LANCOM Systems

Secure User Guidance

for LANCOM Business VPN Router

‘LANCOM 1900EF’

with LANCOM Systems Operating System

‘LCOS 10.32.0029 PR’

and IPsec VPN

Version 1.25
Release

Document History

Date	Version	Editor	Changes
11.04.2019	1.0	SGuddat	First Document Release
21.05.2019	1.10	SGuddat	Added new content: Deletion of secondary firmware, Completion of Device Configuration Changed contents: HTTPS settings, SSHv2 settings, SNMPv3 settings
23.09.2019	1.20	SGuddat	Changed TOE Suggested changes out of BSZ Kick-off
21.01.2021	1.25	SGuddat	Suggested changes out of BSI Pilot

Table of Contents

General Description

This document is the Secure User Guidance for the BSZ certification of the "LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN" (Target of Evaluation, TOE) at the BSI. This document describes the requirements to operate the TOE in a secure manner. Deviations from these requirements are subject to the risk management of the administrator.

Disclaimer

This product is targeted at professional users who have the experience and knowledge to operate network components in a secure manner.

Documentation

Device Documentation

Beside this Secure User Guidance there are additional manuals available. Those documents can be downloaded from the addresses below.

- Reference Manual

  ftp://ftp.lancom.de//Documentation/LCOS/Reference Manual/MA_LCOS-1032-REL-Reference-Manual_EN.pdf

- Menu Reference

  ftp://ftp.lancom.de//Documentation/LCOS/Menu Reference/MA_LCOS-1032-REL-Menu-Reference_EN.pdf

- Installation Guide

  ftp://ftp.lancom.de/Documentation/Installation-Guide/IG_LCOS-devices_EN.pdf

- Hardware Quick Reference

  ftp://ftp.lancom.de/Documentation/Hardware-Quick-Reference/HWS_1900EF_EN.pdf

Note: Within this user guidance there might be references to other documentations like the reference manual. In case of references to configurations accomplished by “LANconfig”, content and paths can be used for the web-based installation described in this document as well.

Acronym Table

Acronym table	
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
CLI	Command Line Interface
DoS	Denial-of-service
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection/Prevention Services
IP	Internet Protocol
IPsec	IP security
LAN	Local Area Network
LCOS	LANCOM Systems Operating System; the operating system of LANCOM routers
LTE	Long Term Evolution
NAT	Network Address Translation

PC	Personal Computer
RFC	Request for Comments (IETF Standard)
SCP	Secure Copy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
VPN	Virtual Private Network
WEBconfig	Web-based management interface

Environment

Preparation of the Environment

The TOE has to be placed in a secure environment (e.g. server room) with no physical access possible by any unauthorized person. Only the administrator of the TOE must have physical access. He also has to make sure that the connection to an untrusted network is only controlled by the TOE and that the computer used for TOE configuration is trustworthy. The administrator must ensure that any unintended bypass is prohibited (e.g. by preventing physical access and organizational means).

Configuration

WEBconfig

The TOE contains two ways to configure device settings when logged in via a web browser. The first one (WEBconfig1) is based on the device CLI and allows to change most settings in the same way as the CLI. The second (WEBconfig2) is a more user and category-based way which therefore contains less configuration options. Both ways are used within this documentation, note the respective paths in the upcoming table entries below.

WEBconfig	
WEBconfig1	`Configuration path:` **(LCOS Menu Tree => ……)**
WEBconfig2	`Configuration path:` **(Configuration => ……)**

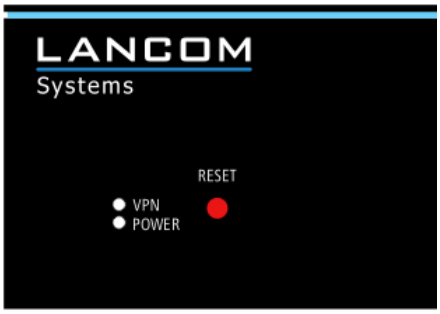
Firmware Download

Before starting with the initial configuration, it is mandatory to update the device to the firmware LCOS 10.32 PR (the firmware can be downloaded from the LANCOM homepage via: https://www.lancom-systems.com/downloads/). Once downloaded the administrator has to make sure that the downloaded file has the same SHA256 checksum as listed below:

SHA256 hash sum	
File	`LC-1900EF-10.32.0029-PR.upx`
SHA256 sum	`ab22d3767f6e617b01c09869ef5b126403449a9b48e8e9e67ebb11db56b5c87b`

Initial Configuration

To connect to the web interface of the TOE the administrator has to follow the steps mentioned in the “Installation Guide -> Configuration via WEBconfig” which is being shipped with the product (or can be downloaded via the link mentioned at “Device Documentation”). It is mandatory to do the initial configuration via a single configuration device (e.g. notebook) and with no other network or device connected. Before starting with the device configuration, it is mandatory to do a device reset. To do the device reset, use a small paperclip, click and hold the reset button on the front of the device (below the product name and next to the front LEDs) for at least 5 seconds. The reset is completed when all LEDs are glowing red. Now you can remove the paperclip and wait for the device to boot up. Once you are physically connected to the TOE open up a web browser and connect to the device configuration page via HTTPS (it is mandatory to use HTTPS only whenever a web browser is used to access the device). Depending on the pre-installed device firmware you might have to click on “Terminate this wizard” followed by “Back to entry page” or hit enter when being asked for a password. In some cases, it might be necessary to configure a device password afterwards, if this is the case then click on “Configure device password”, create a temporary password and click on “Apply” followed by “Back to entry page”. Now find on the left menu “File management” and click on “Perform a Firmware Upload”, select the downloaded firmware file



and click on “Start Upload”. After the firmware update completed and the device finished rebooting, it is mandatory to do a device reset again (click and hold reset button again). After the reset is completed connect to the web page of the device, there you will see the start-up wizard again. Now please follow the steps and make sure to set the following values:

Start-up wizard		
Device name	e.g. 1900EF	
Password	********	Create a strong password (i.e. at least 8 characters containing alphabetic, numeric and special characters).
Device access	Local net	Set access to LAN or LAN+ (only via VPN).
DHCP	Server	Keeping “server” is recommended to most customers.
IP-Address **Net mask**	e.g. 172.16.1.1 e.g. 255.255.255.0	Enter designated IP of the device.
Time configuration	Time zone Summer time Time server	It’s recommended to use the predefined values. If necessary, please change accordingly.
Layer-7 detection	No	Disable the layer 7 app detection.
LCOS auto update	No automatic updating	Choose “No automatic updating” to manually choose which update to install.
LANCOM Management Cloud	No	It is mandatory to deactivate the LMC feature by deselecting the checkbox.

After completing the initial configuration, it is mandatory to delete the secondary firmware which was previously installed on the device. To do that connect to the device webpage via HTTPS again, log in, and click on the left page on “LCOS Menu Tree -> Firmware -> Table-Firmsafe”. There select the inactive firmware and click on the red X to delete the preinstalled firmware followed by hitting the “Delete” button at the bottom of the page.

Access Rights – Protocols (Access ways)

After the start up wizard has been completed it is mandatory to change the access rights as listed below:

Mandatory access rights (Configuration => Management => Admin => Access rights – Protocols (Access ways))		
From a LAN interface	TELNET	Set TELNET to “denied”
	TELNET OVER SSL	Set TELNET OVER SSL to “denied”
	SSH	Set SSH to “allowed”
	TFTP	Set TFTP to “denied”
	SNMPv1/v2	Set SNMPv1/v2 to “denied”
	SNMPv3	Set SNMPv3 to “allowed”
	HTTP	Set HTTP to “denied”
	HTTPS	Set HTTPS to “allowed”
From a WAN interface	TELNET	Set TELNET to “denied”
	TELNET OVER SSL	Set TELNET OVER SSL to “denied”
	SSH	Set SSH to “only via VPN” or “denied”
	TFTP	Set TFTP to “denied”
	SNMPv1/v2	Set SNMPv1/v2 to “denied”
	SNMPv3	Set SNMPv3 to “only via VPN” or “denied”
	HTTP	Set HTTP to “denied”
	HTTPS	Set HTTPS to “only via VPN” or “denied”
Through a WLC tunnel (WLAN)	TELNET	Set TELNET to “denied”
	TELNET OVER SSL	Set TELNET OVER SSL to “denied”
	SSH	Set SSH to “denied”
	TFTP	Set TFTP to “denied”
	SNMPv1/v2	Set SNMPv1/v2 to “denied”
	SNMPv3	Set SNMPv3 to “denied”
	HTTP	Set HTTP to “denied”
	HTTPS	Set HTTPS to “denied”

Unused protocols should be set to “denied” as well. The administrator has to make sure that only HTTPS / SSHv2 is used to manage the TOE and that only SNMPv3 is used to monitor the status of the TOE.

Access Rights - Protocols (Web server services)

Additionally, it is mandatory to disable the HTTP access for WEB services.

Mandatory access rights (Configuration => Management => Admin => Access rights – Protocols (Web server services))		
From a LAN interface	HTTP port	Set HTTP port to “disabled”.
From a WAN interface	HTTP port	Set HTTP port to “disabled”.
Through a WLC tunnel (WLAN)	HTTP port	Set HTTP port to “disabled”.

Telnet Configuration

Make sure to disable the Telnet settings like listed below:

Mandatory Telnet setting (LCOS Menu Tree => Setup => Config)		
Telnet-Operating	No	It is mandatory to set “Telnet-Operating” to “no”.

Telnet-SSL Configuration

Make sure to disable the Telnet-SSL settings like listed below:

Mandatory Telnet-SSL setting (LCOS Menu Tree => Setup => Config => Telnet-SSL)		
Operating	No	It is mandatory to set “Operating” to “no”.

TFTP Configuration

Make sure to disable the TFTP settings like listed below:

Mandatory SFTP setting (LCOS Menu Tree => Setup => Config)		
TFTP-Operating	No	Set “TFTP-Operating” to “No”.

SFTP Configuration

Make sure to disable the SFTP settings like listed below:

Mandatory SFTP setting (LCOS Menu Tree => Setup => Config => SSH => SFTP-Server)		
Operating	No	Set “Operating” to “No”.

Printer Configuration

Make sure to disable the Printer settings like listed below:

Mandatory Printer setting (LCOS Menu Tree => Setup => Printer => Printer => “*”)		
Activ	No	It is mandatory to set “Activ” to “no”.

HTTP Configuration

Make sure to disable HTTP like listed below:

Mandatory HTTP setting (LCOS Menu Tree => Setup => HTTP)		
Port	0	It is mandatory to set “Port” to “0”. This will deactivate HTTP.

Further Configuration

HTTPS Configuration

It is mandatory to change the HTTPS configuration of the device to the settings listed below:

Mandatory HTTPS settings (LCOS Menu Tree => Setup => HTTP => SSL)		
Crypto-Algorithms	AES-256 AESGCM-256	Select one or more of the listed algorithms on the left side.
Elliptic-Curves	scep256r1 scep384r1 scep521r1	Select one or more of the listed elliptic curves on the left side.
Hash-Algorithms	SHA-256 SHA-384	Select one or both of the listed algorithms on the left side.
Keyex-Algorithms	DHE ECDHE	Select one or more of the listed algorithms on the left side.
Port	443	Leave to port 443 or change if desired.
Prefer-PFS	Yes	PFS must be set to yes.
Renegotiations	ignored forbidden	Renegotiations must be either set to “ignored” or “forbidden”.
Signature-Hash-Algorithms	SHA256-RSA SHA384-RSA SHA512-RSA SHA256-ECDSA SHA384-ECDSA SHA512-ECDSA	Select one or more of the listed algorithms on the left side.
Use-User-Provided-Certificate	Yes	Set this value to yes to allow user provided certificates.
Versions	TLSv1.2	Only TLSv1.2 must be used, please select accordingly.

The administrator must make sure to always connect via HTTPS whenever the device is accessed via web browser.

SSHv2 Configuration

Make sure to change the SSHv2 settings like listed below:

Mandatory SSHv2 settings (LCOS Menu Tree => Setup => Config => SSH)		
Cipher algorithms	aes256-gcm aes256-ctr aes256-cbc	Select one or more of the listed algorithms on the left side.
Compression	No	Please select NO here.
DH-Groups	Group-14 Group-15 Group-16	Select one or more of the listed DH-groups on the left side.
Elliptic-Curves	nistp256 nistp384 nistp521	Select one or more of the listed Hostkey-Algorithms on the left side.
Hostkey-Algorithms	ecdsa-sha2 rsa-sha2-256 rsa-sha2-512	Select one or more of the listed Hostkey-Algorithms on the left side.
Keepalive-Interval	60	Leave at 60.
Key-Exchange-Algorithms	diffie-hellman-group-exchange-sha256 ecdh-sha2	Select one or more of the listed Key-Exchange-Algorithms on the left side.
MAC-Algorithms	hmac-sha2-256 hmac-sha2-512	Select “HMAC-SHA2-256” and / or “HMAC-SHA2-512” as MAC-Algorithm.
Max-Hostkey-Length	8192	Leave at 8192.
Min-Hostkey-Length	2048	Minimum value is 2048, don’t use any lower value.
Operating	Yes	Leave at Yes.
Port	22	Leave at 22 or change if desired.

If you want to connect to the TOE via SSHv2 and an own private key, make sure to generate a RSA key pair with at least 2048 bit (refer to 2.14 of the reference manual for more information). To upload your public key, go to “File management” and click on “Upload Certificate or File”, then select “SSH – accepted public keys” and upload your public key. Now you can connect to the device via SSHv2 and your own private key.

SNMPv3 Configuration

To securely monitor the TOE it is mandatory to use SNMPv3 only. Please refer to the reference manual for more information about configuring SNMPv3 (19.8.2) and use the following protocol settings:

Mandatory SNMPv3 settings (Configuration => Management => Admin)		
Protocol versions	SNMPv3	Select SNMPv3 only.
SNMPv3 access settings for administrators	No	Disallow SNMPv3 access to administrators.
Enforce-Password-Rules	Yes	It is mandatory to set "Enforce-Password-Rules" to Yes. This setting must also not be deactivated afterwards.
Users	User name	Create a new entry by clicking on "add" and put in the desired user name.
	Authentication: HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	Select HMAC-SHA256 or higher.
	Password for auth: *******	Create a strong password (i.e. at least 16 characters containing alphabetic, numeric and special characters).
	Privacy: AES256	Use AES256 for SNMPv3 encryption.
	Password for priv: ********	Create a strong password (i.e. at least 16 characters containing alphabetic, numeric and special characters).
Groups	Group name	Create a new entry by clicking on "add" and put in the group name "SNMPv3-ReadOnly".
	User/Security name	Select the previously added SNMPv3 user.
	Security model	Select "SNMPv3 (USM)" as security model.
Access rights	SNMPv3-ReadOnly	Select and edit the "Default" entry with the group name "SNMPv3-ReadOnly".

	Readonly view	Set “Readonly view” to “Full-Access”.
	Readonly view(Traps)	Set “Readonly view(Traps)” to “Full-Access”.
	Write view	Set “Write view” to “other…”.
	Minimal security level	Verify that the Minimal security level is set to “Authentication and privacy”.

Firewall Configuration

Before configuring the firewall, it is mandatory that the administrator of the TOE develops a security concept on that he bases the following configuration on. It is recommended to use a “deny all” strategy (refer to chapters 8.3.6 and 8.3.7 of the reference manual for more information). For more information regarding IDS/DoS please refer to chapters 8.8 and 8.9 of the reference manual.

Besides that, the following settings have to be set:

Mandatory Firewall settings (LCOS Menu Tree => Setup => IP-Router => Firewall)		
Operating	Yes	It is mandatory to set Operating to “yes”.
Max.-Half-Open-Conns.	100	It is mandatory to set half open connections (DoS) to “100”.
DoS-Action	%d %n	It is mandatory to set the DoS-Action value to “%d %n”.
Port-Scan-Threshold	50	It is mandatory to set the Port-Scan-Threshold (IDS) to “50”.
IDS-Action	%d %n	It is mandatory to set the IDS-Action to “%d %n”.

IKEv2 Configuration

To configure a VPN connection based on IKEv2, please refer to the IKEv2 configuration (10.20.1 - 10.20.4) of the reference manual. Make sure to only configure IPv4 based connections.

Mandatory IKEv2 settings (Configuration->VPN->IKEv2/IPSec)		
Enforce Preshared Key rules	Yes	Select the checkbox to activate the password rules for preshared keys.
Encryption	Permitted DH groups: 14-16, 19-21 PFS: Yes IKE-SA Cipher list: AES-CBC-256 / AES-GCM-256 Digest list: SHA-256 / SHA-384 / SHA-512 Child-SA Cipher list: AES-CBC-256 / AES-GCM-256 Digest-list: SHA-256 / SHA-384 / SHA-512	Please use only secure and “state of the art” algorithms / protocols as listed on the left side.
Authentication	Local & remote authentication: PSK RSA Digital signature	It is mandatory to use either PSK, RSA or Digital Signature based connections. The use of Digital Signature is recommended, the use of PSK is not recommended.
	Local & Remote password:	Create a strong password (i.e. at least 32 characters containing alphabetic, numeric and special characters) when using PSK based connections. Note: If certificate-based connections are used, ensure to use proper X.509 RSA certificates with at least 2048 bit or higher.
Digital signature profile	Authentication method: RSASSA-PSS SHA-256 / SHA-384 / SHA-512	It is mandatory to use RSASSA-PSS with at least SHA-256 or higher if digital signature is used.

Lifetimes	Name: Default	It is mandatory to change the lifetimes of the entry named “Default” to the following values:
	IKE SA: seconds	86400 seconds
	IKE SA: kBytes	0 kBytes
	Child SA: seconds	14400 seconds
	Child SA: kBytes	0 kBytes

Internet Configuration

To set up an internet connection please use the internet configuration wizard (part of “Setup Wizards” in the menu tree) and follow the steps. Make sure to only create an IPv4 based internet connection.

Configuration Export

Configuration scripts or files must be secured with a strong password (i.e. at least 8 characters containing alphabetic, numeric and special characters).

Firmware Updates

It is mandatory to get information about product updates, which can be achieved by visiting the company homepage on a regular basis or by adding yourself to the product newsletter on the homepage.

Note: Updates are only allowed when a recertification with a newer firmware has been completed. Updated documents will be available then.

Completion of Device Configuration

Now after everything has been configured in a secure manner the TOE is ready to be installed in the desired environment.

Events

Event log

The event log contains messages about device logins. It is mandatory to check it on a regular basis. It is accessible via “LCOS Menu Tree > Status > Config > Event-Log”.

Syslog events

The syslog contains information about system events (e.g. connection establishments). It is mandatory to check it on a regular basis. It is accessible via “LCOS Menu Tree > Status > TCP-IP > Syslog > Last-Messages”.

Firewall events

The firewall log table contains messages about firewall events. It is mandatory to check it on a regular basis. It is accessible via “LCOS Menu Tree > Status > IP-Router > Log-Table”.

Decommissioning

Decommissioning of the TOE

To put the TOE out of operation, there are a few steps necessary. First it is mandatory to remove the TOE from any connected network by plugging out all network cables. Now, when only the power cable is left connected to the TOE, run the device reset via a small paperclip. Click and hold the reset button on the front of the TOE (below the product name) for at least 5 seconds. The reset is completed when all LEDs are glowing red. Now you can remove the paperclip and wait for the device to boot up again. Next it is mandatory to connect to the TOE via a single configuration device (e.g. notebook) and with no other network or device connected. Once you are physically connected to the TOE open up a web browser and connect to the device configuration page via HTTPS (it is mandatory to use HTTPS only whenever a web browser is used to access the device). There you have to click on “Terminate this wizard” followed by “Back to entry page”. In some cases, it might be necessary to configure a device password afterwards, if this is the case then click on on “Configure device password”, create a temporary password and click on “Apply” followed by “Back to entry page”. Now find on the left menu “LCOS Menu Tree” and click on “Status” and then on “File-System”. Now perform a secure erase by clicking on “Secure-Erase”, putting in “flash” at “Arguments” and then by clicking on “Execute”. Now the TOE has been decommissioned successfully.