SECURITY TARGET
FOR
LANCOM R&S®UNIFIED FIREWALL UF-360
WITH LANCOM SYSTEMS OPERATING SYSTEM
LCOS FX 10.11 RU4 AND IPSEC VPN

Version 1.5

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Context of this document

This document is the Security Target (ST) for the BSZ certification of the "LANCOM R&S Unified Firewall UF-360 with LCOS FX 10.11 RU4 and IPSec VPN" (Target of Evaluation, TOE) at the BSI. The configuration chosen is a typical use case of the TOE. The document itself was written by Dr. Jens Janßen and Dr. Hannes Riechmann-Thies. Review was performed by Roman Masanes Martinez. It was released by Markus Irle (Vice President Firewall & Security, LANCOM Systems GmbH). Note: This document uses gender-neutral language, especially the 'singular they' instead of the 'generic he'.

1.2 Product Identification

TOE name: “LANCOM R&S Unified Firewall UF-360”

TOE version: “LANCOM LCOS FX 10.11 RU4”

The TOE name is displayed on the front side of the device and the product label at the bottom.

The TOE version is displayed in the WebConfig at the top of the info area at the right side of the interface.

1.3 References / Acronyms

Acronym	
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
COM	Communication
DoS	Denial-of-service
DSL	Digital Subscriber Line
http	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection Services
IT	Information Technology
LAN	Local Area Network
LCOS FX	LANCOM Systems Operating System Firewall Linux
MITM	Man-in-the-middle
NAT	Network Address Translation
RFC	Request for Comments (IETF Standard)
SSL	Secure Socket Layer
ST	Security Target Document
SUG	Secure User Guidance Document

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WebConfig	Web-based Management Interface

References

RFC 4301	Security Architecture for the Internet Protocol www.rfc-editor.org/rfc/rfc4301
RFC 9110	HTTP Semantics www.rfc-editor.org/rfc/rfc9110
RFC 8446	The Transport Layer Security Protocol Version 1.3 www.rfc-editor.org/rfc/rfc8446

2. PRODUCT DESCRIPTION

2.1 General description

The LANCOM R&S Unified Firewall UF-360 offers network segmentation and secure VPN site connectivity. It has two 10G Fiber ports, 6 Gigabit Ethernet ports and works with high-speed fiber-optic connections and any external DSL or cable modems. A stateful inspection firewall segments different networks. IPSec VPN allows to connect different sites or remote clients.

2.2 Features and interfaces

2.2.1 Roles

The TOE supports two independent roles – an administrator and a user:

The administrator installs and manages the TOE. They have physical access to the TOE for the physical installation (e.g. cabling). They use management network access to configure and monitor the TOE and to update the TOE firmware. The default configuration contains one specific administrator account called admin which cannot be deleted. It is necessary to create and use personalized administrator accounts during the initial configuration.

The user communicates through the TOE. They have neither physical access nor management network access to the TOE. If allowed by the TOE's configuration, they use the Internet access, IPSec VPN, firewall and routing services of the TOE.

Additionally, there is a user called “gpadmin” on the underlying Linux system which is used to access the system via SSH or serial cable. Both methods are out of scope of this evaluation.

2.2.2 Physical interfaces

The TOE has 6 Ethernet ports, two 10G Fiber ports, a COM (serial) port and 2 USB ports:

The Ethernet ports support Gigabit Ethernet (1 Gbps). They can be used individually to connect the TOE to either local networks (e.g. LAN) or remote networks (e.g. Internet).

The 10G Fiber ports support 10 Gigabit Ethernet (10 Gbps). They can be used individually to connect the TOE to either local networks (e.g. LAN) or remote networks (e.g. Internet).

2.2.3 Logical interfaces

WebConfig

The TOE offers an HTTPS Webserver for the administration. In the default configuration this is active on all Ethernet and Fiber ports on port TCP 3438. During the initial configuration the administrator has to restrict access to the HTTPS Webserver to trusted networks.

This HTTPS server provides a graphical user interface to configure and monitor the TOE and to update the TOE firmware using a web browser. This is called the management interface or WebConfig.

Internet Access

The TOE provides the user in local networks (e.g. LANs) with access to remote networks (e.g. Internet). Detailed control over allowing and denying communication sessions can be configured by the administrator via the rule desktop visualization in the Web Config.

IPSec VPN connections

The TOE provides IPSec VPN services for the user. IPSec VPN provides confidentiality, integrity and authenticity for user data transmitted over networks (e.g. Internet) by encrypting and authenticating the user data. It can be used:

- to connect local networks on site (e.g. LANs in local company branch) with local networks on different sites (e.g. LANs in company central site) over remote networks (e.g. Internet) and/or
- to connect mobile devices (e.g. road warriors, home office workplaces) with local networks (e.g. LANs in local company branch) over remote networks (e.g. Internet).

Firewall / Routing

The TOE provides IPv4 firewall and routing services for the user. The IPv4 stateful packet inspection firewall allows or denies communication sessions according to its configuration by the administrator. When a communication session is allowed by the firewall, the path to the destination is determined by the routing service.

2.3 Product Usage

2.3.1 General concepts

The TOE is intended as a router and firewall to separate different local networks (e.g. LANs) and remote networks (e.g. Internet). The IPv4 stateful packet inspection firewall of the TOE allows or denies communication sessions to/from/over the local and remote networks (e.g. Internet) according to its configuration. In particular, it can allow or deny:

- Local communication: Users in one local network are provided with access to other local networks or specific hosts in other local networks.
- Internet access: Users in local networks (e.g. LANs) are provided with access to remote networks (e.g. Internet).
- IPSec VPN connections of Local networks (e.g. LANs in local company branch) can be connected to remote networks (e.g. LANs in remote company branches) over remote networks (e.g. Internet) using IPSec VPN, which provides confidentiality, integrity and authenticity by encrypting and authenticating the user data transmitted.
- IPSec VPN connections of Mobile devices (e.g. road warriors, home office workplaces) can be connected to local networks (e.g. LANs in local company branch) over remote networks (e.g. Internet) using IPSec VPN, which provides confidentiality, integrity and authenticity by encrypting and authenticating the user data transmitted.

2.3.2 By the administrator

The administrator of the TOE uses the management interface WebConfig to configure:

- the local networks (e.g. LANs)
- the remote networks (e.g. Internet)
- the IPSec VPN connections
- the IPv4 firewall and routing services and
- other security relevant settings.

The administrator also uses the management interface WebConfig to monitor the TOE and to update the TOE firmware. Details can be found in the Secure User Guidance (SUG) document.

2.3.3 By the user

If allowed by the TOE's configuration, the user communicates through the TOE

- from within local networks (e.g. LANs) with services in the remote networks (e.g. Internet)
- from within a local network with services in another local network
- from within local networks (e.g. LANs in local company branch) with remote company networks (e.g. LANs in remote company branches) over remote networks (e.g. Internet) using IPSec VPN connections
- from mobile devices (e.g. road warriors) with local networks (e.g. LANs in local company branch) over remote networks (e.g. Internet) using IPSec VPN connections.

2.4 Operating Environment

The TOE must only be operated in the supported combination of UF-360 with LCOS FX. Apart from that no specific hard- or software is necessary. Connected switches and devices must be compatible Ethernet (RJ45 or fiber) devices.

The TOE is intended for environments with physical access restrictions. The administrator has physical access to the TOE for the physical installation (e.g. cabling). They manage the TOE using the following protocols over IPv4:

- WebConfig: HTTP/1.1 [RFC 9110 ff.] over TLS 1.3 [RFC 8446]. Supported browsers are recent versions of Google Chrome (version 70 or newer) and Mozilla Firefox (version 63 or newer).

The user has no physical access to the TOE. If allowed by the TOE's configuration, they communicate through the TOE using the IPv4 protocol.

The IPSec VPN service uses the following protocol:

- IPSec [RFC 4301 ff.]

The product additionally provides additional network and security services that are out of scope for this ST.
In particular the following services run in the default configuration:

- TFTP (UDP, Port 69) providing some metadata about the TOE, this is restricted to local networks
- DNS (UDP/TCP, Port 53,10053) providing DNS forwarding, this is restricted to local networks
- A webservice (TCP Port 1813) providing a error page if called directly, this is restricted to local networks and used by UTM services

3. SECURITY PERIMETER

3.1 Users

For the TOE, the following users exist:

Administrator: Mapped to the administrator role. The administrator installs and manages the TOE. They have physical access to the TOE for the physical installation (e.g. cabling). They use the WebConfig to configure and monitor the TOE and to update the TOE firmware. They are allowed to establish connections to the management interfaces either from local networks (e.g. LANs), or from remote networks (e.g. LANs in remote company branches, Internet) using IPSec VPN connections to the TOE. They are authenticated via username and password.

Normal User: Mapped to the user role. This user has no physical access to the TOE. Also, this user is not allowed to use the WebConfig of the TOE, i.e. they do not have an account for the WebConfig. Normal users communicate through the TOE, if allowed by the TOE's configuration, by using the Internet access, IPSec VPN, firewall and routing services of the TOE. Normal users are identified by the source IP address and, depending on the IP protocol (e.g. TCP, UDP), the TCP or UDP source port of the first IP packet of a communication session.

Note: The notion 'normal user' is only used in this section to differentiate it from this section's topic 'Users'. In all further sections, they are simply called 'user' again.

3.2 Assumptions

For the TOE to fulfil its security properties, the following assumptions must apply:

- **Assumption.OnlyConn** – The TOE shall be the only logical and physical connection between the protected local networks (e.g. LANs) and the untrusted remote networks (e.g. Internet). Otherwise, the TOE cannot keep the networks separated on its own.
- **Assumption.PhysAcc** – The physical access to the TOE shall be limited to trustworthy personnel. Otherwise, an attacker could perform physical attacks against the TOE (e.g. attaching a hardware debugger to read or change the TOE's configuration). Additionally, an attacker could physically connect a MITM device to local networks (e.g. LANs) right next to the TOE (e.g. to perform sniffing or DNS redirecting attacks).
- **Assumption.AccBackup** – Any backup of the configuration is stored in a secure location. Access to the backup shall be limited to trustworthy personnel. Otherwise an attacker could extract sensitive configuration data from the backup.
- **Assumption.AdminNoEvil** – The administrator of the TOE shall be trustworthy personnel. Otherwise, the administrator could deliberately configure the TOE to not fulfil its security properties, e.g. allow users from remote networks (e.g. Internet) to access local networks (e.g. LANs).
- **Assumption.AdminKnowHow** – The administrator of the TOE shall be able to configure the TOE securely. Otherwise, the administrator could unknowingly configure the TOE to not fulfil its security properties, e.g. allow users from remote networks (e.g. Internet) to access local networks (e.g. LANs).
- **Assumption.AdminSecCreds** – The administrator of the TOE shall be able to securely generate administrator credentials (e.g. password) and IPSec VPN credentials (e.g. pre-shared keys, RSA keys and certificates). Otherwise, the created credentials may be not strong enough to withstand an attacker.
- **Assumption.AdminSecComp** – The administrator of the TOE shall use a secure computer for the management of the TOE. Otherwise, an attacker could attack the administrator's computer, e.g. to install a keylogger to get access to the administrator credentials or to the TOE's configuration.
- **Assumption.AdminSecAssets** – The administrator of the TOE shall put copies of the TOE's configuration and other valuable assets of the TOE in a secure place when storing them outside of the TOE. Otherwise, an attacker could try to read or change a copy of the TOE's configuration outside of the TOE.
- **Assumption.IPsecPeersTrusted** – The administrator shall configure the TOE to establish IPSec VPN connections only with other certified IPSec VPN peers (e.g. another copy of the TOE used according to this ST and the SUG, other IPSec device with thrusted phase1 credentials). Otherwise, the TOE cannot keep the IPSec VPN connections secured on its own and therefore cannot keep the local networks (e.g. LANs) separated on its own.

3.3 Assets

The TOE protects the following assets and security properties thereof:

- **Asset.TOE.Config** – TOE configuration; confidentiality, integrity, authenticity. The TOE configuration consists of the settings of the TOE, which are the TOE's default settings modified and expanded by the administrator (according to the Secure User Guidance). The TOE configuration determines (together with the TOE firmware) how the TOE fulfills its security properties. It is protected inside the TOE as well as outside of the TOE during transmission to/from the TOE. Confidentiality prevents an attacker from gaining knowledge about the TOE configuration, while integrity and authenticity prevent an attacker from changing the TOE configuration. The TOE configuration includes the certificates and private key for the WebConfig and the local side of the IPSec connections.

- **Asset.TOE.MonData** – TOE monitoring data; confidentiality, integrity, authenticity. The TOE monitoring data consists of information about (previous and current) states and events in the TOE that the TOE automatically collects and stores at runtime. The TOE monitoring data is protected inside the TOE as well as outside of the TOE during transmission from the TOE. Confidentiality prevents an attacker from gaining knowledge about the TOE monitoring data, while integrity and authenticity prevent an attacker from changing the TOE monitoring data.
- **Asset.TOE.Firmware** – TOE firmware; integrity, authenticity. The TOE firmware contains the operating system of the TOE (Linux Vanilla Kernel) and determines (together with the TOE configuration) how the TOE fulfills its security properties. It is protected inside the TOE as well as outside of the TOE during transmission to the TOE. Additionally, it is protected on the websites it can be downloaded from. Integrity and authenticity prevent an attacker from changing the TOE firmware. Confidentiality is provided inside the TOE and during the transmission to the TOE, but not on the websites it can be downloaded from, where the TOE firmware is signed but not encrypted.
- **Asset.Network.Separation** – User data; integrity, authenticity. The user stores data in IT devices connected to local networks (e.g. LANs). Additionally, the user transmits this data over the local networks (e.g. LANs). The TOE protects the user data by limiting access to the local networks (e.g. LANs) from remote networks (e.g. Internet) either between other connected local networks (e.g. LANs). Integrity and authenticity are provided automatically when the access is prevented. Integrity and authenticity prevent an attacker from changing the user data.
- **Asset.VPN.Data.** – User data; confidentiality, integrity, authenticity. The user transmits data (e.g. data containing company confidential information) between local networks (e.g. LANs in local company branch) and remote networks (e.g. LANs in remote company branches), mobile devices (e.g. road warriors, home office workplaces) or other connected local networks (e.g. LANs). The TOE transmits this user data over remote networks (e.g. Internet) protected by IPSec VPN connections. Confidentiality prevents an attacker from gaining knowledge about the user data, while integrity and authenticity prevent an attacker from changing the user data.

Note: The administrator credentials (e.g. password) are part of the TOE configuration and therefore no separate asset.

Note: The IPSec VPN credentials (e.g. pre-shared keys, RSA keys and certificates) are part of the TOE configuration and therefore no separate asset.

3.4 Threat Model: Attackers

The following attackers of the TOE are assumed in the threat model:

- **Attacker.Inet** – User in remote networks (e.g. Internet) who wants to read or change any of the Assets
- **Attacker.LAN** – User in local networks (e.g. LANs) who does not have the administrator role and wants to read or change any of the assets they don’t have access to.

3.5 Threat Model: Threats

The following threats are expected:

- **Threat.WebConfig.Access** – The WebConfig management interface is used by the attacker to read or change the TOE configuration, the TOE monitoring data or the TOE firmware.

- **Threat.WebConfig.MITM** – The WebConfig management interface is used by the administrator to read or change the TOE configuration, the TOE monitoring data or the TOE firmware. The attacker reads or changes the transmitted information as a MITM.
- **Threat.LAN.Access** – The user data is read or changed by the attacker accessing the local networks (e.g. LANs) from other networks (e.g. Internet or other local networks (LANs)).
- **Threat.IPsec.Access** – The user data is read or changed by the attacker accessing the local networks (e.g. LANs) over remote networks (e.g. Internet) after establishing IPSec VPN connections with the TOE.
- **Threat.IPsec.MITM** – The user data is read or changed by the attacker inside IPSec VPN connections as a MITM.
- **Threat.UpdateManipulation** – The attacker is able to insert manipulated firmware updates into the process

3.6 Security Functions

The following security related functions exist to counter the expected threats:

- **SecFunc.HTTPS** – The TOE implements access to the WebConfig management interface with HTTP/1.1 [RFC 9110 ff.] over TLS 1.3 [RFC 8446] (HTTPS). The protocols provide the administrator with secure login and secure access to the management interface by providing confidentiality, integrity and authenticity to the administrator credentials, the TOE configuration, the TOE monitoring data and the TOE firmware when being transmitted to/from the TOE.
- **SecFunc.IPsec** – The TOE implements IPSec VPN connections with IPSec [RFC 4301 ff.]. The protocol provides the user with secure data transmission over insecure networks by providing confidentiality, integrity and authenticity to the user data when being transmitted over untrusted remote networks (e.g. Internet).
- **SecFunc.IPsec.Log** – The TOE logs successful and unsuccessful IPSec VPN connection establishment attempts within the TOE monitoring data.
- **SecFunc.Firewall.Sessions** – The TOE implements IPv4 firewall and routing services. Using the TOE configuration (according to the SUG), they allow the user in local networks (e.g. LANs) to access remote networks (e.g. Internet), and they deny the user in remote networks (e.g. Internet) to access local networks (e.g. LANs). They also allow the user in local networks (e.g. LANs in local company branch) to access other networks (e.g. LANs in remote company branches or other separated LANs) and the user with trusted mobile devices (e.g. road warriors, home office workplaces) to access local networks (e.g. LANs in local company branch) using IPSec VPN connections.
- **SecFunc.Firewall.Sessions.Log** – The TOE logs blocked firewall sessions within the TOE monitoring data.
- **SecFunc.Mgmt.NoInet** – The TOE does not allow access to the WebConfig GUI from remote networks that aren´t connected by using IPSec VPN connection (e.g. Internet) (according to the SUG).
- **SecFunc.Auth.AdmCrds** – The TOE authenticates administrators before granting access to the WebConfig via username and password.
- **SecFunc.Auth.AdmPwdChrs** – The TOE enforces the administrator password to contain at least 8 characters from 3 of the following 4 character classes: lowercase letters, uppercase letters, digits and special characters.
- **SecFunc.Auth.AutoLogOut** – Administrators are automatically logged out from the WebConfig after 10 minutes of inactivity.

- **SecFunc.Auth.BrtFrcCtr** – Rate limiting is enforced by the WebConfig webserver per client IP. Additionally, administrator passwords are hashed using scrypt_mcf. This limits the number of login attempts due to the run time of the hash function.
- **SecFunc.FirmwareUpSign** – Firmware updates or their signature are signed by LANCOM using a LANCOM internal certificate which is signed by a LANCOM CA. The firmware checks signature and checksum before installing an update.

3.7 Threats vs. Assets

Asset	Attacker(s)	Threat(s)	Security Function(s)
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.Inet	Threat.WebConfig.Access	SecFunc.Mgmt.NoInet,
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.Inet	Threat.WebConfig.MITM	SecFunc.IPsec, SecFunc.HTTPS
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.LAN	Threat.WebConfig.Access	SecFunc.Auth.AdmCrds, SecFunc.Auth.AdmPwdChrs, SecFunc.Auth.BrtFrcCtr, SecFunc.Auth.AutoLogOut, SecFunc.Auth.Log
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.LAN	Threat.WebConfig.MITM	SecFunc.HTTPS
Asset.TOE.Firmware	Attacker.Inet Attacker.LAN	Threat.UpdateManipulation	SecFunc.FirmwareUpSign
Asset.Network.Separation	Attacker.Inet	Threat.LAN.Access	SecFunc.Firewall.Sessions, SecFunc.Firewall.Log
Asset.Network.Separation	Attacker.LAN Attacker.Inet	Threat.IPsec.Access	SecFunc.IPsec, SecFunc.IPsec.Log, SecFunc.Firewall.Sessions, SecFunc.Firewall.Log
Asset.VPN.Data	Attacker.Inet	Threat.IPsec.MITM	SecFunc.IPsec, SecFunc.IPsec.Log, SecFunc.Firewall.Sessions, SecFunc.Firewall.Log
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.LAN	Threat.WebConfig.Access	SecFunc.Auth.AdmCrds, SecFunc.Auth.AdmPwdChrs, SecFunc.Auth.BrtFrcCtr, SecFunc.Auth.AutoLogOut, SecFunc.Auth.Log
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.LAN	Threat.WebConfig.MITM	SecFunc.HTTPS

4. LIMITS OF EVALUATION

The following features of the product are out of scope for the evaluation:

- The product has a COM (serial) port that can be used to directly connect a computer to the TOE for management purposes.
- The USB port must only be used to install the initial firmware.
- The product offers SSH access (active in the default configuration, TCP port 22) which must be deactivated according to the SUG.
- The product offers TFTP (UDP port 69) so it can be found by LANCOM Systems LANConfig, this is not evaluated.
- The product offers SNMP for monitoring, SNMP is not active by default.
- The product provides advanced security mechanisms (Unified Threat Management).
- The product provides other VPN mechanisms apart from IPSec, e.g., VPN-SSL via OpenVPN.
- The product allows normal users to login for user/group specific communication rules.
- The product offers dynamic routing.