LANCOM
SYSTEMS

SECURITY TARGET
FOR LANCOM MULTI-WAN SD-WAN GATEWAY
'LANCOM 1930EF'
WITH LANCOM SYSTEMS OPERATING SYSTEM
'LCOS 10.80'
AND IPSEC VPN

Version 1.04
Release

Table of Contents

1. Introduction 3

1.1 Context of this Document 3

1.2 Product Identification 3

1.3 References / Acronyms 3

2. Product Description 6

2.1 General Description 6

2.2 Features and Interfaces 6

2.3 Product Usage 8

2.4 Operating Environment 10

3. Security Perimeter 11

3.1 Users 11

3.2 Assumptions 11

3.3 Assets 12

3.4 Threat Model: Attackers 13

3.5 Threat Model: Threats 13

3.6 Security Functions 14

3.7 Mapping 15

4. Limits of Evaluation 17

1. INTRODUCTION

1.1 Context of this Document

This document is the Security Target (ST) for the BSZ certification of the "LANCOM Multi-WAN SD-WAN Gateway 'LANCOM 1930EF' with LANCOM Systems Operating System 'LCOS 10.80' and IPsec VPN" (Target of Evaluation, TOE) in the scope "Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte" at the BSI. The configuration chosen is the typical use case of the TOE.

The document itself was written by Frank Theinen (Embedded Systems Engineer, LANCOM Systems GmbH). It was released by Simon Lindenlauf (Product Manager, 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 1930EF'

TOE version: 'LCOS 10.80.0742 SU8' / 'Ver. 10.80.0742SU8 / 07.09.2024'

The TOE name and version are displayed on the dashboard in the web-based management interface (WEBconfig). Depending on the configured web browser language (EN/DE), they are shown under:

→ 'Systeminfo' > 'Device type'

→ 'Firmware' > 'Installed version'

or

→ 'Systeminfo' > 'Gerätetyp'

→ 'Firmware' > 'Installierte Version'

The TOE name and version are also displayed in the banner of the command line interface (CLI). The TOE name is additionally printed at two locations on the physical device: on the front side and on the bottom side label.

1.3 References / Acronyms

Acronyms	
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
CLI	Command Line Interface
COM	Communication
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial-of-service
DSL	Digital Subscriber Line

ESP	Encapsulating Security Payload
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection/Prevention Services
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security
IT	Information Technology
LAN	Local Area Network
LCOS	LANCOM Systems Operating System
LPD	Line Printer Daemon
MITM	Man-in-the-middle
NAT	Network Address Translation
RFC	Request for Comments (IETF Standard)
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
SUG	Secure User Guidance
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TP	Twisted Pair
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WEBconfig	Web-based management interface

References		
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	https://tools.ietf.org/html/rfc3411
RFC 4251	The Secure Shell (SSH) Protocol Architecture	https://tools.ietf.org/html/rfc4251
RFC 4301	Security Architecture for the Internet Protocol	https://tools.ietf.org/html/rfc4301

RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
RFC 7230	Hypertext Transfer Protocol (HTTP/1.1)	https://tools.ietf.org/html/rfc7230
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3	https://tools.ietf.org/html/rfc8446

2. PRODUCT DESCRIPTION

2.1 General Description

The LANCOM Multi-WAN SD-WAN gateway 'LANCOM 1930EF' offers secure VPN site connectivity over high-performance Internet connections. It has two Gigabit Ethernet WAN ports and works with high-speed fiber-optic connections and any external DSL or cable modems. A stateful inspection firewall protects the whole network with features such as Intrusion Prevention and Denial-of-Service protection.

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 trusted network access to configure and monitor the TOE and to update the TOE firmware.
- → The user communicates through the TOE. They have no physical 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.

2.2.2 Interfaces

The TOE has 4 LAN Ethernet ports, 2 WAN Ethernet ports, a COM (serial) port and an USB port:

- → The LAN Ethernet ports support Gigabit Ethernet (1 Gbit/s). They can be used individually to connect the TOE to either trusted local networks (e.g. LAN) or untrusted remote networks (e.g. Internet).
- → The WAN Ethernet ports support Gigabit Ethernet (1 Gbit/s). They can be used individually to connect the TOE to either trusted local networks (e.g. LAN) or untrusted remote networks (e.g. Internet). Note that one of the WAN Ethernet ports is a SFP/TP combo port, and therefore has two sockets.
- → The COM (serial) port supports serial data communication (up to 115 kbit/s). It can be used to connect a computer directly to the TOE for management purposes.
- → The USB port supports USB 2.0 (480 Mbit/s). It can be used for management purposes.

The typical configuration of the TOE consists of trusted local networks connected to LAN Ethernet ports and untrusted remote networks connected to WAN Ethernet ports. Management of the TOE is done using only trusted networks. The COM and USB ports are not used. More complex configurations are possible but out of scope for this ST.

2.2.3 Management Services

The administrator can manage the TOE using the following interfaces:

- → WEBconfig: An HTTPS server provides a graphical user interface to configure and monitor the TOE and to update the TOE firmware using a web browser.
- → CLI: An SSH server provides a command line interface to configure and monitor the TOE using an SSH client. Updating the TOE firmware can be done using Secure Copy (SCP).
- → SNMP: An SNMPv3 server allows SNMP monitoring software to monitor the TOE.

2.2.4 Internet Access

The TOE provides the user in trusted local networks (e.g. LANs) with access to untrusted remote networks (e.g. Internet). If the access to untrusted remote networks uses IPv4 Network Address Translation (NAT),

- → communication sessions originating from trusted local networks are automatically allowed, whereas
- → communication sessions originating from untrusted remote networks are automatically denied.

More detailed control over allowing and denying communication sessions can be configured by the administrator in the firewall.

2.2.5 IPsec VPN Connections

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

- → to connect trusted local networks (e.g. LANs in local company branch) with trusted remote networks (e.g. LANs in remote company branches) over untrusted remote networks (e.g. Internet) and/or
- → to connect trusted mobile devices (e.g. road warriors) with trusted local networks (e.g. LANs in local company branch) over untrusted remote networks (e.g. Internet).

2.2.6 IPv4 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. Additionally, it provides Denial-of-Service (DoS) protection and Intrusion Detection/prevention Services (IDS). When a communication session is allowed by the firewall, the path to the destination is determined by the routing service.

The TOE additionally provides IPv6 protocol services that are out of scope for this ST.

2.2.7 Table of Interfaces

Physical Interface	Logical Interface	Protocol	Description	Scope of Evaluation
LAN1-4	443/TCP	HTTPS	Administrative web interface (WEBconfig)	Yes
LAN1-4	80/TCP	HTTP	Administrative web interface (WEBconfig)	No
LAN1-4	22/TCP	SSH	Administrative command line interface (CLI)	Yes
LAN1-4	22/TCP	SFTP	Administrative command line interface (CLI)	No
LAN1-4	992/TCP	TELNET over TLS/SSL	Administrative command line interface (CLI)	No
LAN1-4	23/TCP	TELNET	Administrative command line interface (CLI)	No
LAN1-4	69/UDP	TFTP	Administrative command line interface (CLI)	No
LAN1-4	161/UDP	SNMP	Administrative monitoring interface	Yes
LAN1-4	67/UDP	DHCP	Automatic configuration of devices (e.g. IP address)	Yes
LAN1-4	53/UDP	DNS	Domain name resolution	Yes
LAN1-4	123/UDP	SNTP	Simple Network Time Protocol	No
LAN1-4	515/TCP	LPD	Printserver	No
LAN1-4	9100/TCP	Raw IP	Printserver	No
WAN1-2	500/UDP	IKEv2	Negotiation of IPsec VPN connections	Yes
WAN1-2	50/IP	ESP	Data transport of IPsec VPN connections	Yes
WAN1-2	4500/UDP	IKEv2 ESP	Negotiation and data transport of IPsec VPN connections	Yes
COM			Device management in case of physical access	No
USB			Device management in case of physical access	No

2.3 Product Usage

2.3.1 General Concepts

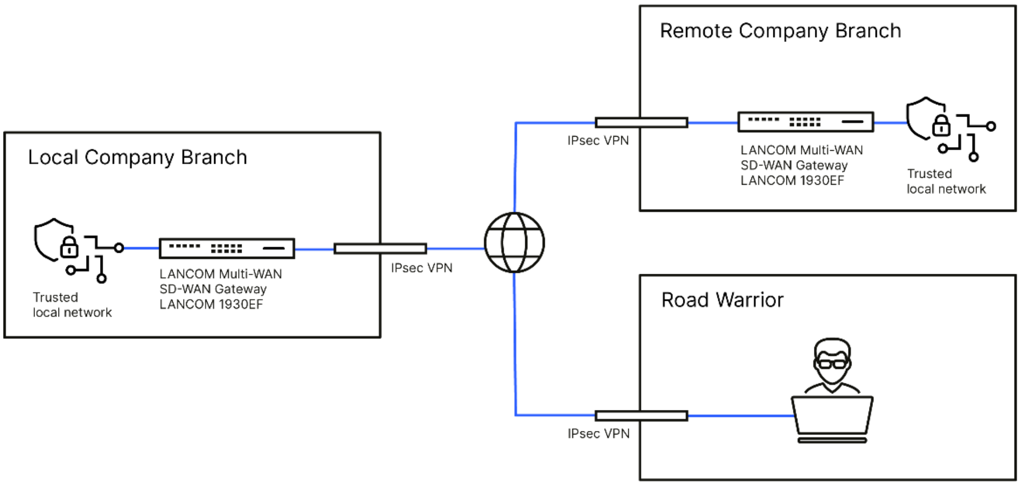
The TOE is intended as an edge router to separate trusted local networks (e.g. LANs) from untrusted remote networks (e.g. Internet). The IPv4 stateful packet inspection firewall of the

TOE allows or denies communication sessions to/from/over the untrusted remote networks (e.g. Internet) according to its configuration. In particular, it can allow:

→ Internet access: Users in trusted local networks (e.g. LANs) are provided with access to untrusted remote networks (e.g. Internet).

→ IPsec VPN connections: Trusted local networks (e.g. LANs in local company branch) can be connected to trusted remote networks (e.g. LANs in remote company branches) over untrusted 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: Trusted mobile devices (e.g. road warriors) can be connected to trusted local networks (e.g. LANs in local company branch) over untrusted 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 interfaces WEBconfig and/or CLI to configure:

→ the trusted local networks (e.g. LANs),

→ the untrusted 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 interfaces to monitor the TOE (WEBconfig, CLI and/or SNMP) and to update the TOE firmware (WEBconfig and/or CLI).

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 trusted local networks (e.g. LANs) with services in the untrusted remote networks (e.g. Internet),

→ from within trusted local networks (e.g. LANs in local company branch) with trusted remote networks (e.g. LANs in remote company branches) over untrusted remote networks (e.g. Internet) using IPsec VPN connections and/or

→ from trusted mobile devices (e.g. road warriors) with trusted local networks (e.g. LANs in local company branch) over untrusted remote networks (e.g. Internet) using IPsec VPN connections.

2.4 Operating Environment

The TOE is intended for environments with physical access restrictions and trusted local users. Remote users are either trusted or untrusted.

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

→ WEBconfig: HTTP/1.1 [RFC 7230 ff.] over TLS 1.2/1.3 [RFC 5246/8446] (HTTPS)

→ CLI: SSH [RFC 4251 ff.]

→ SNMP: SNMPv3 [RFC 3411 ff.]

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:

→ Users in trusted local networks (e.g. LANs) are trusted.

→ Users in untrusted remote networks (e.g. Internet) are untrusted in general, but are trusted if allowed by the TOE's configuration.

→ Users in trusted remote networks (e.g. LANs in remote company branches) connected using IPsec VPN are trusted.

→ Users with trusted mobile devices (e.g. road warriors) connected using IPsec VPN are trusted.

The IPsec VPN service uses the following protocol:

→ IPsec [RFC 4301 ff.]

The TOE additionally provides IPv6 protocol services that are out of scope for this ST.

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, CLI and SNMP management interfaces to configure and monitor the TOE and to update the TOE firmware. They are allowed to establish connections to the management interfaces either from trusted local networks (e.g. LANs), or from trusted remote networks (e.g. LANs in remote company branches) over untrusted remote networks (e.g. Internet) using IPsec VPN connections to the TOE. They are authenticated either via username and password or via an SSH key.

→ **Normal User:** Mapped to the user role. This user has no physical access to the TOE, and is not allowed to use the management interfaces of the TOE. They 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. They 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 fulfill its security properties, the following assumptions must apply:

→ **Assumption.OnlyConn –** The TOE shall be the only logical and physical connection between the trusted 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 trusted local networks (e.g. LANs) right next to the TOE (e.g. to perform sniffing or DNS redirecting attacks).

→ **Assumption.AdminNoEvil –** The administrator of the TOE shall be trustworthy personnel. Otherwise, the administrator could deliberately configure the TOE to not fulfill its security properties, e.g. allow users from untrusted remote networks (e.g. Internet) to access trusted 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 fulfill its security properties, e.g. allow users from untrusted remote networks (e.g. Internet) to access trusted local networks (e.g. LANs).

→ **Assumption.AdminSecCreds –** The administrator of the TOE shall be able to securely generate administrator credentials (e.g. password, SSH key) 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 trusted IPsec VPN peers (e.g. another copy of the TOE used according to this ST and the SUG). Otherwise, the TOE cannot keep the IPsec VPN connections secured on its own and therefore cannot keep the trusted 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.

→ **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. Additionally the administrator can command the TOE (in the CLI management interface) to collect tracing information. 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 (LCOS) 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 from which it can be downloaded. 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 website from which it can be downloaded, where the TOE firmware is signed but not encrypted.

→ **Asset.User.Data.LAN –** User data; confidentiality, integrity, authenticity. The user stores data (e.g. data containing company confidential information) in IT devices connected to trusted local networks (e.g. LANs). Additionally the user transmits this data over the trusted local networks (e.g. LANs). The TOE protects the user data by limiting access to the trusted local networks (e.g. LANs) from untrusted remote networks (e.g. Internet). Confidentiality, integrity and authenticity are provided automatically when the access is prevented. Confidentiality prevents an attacker from gaining knowledge about the user data, while integrity and authenticity prevent an attacker from changing the user data.

→ **Asset.User.Data.Inet –** User data; confidentiality, integrity, authenticity. The user transmits data (e.g. data containing company confidential information) between trusted local networks (e.g. LANs in local company branch) and trusted remote networks (e.g. LANs in remote company branches) or trusted mobile devices (e.g. road warriors). The TOE transmits this user data over untrusted 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, SSH key) 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 untrusted networks (e.g. Internet) who wants to read or change any of the assets

→ **Attacker.LAN –** User in trusted networks (e.g. LANs) who does not have the administrator role and wants to read or change any of the assets only the administrator role is allowed to read or change

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

→ **Threat.CLI.MITM –** The CLI 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.SNMP.Access –** The SNMP management interface is used by the attacker to read or change the TOE monitoring data.

→ **Threat.SNMP.MITM –** The SNMP management interface is used by the administrator to read or change the TOE monitoring data. 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 trusted local networks (e.g. LANs) from untrusted remote networks (e.g. Internet).

→ **Threat.IPsec.Access** – The user data is read or changed by the attacker accessing the trusted local networks (e.g. LANs) over untrusted 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.

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 7230 ff.] over TLS 1.2/1.3 [RFC 5246/8446] (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.SSH** – The TOE implements access to the CLI management interface with SSH [RFC 4251 ff.]. The protocol provides 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.SNMPv3** – The TOE implements access to the SNMP management interface with SNMPv3 [RFC 3411 ff.]. The protocol provides the administrator with secure login and secure access to the management interface by providing confidentiality, integrity and authenticity to the administrator credentials and the TOE monitoring data 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 trusted local networks (e.g. LANs) to access untrusted remote networks (e.g. Internet), and they deny the user in untrusted remote networks (e.g. Internet) to access trusted local networks (e.g. LANs). They also allow the user in trusted local networks (e.g. LANs in local company branch) to access trusted remote networks (e.g. LANs in remote company branches) and the user with trusted mobile devices (e.g. road warriors) to access trusted local networks (e.g. LANs in local company branch) using IPsec VPN connections

→ **SecFunc.Firewall.DoS.IDS** – The TOE implements an IPv4 firewall that provides Denial-of-Service (DoS) protection and Intrusion Detection/prevention Services (IDS). The DoS protection can detect and react on TCP SYN flooding, Smurf attacks, LAND attacks, Ping of Death attacks, Teardrop attacks, and Bonk attacks. The IDS can detect and react on IP spoofing and port scans.

→ **SecFunc.Firewall.Log** – The TOE logs access attempts denied by the firewall within the TOE monitoring data.

- → **SecFunc.Auth.AdmCrds** – The TOE authenticates administrators before granting access to the WEBconfig, CLI and SNMP management interfaces, either via username and password or via an SSH key (the latter only being usable in case of the CLI management interface).
- → **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.BrtFrcCtr** – The TOE counters brute-force attacks against the password by locking the login functionality of an interface for a configured amount of time after a configured number of failed login attempts.
- → **SecFunc.Auth.AutoLogOut** – The TOE automatically logs out the administrator after a configured time of inactivity.
- → **SecFunc.Auth.Log** – The TOE logs successful and unsuccessful login attempts within the TOE monitoring data.
- → **SecFunc.Mgmt.NoInet** – The TOE does not allow access to the WEBconfig, CLI and SNMP management interfaces from untrusted networks in the TOE configuration (according to the SUG).
- → **SecFunc.Mgmt.Ports** – The TOE can be configured to use non-standard TCP/UDP ports for the protocols HTTPS, SSH and SNMPv3, which are used to access the WEBconfig, CLI and SNMP management interfaces.

Note: The TOE verifies the integrity and authenticity of the received TOE firmware during a firmware update (according to Appendix 'Update Mechanism').

3.7 Mapping

The following table shows which security functions protect which assets against which threats by which attackers:

Asset(s)	Attacker(s)	Threat(s)	Security Function(s)
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.Inet	Threat.WEBconfig.Access	SecFunc.Mgmt.NoInet, SecFunc.Mgmt.Ports
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.Inet	Threat.CLI.Access	SecFunc.Mgmt.NoInet, SecFunc.Mgmt.Ports
Asset.TOE.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.Inet	Threat.CLI.MITM	SecFunc.IPsec, SecFunc.SSH
Asset.TOE.MonData	Attacker.Inet	Threat.SNMP. Access	SecFunc.Mgmt.NoInet, SecFunc.Mgmt.Ports
Asset.TOE.MonData	Attacker.Inet	Threat.SNMP. MITM	SecFunc.IPsec, SecFunc.SNMPv3

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.Config, Asset.TOE.MonData, Asset.TOE.Firmware	Attacker.LAN	Threat.CLI.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.CLI.MITM	SecFunc.SSH
Asset.TOE.MonData	Attacker.LAN	Threat.SNMP. Access	SecFunc.Auth.AdmCrds, SecFunc.Auth.AdmPwdChrs, SecFunc.Auth.BrtFrcCtr, SecFunc.Auth.AutoLogOut, SecFunc.Auth.Log
Asset.TOE.MonData	Attacker.LAN	Threat.SNMP. MITM	SecFunc.SNMPv3
Asset.User.Data.LAN	Attacker.Inet	Threat.LAN. Access	SecFunc.Firewall.Sessions, SecFunc.Firewall.DoS.IDS, SecFunc.Firewall.Log
Asset.User.Data.LAN	Attacker.Inet	Threat.IPsec. Access	SecFunc.IPsec, SecFunc.IPsec.Log, SecFunc.Firewall.Sessions, SecFunc.Firewall.DoS.IDS, SecFunc.Firewall.Log
Asset.User.Data.Inet	Attacker.Inet	Threat.IPsec. MITM	SecFunc.IPsec, SecFunc.IPsec.Log, SecFunc.Firewall.Sessions, SecFunc.Firewall.DoS.IDS, SecFunc.Firewall.Log

4. LIMITS OF EVALUATION

The following features of the TOE are out of scope for the evaluation, because they are not used in the typical use case:

→ The TOE has a COM (serial) port that can be used to connect a computer directly to the TOE for management purposes.

→ The TOE has an USB port that can be used for management purposes.

→ The TOE provides IPv6 protocol services.