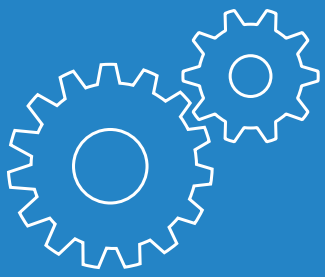
SECURE. NETWORKS.

LANCOM Firewall Jump Start



LANCOM
Systems

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.

Google Chrome™ is a registered trademark of Google LLC.

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

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names or descriptions used may be trademarks or registered trademarks of their owners.

Subject to change without notice. No liability for technical errors 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 made available upon request.

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

Wuerselen, 09/2021

Table of contents

Introduction

Thank you for purchasing a LANCOM Firewall Jump Start. This document informs you about the contents of the LANCOM Firewall Jump Start. It is intended for buyers of a Firewall Jump Start voucher, as well as for interested parties. After general notes in this chapter, the following chapters will deal with the exact contents and the network scenarios covered by the LANCOM Firewall Jump Start.

Remote support for initial setup

LANCOM Firewall Jump Start offers competent support for the initial setup of your LANCOM R&S®Unified Firewall. No previous experience with firewalls is required. An experienced technician will set up your firewall with you and guide you during a remote session through the initial setup process of a scenario predefined by LANCOM, provide you with best practice knowledge and demonstrate how to activate UTM functions such as the application filter and antivirus functions, among other things.

Target group

- You have network knowledge, but no prior knowledge of LANCOM R&S®Unified Firewall products and their UTM features.
- You need support for the initial setup of your LANCOM R&S®Unified Firewall - from integration into the network to a firewall that runs with a standard configuration.
- You would like an introduction to the functions of your new LANCOM R&S®Unified Firewall, or you have run through the wizard and are wondering: what next?

If any of the above points apply, we recommend booking our Firewall Jump Start service. This involves setting up your LANCOM R&S®Unified Firewall from scratch together with an expert via remote maintenance. If, on the other hand, it is necessary to extend the configuration of a firewall already integrated in the network, we recommend booking the LANCOM Config Service.

Tabular overview of the LANCOM Firewall Jump Start variants

		Smart	Enterprise
Setup	Estimated time	approx. 90 min.	approx. 4 hrs
	Simple network scenarios*	✓	✓
	Complex network scenarios*	—	✓
	Cluster	—	✓
	HTTPS proxy	✓	✓
	Antivirus	✓	✓
	IDS or IPS	✓	✓
	LMC integration	—**	✓
	Command Center integration	—	✓
	E-mail proxy	—	✓
	Individual paket filter rules	—	✓
	VPN connection(s)	—***	✓
Demonstration	Application filter	✓	✓
	Content filter	✓	✓
	URL filter	✓	✓
Completion	Configuration backup	✓	✓
	Information about updates	✓	✓
	Further help (support structure)	✓	✓
	Final report	—	✓

* further details see chapter “Description of the network scenarios” on page 11

** Monitoring only

*** Redirection to internal VPN gateway only

Procedure of the LANCOM Firewall Jump Start

1. **Purchase a LANCOM Firewall Jump Start voucher**
   The purchase of this service is only possible directly via our homepage. You help us by telling us the approximate time frame for the remote appointment when you place your order. After we receive your order, we will coordinate a preliminary technical meeting for you. One of our Jump Start technicians will contact you and advise you regarding the service. The topic of this conversation will be your individual requirements and determining which network scenario is suitable for you. Click here for the order form: https://www.lancom-systems.com/service-order/

2. **Redeem the purchased voucher with us**
   After the preliminary technical meeting, you will receive a voucher number from us. When you have your voucher number, please call us on +49 (0) 2405 49 93 6-210 and we will send you a questionnaire requesting relevant information for the remote appointment. As soon as we have the completed questionnaire, it will be made available to the responsible technician.

3. **Making an appointment with the technician**
   The technician will contact you within five business days (Monday to Friday) to arrange a time for the remote appointment.

4. **Performing the LANCOM Firewall Jump Start**
   The technician will contact you on the agreed date. Together with you, he will configure your LANCOM R&S®Unified Firewall and provide subsequent instruction.
   Once the configuration work is complete, the technician will prepare a final report for you and make it available to you. The final report is stored at LANCOM Systems for a period of 60 days.

Provision of services

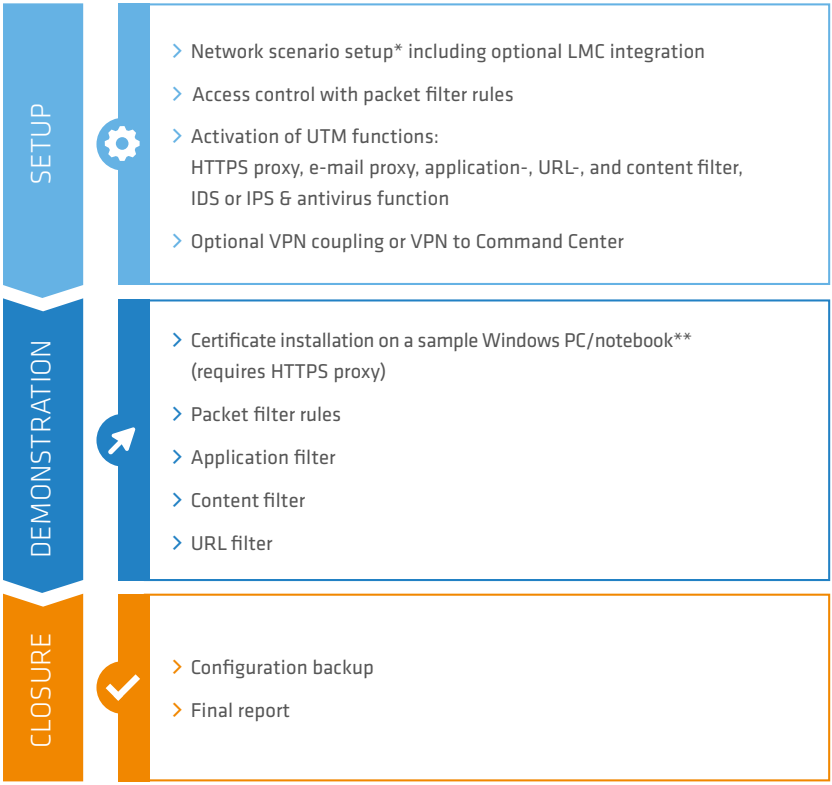
Depending on availability, the LANCOM Firewall Jump Start services are provided by a technician from LANCOM Systems or a subcontractor. In this case, please let us know whether the subcontractor may contact you after the LANCOM Firewall Jump Start services have been provided, e.g. to offer you additional services outside the LANCOM Firewall Jump Start.

Contact

If you need advice on the feasibility of your project in advance or have general questions about the LANCOM Firewall Jump Start services, please contact us using the following details. Please also use these contact details if problems or queries arise during the handling process.
Phone: +49 (0) 2405 49 93 6-210
E-mail: services@lancom.de

Scope of services

This chapter gives you an overview of the services included in the LANCOM Firewall Jump Start and the provisioning requirements. In addition to the features, chapter "Requirements for the remote technician appointment" on page 10 describes the necessary preparations for the actual remote appointment.



*Predefined network scenarios by LANCOM Systems
**Must be provided by customer

Figure 1: Firewall Jump Start, technical contents

Product features

- Remote session for initial setup of a LANCOM R&S®Unified Firewall (corresponds to approx. 90 minutes for Firewall Jump Start Smart or 4 hours for Firewall Jump Start Enterprise)
- Setting up a scenario suggestion predefined by LANCOM (see chapter "Description of the network scenarios" on page 11)
- Provision of best practice knowledge on firewall elements such as the setup wizard, user interface, UTM functions, and monitoring & statistics
- Introduction of the license manager and the update function of the firewall
- Integration of the firewall into your existing LANCOM Management Cloud project or Command Center installation (optional)*
- Final report on completed configurations*
- Provision of a backup configuration file
- Provision of the service by LANCOM or a qualified subcontractor (depending on availability)

Exclusion of benefits

- Services that were not agreed in the context of the LANCOM Firewall Jump Start (see chapter "Scope of services" on page 8)
- Development of scripts
- Integration in third-party tools, e.g. for monitoring or configuration backup
- Troubleshooting network problems
- Activities outside business hours from 08:00 a.m. to 4:30 p.m.
- Configuration of dynamic routing protocols such as RIP, BGP, and OSPF
- Subsequent supervision of the network
- Extension of an existing configuration of the LANCOM R&S®Unified Firewall
- Execution of data and host migrations
- Configuration of other devices or appliances
- Any work related to the creation and editing of virtual machine settings

* Firewall Jump Start Enterprise only

Requirements for the remote technician appointment

- The responsible technical contact person has knowledge of the existing network and administrative access to all relevant network components on site
- Access to a test device with Windows operating system for later certificate installation (if the HTTPS proxy or UTM features should be activated)
- Access to a computer / notebook with wired access to the network and the LANCOM R&S®Unified Firewall including installed TeamViewer client
- Access to the web interface of the LANCOM R&S®Unified Firewall (see LANCOM KnowledgeBase)
- Use of the current LCOS FX firmware (see LANCOM KnowledgeBase)

Description of the network scenarios

As part of the LANCOM Firewall Jump Start, your LANCOM R&S®Unified Firewall is integrated into an existing network. This chapter deals with the four available network scenarios. Each of the scenarios listed here is provided with a link to a LANCOM KnowledgeBase article in which you can find further information on the scenario.

- Scenario A - Serial connection
- Scenario B - Stand-alone operation
- Szenario C – Transparent bridge mode
- Szenario D – HA cluster with two LANCOM R&S®Unified Firewalls *

In cases without a LANCOM router, an appropriate alternative device must be used. In this context, observe the requirements for network configuration. You can refer to the configuration description of the linked KnowledgeBase documents for more information. Please note that the LANCOM Firewall Jump Start cannot be used to configure devices from other manufacturers!

* Firewall Jump Start Enterprise only

Notes on other network devices

LANCOM routers

If your gateway / router is a LANCOM device, we will be happy to adapt its configuration. The scope is limited to the adjustments required for integration. The objective is to put your LANCOM R&S®Unified Firewall into operation. Additional configuration adjustments, such as creating additional networks (for VoIP telephony, for example), are not part of the LANCOM Firewall Jump Start. The prerequisite for this is that the LANCOM router is still within the LANCOM software lifecycle management.

Products of a third-party manufacturer

Third-party network devices cannot be configured by the remote technician. To avoid delays, these must be set up in advance.

Scenario A - Serial connection

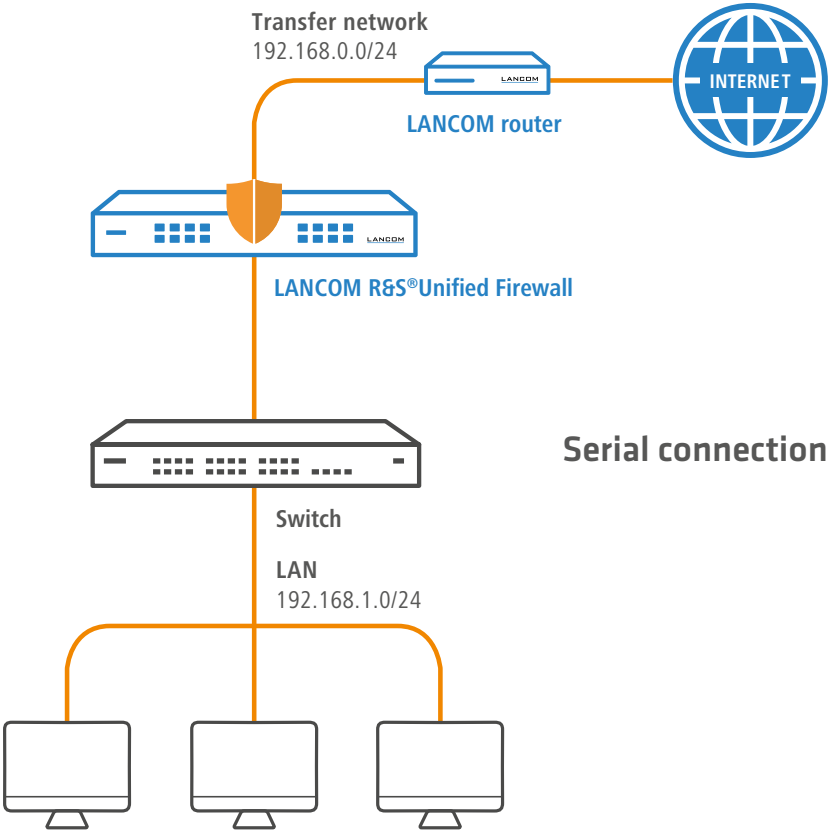


Figure 2: Scenario A - Serial connection

In this scenario it is assumed that a LANCOM router establishes the connection to the Internet. The LANCOM R&S®Unified Firewall is located in a transfer network of the upstream router. The LANCOM R&S®Unified Firewall is the Internet gateway for each of the local networks.

Scenario B - Stand-alone operation

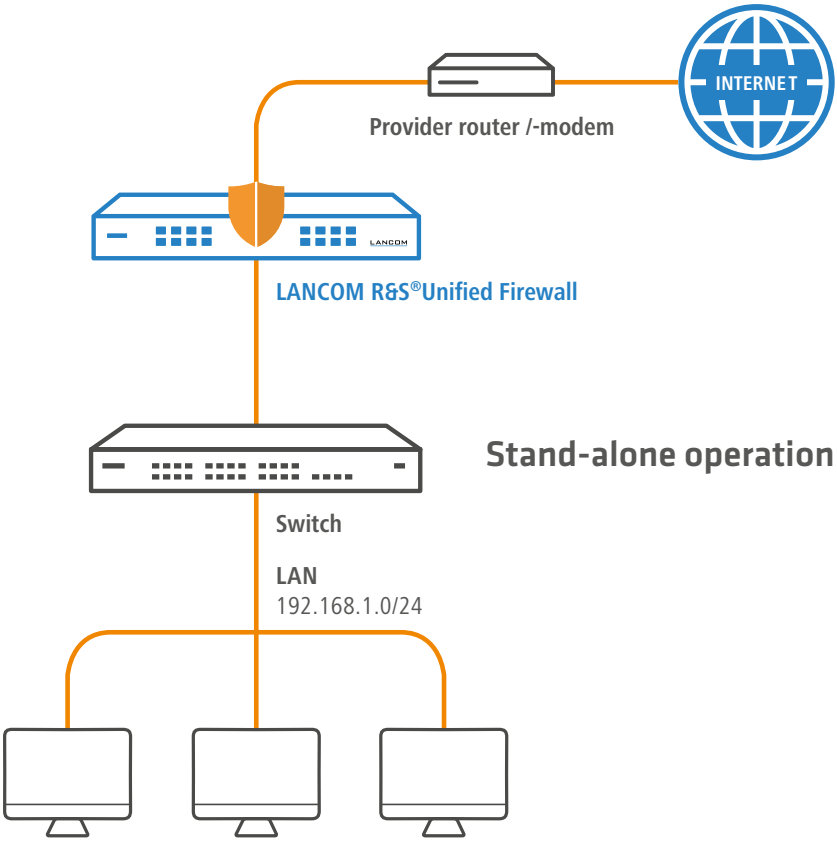


Figure 3: Scenario B - Stand-alone operation

The scenario described here corresponds as far as possible to the serial connection. A modem or router in bridge mode is used in front of the LANCOM R&S®Unified Firewall.

Scenario C - Transparent bridge mode

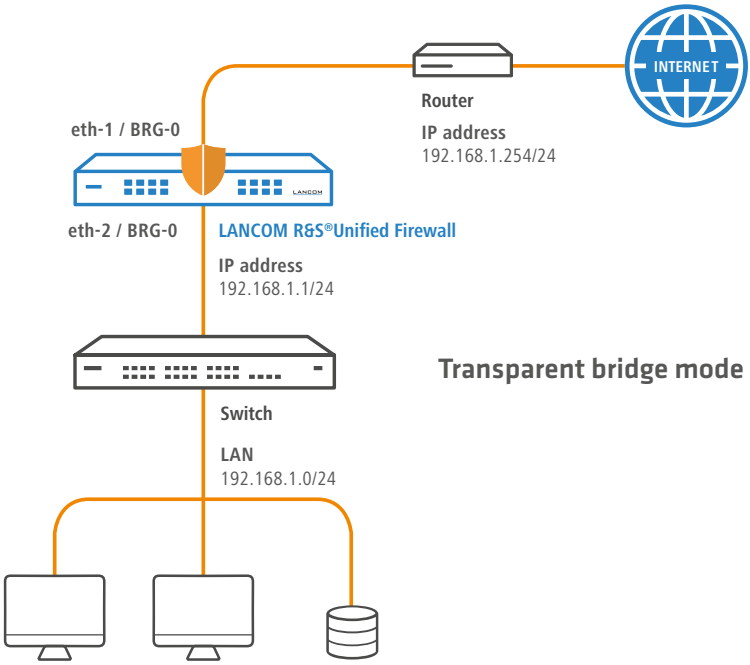


Figure 4: Scenario C - Transparent bridge mode

When operating the LANCOM R&S®Unified Firewall in 'Transparent Bridge Mode', the firewall is connected at layer-2 level between the gateway / router and the existing network (switch). No changes are necessary within the network configuration of the clients. The existing gateway / router remains in this role.

In this scenario, you can use all the firewall UTM functions that do not require routing. Topics such as VPN and routing between networks are always handled by the gateway / router. Likewise, there is no need to integrate the LANCOM R&S®Unified Firewall into the LMC.

Notice: Transparent bridge mode will only be compatible with VLAN networks with a future LCOS FX firmware.

Scenario D -
HA cluster with two LANCOM R&S®Unified Firewalls

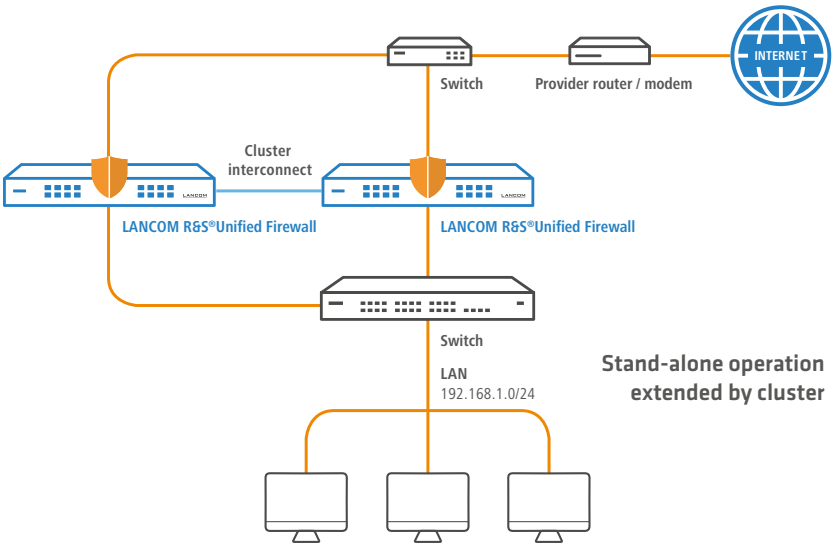


Figure 6: HA cluster with two LANCOM R&S®Unified Firewalls

Scenarios A and B can be optionally extended with high availability in the form of the cluster function with two devices as part of Firewall Jump Start Enterprise. The first firewall is active, the second remains in standby mode and only takes over operation if the first device in the cluster fails. After setting up the cluster once, there is no further configuration on the standby device – the configuration is automatically synchronized between both firewalls. A license (functional license or Service Pack 24/7) is only recommend for the active device. The licenses are automatically transferred to the second device. More information can be found in the LCOS FX user manual in the chapter "High Availability".

The following requirements must be observed:

- Both R&S®Unified Firewalls must be the same model.
- The LCOS FX firmware used must be the same on both devices.
- For the Cluster Connect connection, one free Ethernet port is required per device.
- The cabling of the Ethernet ports must be identical on the LAN and WAN side.
- On the WAN side, a switch is recommended between the upstream router/ modem and the Unified Firewall (see Figure 6).
- There must be a basic or full license for the active firewall.
- Cluster scenarios cannot be implemented in connection with the LMC.

Limitations with the different scenarios

Depending on the network scenario used, there may be restrictions on the use of functions of the upstream router or the LANCOM R&S®Unified Firewall. During the preliminary meeting, the technician will ask you about your scenario and advise you accordingly.

Restrictions for the different scenarios

Depending on the network scenario used, there may be limitations on the use of functions of the upstream router or the LANCOM R&S®Unified Firewall. The following table shows which functions can be used in the individual network scenarios. If you have any further questions on this topic, please clarify them in a preliminary discussion to make an appointment with the responsible technician.

Scenario / Usage of	Public Spot on the LANCOM router	VPN on the upstream router	VPN on the LANCOM R&S®Unified Firewall
A - Serial connection	not possible	possible*	possible*
B - Stand-alone	-	-	possible
C - Layer-3 loop**	possible	possible	not possible***
D - Layer-3 loop via redirect**	possible	possible	not possible***

Table 1: Usable services

* VPN either via router or R&S®Unified Firewall

** Firewall Jump Start Enterprise only

*** Conversion possible, but not part of the Firewall Jump Start Service