed to a traffic group, and the maximum permitted bandwidth.	
Traffic Group	Select the traffic group that this rule should apply to.
Priority	A small number (1) corresponds to a high priority, a high number (7) to a low priority. ⓘ Multiple rules can have the same priority. In this case, the sharing of the transmission capacity is “fair”.
Guaranteed Bandwidth	Guaranteed bandwidth for this traffic group. ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on “g”, “m” or “k” in the input box sets the size to giga, mega or kilo.
Maximum Bandwidth	Maximum bandwidth for this traffic group. ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on “g”, “m” or “k” in the input box sets the size to giga, mega or kilo.
Outbound Rules – Define the rule set for outbound data traffic here	
Traffic Group	Select the traffic group that this rule should apply to.
Priority	A small number (1) corresponds to a high priority, a high number (7) to a low priority. Only one shaping configuration can be active per interface at any time. Traffic that does not match any of the outbound rules has the lowest priority, and bandwidth is not guaranteed. The sum of the guaranteed bandwidths of all rules in any transmission direction must not exceed the maximum interface bandwidth for this transmission direction. The same applies to the maximum bandwidth specified in a rule. ⓘ Multiple rules can have the same priority. In this case, the sharing of the transmission capacity is “fair”.
Guaranteed Bandwidth	Guaranteed bandwidth for this traffic group. ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on “g”, “m” or “k” in the input box sets the size to giga, mega or kilo.
Maximum Bandwidth	Maximum bandwidth for this traffic group.

Input box	Description
	ⓘ The currently valid unit/size (Gbps, Mbps, Kbps) for the entry is displayed on the right-hand side of the bandwidth input box. Clicking on the current size setting opens a menu to adjust it. Also, tapping on "g", "m" or "k" in the input box sets the size to giga, mega or kilo.

If you change any settings, click **Save** to store your changes or **Reset** to discard them. Then click **Close** to quit the editing window.

2.2 Traffic groups

Navigate to **Network** > **Traffic Shaping** > **Traffic Groups** to display and manage the list of traffic groups currently in the system. Data traffic can be assigned to these traffic groups in different ways, i.e. desktop connection, IPsec connection, app routing profile, DSCP value.

Use the buttons in the last column to view and modify the settings for traffic groups or to delete a traffic group from the system. Click on the ⊕ button to configure a new traffic group. An editing window opens that you can use to adjust the settings for a traffic group.

In the **Traffic Group** editing window you can modify the following parameters:

Input box	Description
Name	The name of this traffic group. You can enter up to 7 traffic groups.
Incoming DSCP	From the list, select an optional DSCP value for inbound data traffic. Traffic that has been marked accordingly outside the Unified Firewall is assigned to the current traffic group in the Unified Firewall. The list contains the designations from the relevant RFCs (e.g. "A41") and the group (e.g. "Multimedia conferencing"). Also, the value is numerically represented in various bases (binary, hexadecimal, and decimal). You can search the list according to these representations so that you can quickly find the desired value regardless of the individually preferred representation.

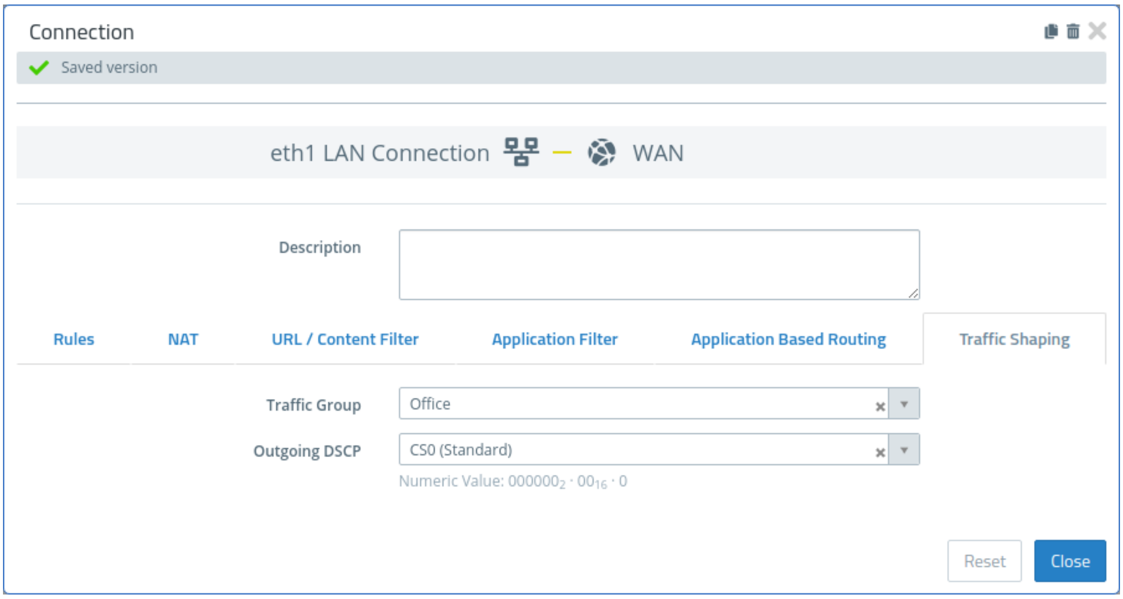
If you change any settings, click **Save** to store your changes or **Reset** to discard them. Then click **Close** to quit the editing window.

2.2.1 Traffic group assignment and DSCP values for outbound traffic

At various points, data traffic can be assigned to a traffic group and a DSCP value can be specified, which is then used to tag the corresponding packets before they are forwarded by the LANCOM R&S®Unified Firewall. Specifying these is always optional. Specifying a **traffic group** allows the related data traffic to be prioritized using a shaping configuration. The value in the field **Outgoing DSCP** allows other devices in the network to classify the related packets and to handle them in the configured manner.

Desktop connections

These settings affect the data traffic relating to the desktop connection that is being edited. The setting options for desktop connections behave like those for NAT settings: They can be made both for the entire desktop connection and for individual rules within this connection. The settings in both those cases are made via the **Traffic Shaping** tab (either at the connection or rule level). In the rule list, the checkboxes in the second column (TS) can be used to see and adjust whether the settings on the connection level should be used or not.


Connection

✓ Saved version

eth1 LAN Connection — WAN

Description:

Traffic Group: Office

Outgoing DSCP: CS0 (Standard)

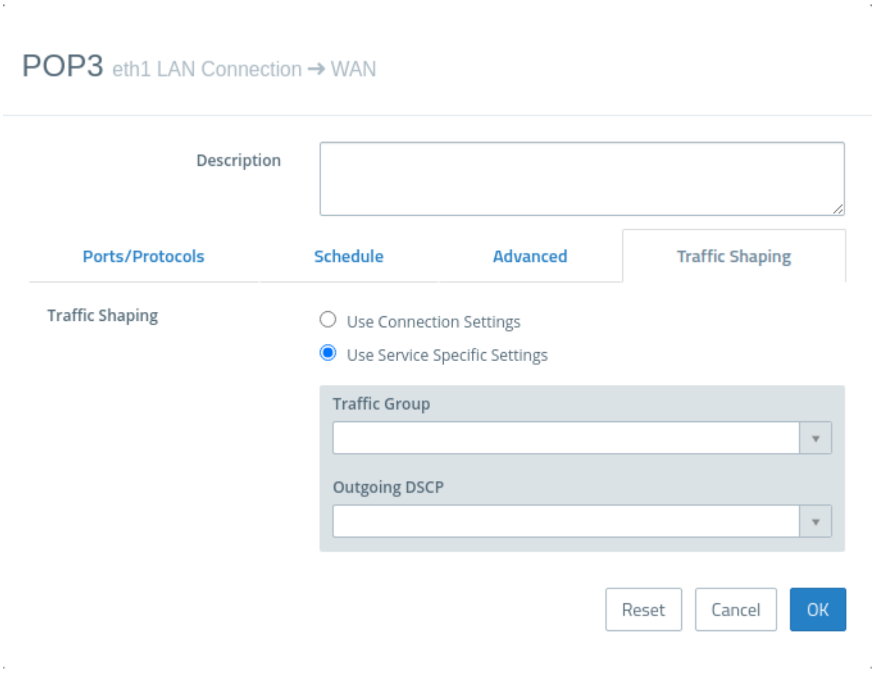
Numeric Value: $000000_2 \cdot 00_{16} \cdot 0$

Figure 1: Desktop connection > Traffic Shaping

On the **Traffic Shaping** tab you can configure the traffic shaping settings for the traffic on the selected connection:

Input box	Description
Traffic Group	Optionally select the name of a traffic group. This applies the rules defined for this group to traffic on this connection. See also *Traffic shaping* on page 5. ⓘ If it is a route-based IPsec tunnel, traffic within a tunnel can be prioritized using a custom shaping configuration.
Outgoing DSCP	From the list, select an optional DSCP value for outbound data traffic. The list contains the designations from the relevant RFCs (e.g. "CS0") and the group (e.g. "Default"). Also, the value is numerically represented in various bases (binary, hexadecimal, and decimal). The list can be searched according to these representations, so that you can quickly find the desired value regardless of your preferred representation.

These settings for the connection can then be used in a firewall rule or overwritten there by service-specific settings.


POP3 eth1 LAN Connection → WAN

Description

Traffic Shaping
○ Use Connection Settings
● Use Service Specific Settings

Traffic Group

Outgoing DSCP

Figure 2: Firewall rule > Traffic Shaping

The tab for the settings under **Traffic Shaping** has the following options:

Input box	Description
Traffic Shaping	Choose from the following options: › **Use Connection Settings** – This setting applies the traffic shaping settings made on connection level. See *Desktop connection settings*. › **Use Service Specific Settings** – This setting allows you to adjust the settings for traffic shaping for each service. The settings described below are displayed for this purpose.
Traffic Group	Optionally select the name of a traffic group. This applies the rules defined for this group to traffic on this connection. See also *Traffic shaping* on page 5. ⓘ If it is a route-based IPsec tunnel, traffic within a tunnel can be prioritized using a custom shaping configuration.
Outgoing DSCP	From the list, select an optional DSCP value for outbound data traffic. The list contains the designations from the relevant RFCs (e.g. "CS0") and the group (e.g. "Default"). Also, the value is numerically represented in various bases (binary, hexadecimal, and decimal). The list can be searched according to these representations, so that you can quickly find the desired value regardless of your preferred representation.

IPsec connections and templates

Under **VPN** > **IPsec** > **Connections** or **VPN** > **IPsec** > **Templates** you can use the traffic shaping rules for IPsec connections or IPsec connection templates.

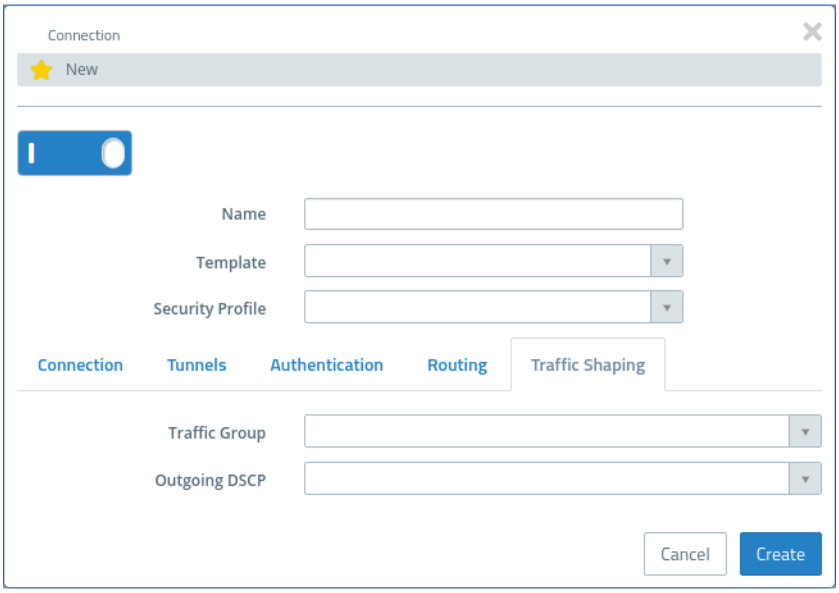


Figure 3: VPN > IPsec > Connections

In the **Traffic Shaping** tab you modify the following fields:

Input box	Description
Traffic Group	Optionally select the name of a traffic group. This applies the rules defined for this group to traffic on this connection. See also *Traffic shaping* on page 5. ℹ If it is a route-based IPsec tunnel, traffic within a tunnel can be prioritized using a custom shaping configuration.
Outgoing DSCP	From the list, select an optional DSCP value for outbound data traffic. The list contains the designations from the relevant RFCs (e.g. "CS0") and the group (e.g. "Default"). Also, the value is numerically represented in various bases (binary, hexadecimal, and decimal). The list can be searched according to these representations, so that you can quickly find the desired value regardless of your preferred representation.

App routing profiles

This item contains the settings not on a separate tab, but directly at the top level of the editor for an app routing profile under **UTM** > **Application Management** > **Routing Profiles**.

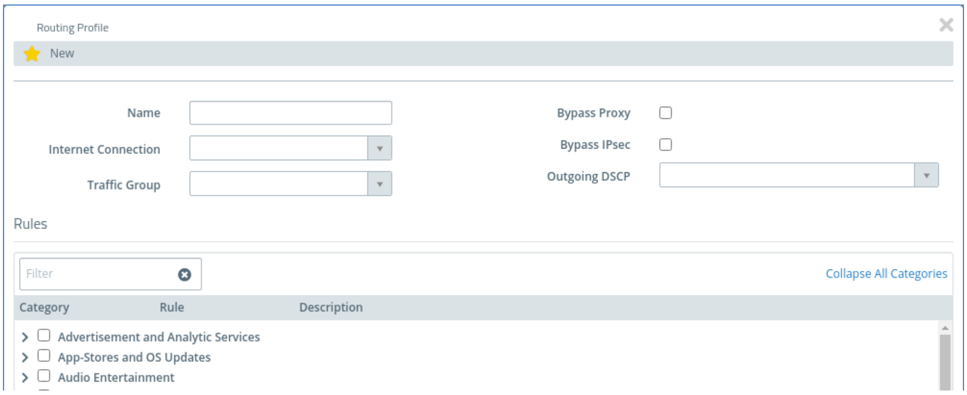
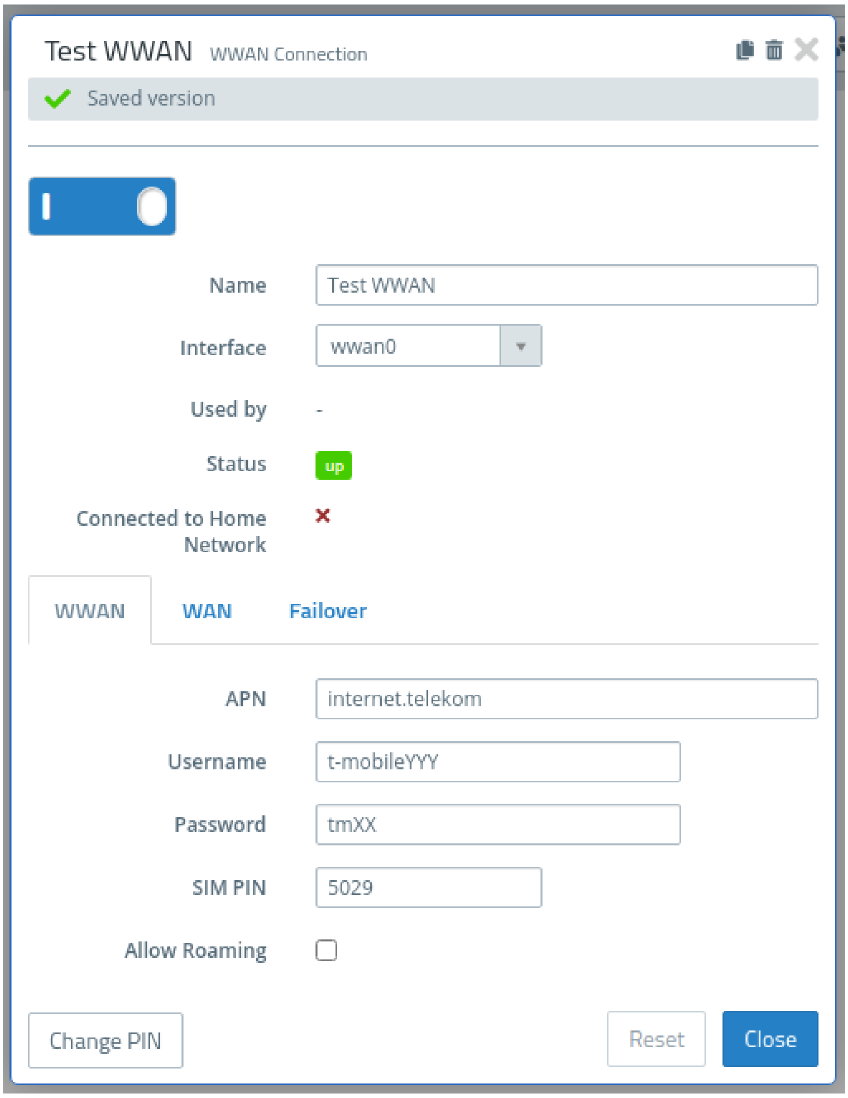


Figure 4: UTM > Application Management > Routing Profiles

Input box	Description
Traffic Group	Optionally select the name of a traffic group. This means that the rules defined for this group are applied to the traffic that the application filter has assigned to the rules that were selected in the routing profile. The data traffic must first also correspond to the desktop connection that uses the edited app routing profile. See also *Traffic shaping* on page 5.
Outgoing DSCP	From the list, select an optional DSCP value for outbound data traffic. The list contains the designations from the relevant RFCs (e.g. "CS0") and the group (e.g. "Default"). Also, the value is numerically represented in various bases (binary, hexadecimal, and decimal). The list can be searched according to these representations, so that you can quickly find the desired value regardless of your preferred representation.

3 WWAN

As of LCOS FX version 10.8, a new line below the status for WWAN connections (**Network** > **Connections** > **WWAN Connections**) now also shows the current roaming status, i.e. whether the connection is currently established to the home network or not.



Test WWAN WWAN Connection

✓ Saved version

Name: Test WWAN

Interface: wwan0

Used by: -

Status: up

Connected to Home Network: ✗

APN: internet.telekom

Username: t-mobileYYY

Password: tmXX

SIM PIN: 5029

Allow Roaming: ☐

Figure 5: Network > Connections > WWAN Connections

Input field	Description
Connected to Home Network	Shows the roaming status of the connection or whether the connection is currently established to the home network or not.

4 BPJM module

As of LCOS FX version 10.8, it is possible to block websites via the URL / Contentfilter using the BPJM module. The BPJM module is published by the german Federal Agency for the Protection of Children and Young People in the Media and blocks websites that may not be made accessible to children and young people in Germany. This is especially important for schools. This is realized via a separate Contentfilter category.