Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zertifizierungsreport

BSI-DSZ-BSZ-0008-2024

zu

LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN, LANCOM LCOS FX 10.11 RU4

der

LANCOM Systems GmbH

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
bsz@bsi.bund.de
Internet: https://www.bsi.bund.de/bsz

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-BSZ-0008-2024(*)

LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN, LANCOM LCOS FX 10.11 RU4

von **LANCOM Systems GmbH**

für den Geltungsbereich
Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte

Beschleunigte Sicherheitszertifizierung

fixed time certification

Das in diesem Zertifikat genannte IT-Produkt wurde von einer anerkannten Prüfstelle nach der Evaluationsmethodologie EN 17640 „Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte“ (FiT CEM) ergänzt um Anforderungen und Interpretationen des Zertifizierungsprogramms Beschleunigte Sicherheitszertifizierung (BSZ) des Bundesamtes für Sicherheit in der Informationstechnik evaluiert.
Das Zertifizierungsverfahren wurde in Übereinstimmung mit den Anforderungen und Regeln des BSI eigenen Programms zur Beschleunigten Sicherheitszertifizierung (BSZ) durchgeführt.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 4 zu entnehmen.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 09.10.2024
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola
Abteilungsleiter

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn – Postfach 20 03 63 - D-53133 Bonn
Infoline +49 (0)800 247 1000 – Internet www.bsi.bund.de

Inhaltsverzeichnis

A Zertifizierung

1 Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produkts wird auf Veranlassung des Herstellers oder eines Vertreibers – im folgenden Antragsteller genannt – durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produkts gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produkts, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern und für Heimat
- Produktzertifizierung im BSI: Programm Beschleunigte Sicherheitszertifizierung (BSZ-Produkte) [1]
- Anerkennung von Prüfstellen im BSI: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ-Prüfstellen) [2]
- Anwendungshinweise und Interpretationen zum Schema für die BSZ (AIS B) [3]

Das Verfahren wurde im Geltungsbereich **„Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte“** der Beschleunigten Sicherheitszertifizierung durchgeführt.

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 11 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist

[2] Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

[3] Besondere Gebührenverordnung BMI (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019 (BGBl. I S. 1359), die zuletzt durch Artikel 1 der Verordnung vom 10. September 2021 (BGBl. I S. 4429) geändert worden ist

3 Anerkennungsvereinbarungen

Um die Mehrfachzertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden, besteht ein Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten der Programme CSPN (Certification de sécurité de premier niveau) und BSZ zwischen dem BSI und der französischen ANSSI (Agence nationale de la sécurité des systèmes d'information) [4]. Das Abkommen ist befristet auf zwei Jahre, d.h. bis zum 14.05.2026. Damit werden grundsätzlich alle CSPN-Zertifikate in Deutschland vom BSI und alle BSZ-Zertifikate von der ANSSI anerkannt.

Es können allerdings Zertifikate von der Anerkennung ausgenommen werden. Dies kann sowohl durch die ausstellende Seite als auch durch die anerkennende Seite geschehen.

4 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN, LANCOM LCOS FX 10.11 RU4 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluierung des Produkts LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN, LANCOM LCOS FX 10.11 RU4 wurde von TÜV Informationstechnik GmbH durchgeführt. Die Evaluierung wurde am 15. April 2024 abgeschlossen. Das Prüflabor ist eine vom BSI anerkannte Prüfstelle (ITSEF)[4].

Der Antragsteller ist: LANCOM Systems GmbH.

Das Produkt wurde entwickelt von: LANCOM Systems GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5 Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produkts. Die Ergebnisse der Zertifizierung gelten nur, wenn das Produkt unter den folgenden Bedingungen betrieben wird:

- Alle Auflagen hinsichtlich der Generierung, der Konfiguration und des Einsatzes des Produkts, die in diesem Report gestellt werden, werden beachtet.
- Das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben (Englisch: Security Target, ST) beschrieben ist.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produkts gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln, ist es erforderlich, die maximale Gültigkeit des Zertifikates zu begrenzen. Dieses Zertifikat, erteilt am 09.10.2024, ist gültig bis 08.10.2026. Die Gültigkeit kann im Rahmen einer Rezertifizierung erneuert werden.

[4] Information Technology Security Evaluation Facility

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produkts auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produkts den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produkts zur Verfügung zu stellen,
2. eine Kontaktadresse zur Meldung von potenziellen Schwachstellen durch Dritte security@lancom.de zu betreiben,
3. eingehende Meldungen bezüglich potenzieller Schwachstellen des Produkts unverzüglich zu prüfen und die Prüfung zu dokumentieren, hierzu gehört insbesondere die Prüfung der über die Kontaktadresse gemäß 2. gemeldeten Schwachstellen,
4. die Marktaufsicht des BSI unaufgefordert und unverzüglich nach Bekanntwerden und Bewertung über Schwachstellen des Produkts, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden, via Email an marktaufsicht@bsi.bund.de zu informieren. Hinweise zur sicheren Kommunikation und öffentliche Schlüssel zur Verschlüsselung der Emails finden Sie auf der Webseite des BSI unter https://www.bsi.bund.de/dok/Kontakt-MA.
5. Des Weiteren müssen Sie den Anwendern des Produkts unverzüglich kostenfrei über den im Zertifizierungsreport genannten sicheren Update-Kanal eine Fehlerkorrektur und auf Wunsch des Anwenders ergänzende Informationen zur Auswirkung der Schwachstelle zur Verfügung zu stellen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller zur Aufrechterhaltung der Vertrauenswürdigkeit eine Rezertifizierung in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Abweichungen von den Sicherheitsvorgaben und weiteren Anforderungen aufdeckt.

6 Veröffentlichung

Das Produkt LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN, LANCOM LCOS FX 10.11 RU4 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de/bsz).

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produkts angefordert werden. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand (Englisch: Target of Evaluation, TOE),
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Zusammenfassung

Der Evaluierungsgegenstand (TOE) ist eine Firewall mit dynamischer Paketfiltertechnik.

1.1 Produktbeschreibung

Das Produkt bietet Netzwerksegmentierung und sichere Standortanbindung über VPN an. Dafür verfügt es über zwei 10G-Fiber-Ports und sechs Gigabit-Ethernet-Ports. Die dynamische Paketfilter-Firewall segmentiert verschiedene Netzwerke und die Standorte können über IPsec VPN verbunden werden.

1.2 Produktidentifikation

Nr	*Typ*	*Identifier*	*Version*	*Auslieferungsart*
1	Hardware	LANCOM R&S Unified Firewall	UF-360	-
2	Software	LANCOM R&S UNIFIED FIREWALL UF-360 mit der Betriebssystemversion LANCOM LCOS FX 10.11 RU4 und IPSEC VPN	LANCOM LCOS FX 10.11 RU4	Partner Portal der LANCOM Systems GmbH[5]
3	Dokument	Security Target Lancom vom 06.09.2024	1.6	Herstellerwebseite[6]/ BSI-Webseite
4	Dokument	Secure User Guidance vom 26.07.2024	1.4	Herstellerwebseite[7]

Tabelle 1: Auslieferungsumfang des Evaluierungsgegenstands (TOE)

Der Name vom TOE wird auf der Vorderseite vom Gerät angezeigt und zusätzlich am Boden der Unterseite des Gerätes auf dem Aufkleber zu finden. Die Version vom TOE wird im oberen rechten Infobereich der Oberfläche angezeigt.

1.3 Sicherheitsfunktionen des Evaluierungsgegenstands

Die Werte, die durch den TOE geschützt werden, sind in den Sicherheitsvorgaben [06], Kapitel 3.3, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen in Kapitel 3.2, Angreifern in Kapitel 3.4 dar und Bedrohungen in Kapitel 3.5. Der TOE bietet die in Tabelle 2 aufgezählten Sicherheitsfunktionen an, um die Werte vor den beschriebenen Bedrohungen zu schützen. Diese Sicherheitsfunktionen des TOE wurden in der Evaluation betrachtet.

[5] https://my.lancom-systems.de/mylancom/lizenzportal/downloads/ bzw. https://my.lancom-systems.com/mylancom/license-portal/downloads/
[6] https://www.lancom-systems.de/pdf/BSZ/LANCOM-BSZ-Security-Target-UF-360.pdf
[7] https://www.lancom-systems.de/pdf/BSZ/LANCOM-BSZ-Secure-User-Guidance-UF-360.pdf

Sicherheitsfunktionen des TOE	*Beschreibung*
SecFunc.HTTPS	Der TOE implementiert den Zugriff auf die Management-Schnittstelle der WEBConfig mittels HTTP/1.1 [RFC 9110 ff.] über TLS 1.3 [RFC 8446] (HTTPS). Das Protokoll bietet dem Administrator die Möglichkeit des sicheren Logins und des sicheren Zugriffs zur Management Schnittstelle in Hinblick auf Vertraulichkeit, Integrität und Authentizität der Administrator Zugangsdaten, der Konfiguration, der Überwachungsdaten und der Firmware vom TOE, wenn diese vom oder zum TOE hin übertragen werden.
SecFunc.IPsec	Der TOE implementiert IPSec VPN-Verbindungen mit IPSec [RFC 4301 ff.]. Das Protokoll bietet dem Nutzer eine sichere Datenübertragung über unsichere Netzwerke in Hinsicht auf Vertraulichkeit, Integrität und Authentizität der Nutzerdaten, die über unsichere entfernte Netzwerke übertragen werden.
SecFunc.IPsec.Log	Der TOE loggt erfolgreiche und nicht erfolgreiche Verbindungsversuche von IPSec VPN-Verbindungen innerhalb der Überwachungsdaten des TOE.
SecFunc.Firewall.Sessions	Der TOE implementiert IPv4 Firewall- und Routingdienste. Unter Verwendung der TOE-Konfiguration (gemäß des SUG), die Dienste erlauben den Nutzer in lokalen Netzwerken (LAN) auf entfernte Netzwerk (Internet) zuzugreifen und verweigern den Nutzern in entfernten Netzwerken auf lokale Netzwerke zuzugreifen. Außerdem erlauben die Dienste Nutzern in lokalen Netzwerken (wie LANs in entfernten Firmennetzwerken oder separaten LANs) und solchen Nutzern mit geschützten mobilen Geräten (wie mobile Mitarbeiter oder Mitarbeiter im Homeoffice) den Zugriff auf lokale Netzwerke mit IPSec VPN-Verbindungen.
SecFunc.Firewall.Sessions.Log	Der TOE protokolliert blockierte Firewallsitzungen in den Überwachungsdaten des TOE.
SecFunc.Mgmt.NoInet	Der TOE erlaubt keinen Zugriff zur GUI der WEBconfig von entfernten Netzwerken, die nicht mit IPSec VPN-Verbindungen verbunden sind.
SecFunc.Auth.AdmCrds	Der TOE authentifiziert Administratoren bevor Sie Zugang zur WEBconfig haben per Nutzername und Password.
SecFunc.Auth.AdmPwdChrs	Der TOE erzwingt, dass das Administratorpassword mindestens 8 Zeichen aus 3 der folgenden 4 Kategorien: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten muss.
SecFunc.Auth.AutoLogOut	Der TOE loggt automatisch Administratoren aus der WEBconfig aus, die länger als 10 Minuten inaktiv waren.
SecFunc.Auth.BrtFrcCtr	Der TOE setzt Zugriffsbeschränkungen von Klienten IPs mittels des WEBConfig Webservers um. Zusätzlich werden Passwörter von Administratoren gehasht mit scrypt_mcf. Dies ermöglicht eine Limitierung von Login Versuchen während der Laufzeit mittels der Hashfunktion.
SecFunc.FirwareUpSign	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.

Tabelle 2: Sicherheitsfunktionen des TOE

1.4 Konfiguration des Evaluierungsgegenstands

Dieses Zertifikat gilt nur für die in den Sicherheitsvorgaben [06], Kapitel 3 beschriebene Sicherheitsproblemdefinition, und in der Secure User Guidance [08] beschriebenen Konfigurationen des TOE. Insbesondere sind die folgenden Funktionen, wie in Kapitel 4 unter „Limits of Evaluation“ der Sicherheitsvorgaben [06] beschrieben, von der Evaluation ausgeschlossen und nicht vom Zertifikat abgedeckt:

- Das Produkt besitzt für Managementzwecke, bei direkter Verbindung mit dem Computer, eine serielle COM-Schnittstelle.
- Der USB-Anschluss wird ausschließlich für die initiale Installation der Firmware verwendet.
- Das Produkt besitzt einen SSH-Zugriff (aktiv in der Default-Konfiguration auf TCP Port 22) welcher gemäß des SUG deaktiviert werden muss.
- Das Produkt besitzt TFTP zur Erkennung im Netzwerk von weiteren Lancom-Geräten, welcher ebenfalls deaktiviert ist.
- Das Produkt besitzt SNMP für die Überwachung, welches nicht aktiv ist im Default-Zustand.
- Das Produkt bietet erweiterte Sicherheitsmaßnahmen, genannt „Unified Threat Management”.
- Das Produkt bietet weitere VPN-Mechanismen neben IPSec, wie zum Beispiel VPN-SSL über OpenVPN
- Das Produkt erlaubt normalen Nutzern den Login für Nutzer/Gruppenspezifische Kommunikationsregeln.
- Das Produkt besitzt dynamisches Routing.

Hinweis: Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

1.5 Beschreibung der Einsatzumgebung

In den Sicherheitsvorgaben, Kapitel 2.4 wird die Einsatzumgebung des TOE beschrieben. Hierbei werden Annahmen gemacht, die beim Einsatz des TOE zu praktischen Anforderungen an die Einsatzumgebung werden, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist. Hierbei sind die folgenden Punkte relevant:

- Angeschlossene Geräte im Netzwerk müssen stellen kompatible Ethernet-Geräte (RJ45 oder Glasfaser) dar.
- Der TOE wird nur in Umgebungen mit physischen Zugriffsbeschränkungen genutzt.
- Der Administrator hat ausschließlich für die physische Installation Zugriff auf den TOE.
- Nutzer des Gerätes haben niemals physischen Zugriff auf das Gerät.
- Für IPSec-VPN Verbindungen wird der [RFC 4301 ff.] Standard verwendet.

1.6 Dokumente

Die evaluierten Dokumente Sicherheitsvorgaben und Secure User Guidance, die in Tabelle 1 aufgeführt sind, werden zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem TOE in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des TOE, die im Teil B Abschnitt 2.6 enthalten sind, müssen befolgt werden.

2 Die Evaluierung

Der TOE wurde nach der Evaluationsmethodologie für die Beschleunigte Sicherheitszertifizierung (BSZ) evaluiert. Hierbei wurden die Anwendungshinweise und Interpretationen zum Schema BSZ (AIS B) [3] beachtet. Insbesondere wurde die AIS B4 „Anforderungen an die Evaluierung gemäß BSZ“ befolgt.

Basierend auf dem Ansatz der BSZ mit risikogetriebener Evaluierung innerhalb einer fester Evaluierungszeit wurde der Prozess der Inbetriebnahme sowie die Übereinstimmung des TOE zu der Beschreibung in den Sicherheitsvorgaben und der AIS B6 „Anforderungen an einen TOE “ überprüft. Hauptteil der Evaluierung war die Untersuchung der Widerstandsfähigkeit der Sicherheitsfunktionen mittels Penetrationstests.

2.1 Inbetriebnahme und Konfiguration

Der TOE wurde wie in AIS B4 [3] gefordert in Betrieb genommen und konfiguriert.

Der TOE kann durch die Beschreibung in den Sicherheitsvorgaben [6], Kapitel 3.2 Assumptions und der Secure User Guidance [8] in die zertifizierte Konfiguration gebracht werden.

2.2 Konformität und Funktionsanalyse der Sicherheitsfunktionen

Die tatsächlichen Sicherheitsfunktionen des TOE stimmen mit den in den Sicherheitsvorgaben beschriebenen Sicherheitsfunktionen (siehe Tabelle 2) überein. Ergänzend dazu erfüllt der TOE alle in AIS B6 [3] geforderten Mindestanforderungen.

2.3 Widerstandsfähigkeit der Sicherheitsfunktionen

Das TOE wurde einem Penetrationstest unterzogen um die Widerstandsfähigkeit der Sicherheitsfunktionen zu überprüfen. Hierbei wurde untersucht, ob die in Kapitel 3.4 der Sicherheitsvorgaben [06] beschriebenen Angreifer die Sicherheitsfunktionen unter Ausnutzung von Schwachstellen brechen oder umgehen konnten. Es konnten keine ausnutzbaren Schwachstellen gefunden werden.

2.4 Ergebnis der kryptographischen Bewertung

Die Implementierung der kryptografischen Funktionen wurde nach AIS B2 [3] geprüft. Sie ist konform zu den in [3] geforderten SCES-ACM und BSI-TR-02102 Vorgaben und es konnten keine ausnutzbaren Schwachstellen gefunden werden.

Die Stärke der kryptografischen Algorithmen wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 100/120 Bit nicht länger als sicher angesehen werden, ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden, ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der „Technischen Richtlinie BSI TR-02102“ (https://www.bsi.bund.de/dok/6615148) entnommen werden.

Die folgende Tabelle gibt einen Überblick über die im TOE enthaltenen kryptographischen Funktionen und legt deren Bewertung des Sicherheitsniveaus aus kryptografischer Sicht dar. Jede kryptografische Funktion, die in der Spalte 'Sicherheitsniveau mehr als 120 Bit' ein 'Nein' enthält, erreicht nur ein Sicherheitsniveau unterhalb von 120 Bit (im allgemeinen Anwendungsfall).

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
1	*Vertrauenswürdiger Kanal zum WebConfig via http mittels TLS*	*TLS 1.3*	*[RFC 8446] (TLS 1.3)*			
2	Authentizität	RSA Signatur (RSASSA-PKCS1-v1_5) mittels SHA-2	[RFC 8446] (TLS 1.3), [RFC 8017] (PKCS#1 v2.1), [RFC 5280] (PKIX), [FIPS 180-4] (SHA)	2048 (default Zertifikat, muss vom Admin durch ein neues Zertifikat nach dem ersten Start ersetzt werden), 3072, 4096	Ja	Sicherheitsniveau wird erreicht durch Austausch des default Zertifikats gegen ein Zertifikat mit einer RSA-Schlüssellänge von mindestens 3072 Bit.
3		ECDSA Signatur mittels SHA-2 (secp256r1, secp384r1, secp521r1)	[RFC 8446] (TLS 1.3) [FIPS 180-4] (SHA)	256, 384, 521	Ja	
4	Authentisierung	RSA Signatur (RSASSA-PKCS1-v1_5) using SHA-2	[RFC 8446] (TLS 1.3), [RFC 8017] (PKCS#1 v2.1), [RFC 5280] (PKIX), [FIPS 180-2] (SHA)	2048 (default Zertifikat, muss vom Admin durch ein neues Zertifikat nach dem ersten Start ersetzt werden), 3072, 4096	Ja	Sicherheitsniveau wird erreicht durch Austausch des default Zertifikats gegen ein Zertifikat mit einer RSA-Schlüssellänge von mindestens 3072 Bit.
5		ECDSA Signatur mittels SHA-2 (secp256r1, secp384r1, secp521r1)	[RFC 8446] (TLS 1.3), [FIPS 180-4] (SHA)	256, 384, 521	Ja	
6	Schlüsselaustausch	ECDHE (secp256r1, secp384r1, secp521r1, x25519, x448)	[RFC 8446] (TLS 1.3), [IEEE P1363] (ECDH),	256, 384, 521, 256, 456	Ja (secp-Kurven) Nicht bewertet (x25519, x443)	Für die Kurven x25519, x443 liegt keine Bewertung vor, ob sie das Sicherheitsniveau 120 Bit erreichen. Es liegen aber auch keine Anhaltspunkte vor, dass sie es unterschreiten.

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
7	Vertraulichkeit und Integrität	AES in GCM Modus	[RFC 5288]	128, 256	Ja	
8		ChaCha20-Poly1305	[RFC 8439, 7905]	256	Nicht bewertet	Vgl. Kommentar in Zeile 6.
9	***VPN Tunnel mittels IPsec***	***Protokolle IKEv2 und ESP***				
10	***IKEv2***					
11	Authentizität	Durch Admin generierte sichere pre-shared keys	[RFC 8247] (IKEv2)	-		
12	Authentisierung	MAC mittels pre- shared keys und SHA2	[RFC 8247] (IKEv2), [FIPS 180-4] (SHA2)	256, 384, 512	Ja	
13	Schlüsselaustausch	DH (modp3072, modp4096)	[RFC 3526]	3072, 4096	Ja	
14		DH (NIST Kurven ecp256, ecp384, ecp512)	[RFC 5903]	256, 384, 521	Ja	
15		DH (Brainpool Kurven ecp256bp, ecp384bp, ecp512bp)	[RFC 6954]	256, 384, 512	Ja	
16	Vertraulichkeit und Integrität	AES im GCM Modus	[RFC 4106, RFC 4869]	128, 256	Ja	GCM bietet gleichzeitig Vertraulichkeit und Integritätsschutz
17		AES im CCM Modus	[RFC 4309]	128, 256	Ja	CCM bietet gleichzeitig Vertraulichkeit und Integritätsschutz (CBC-MAC)
18		AES im CBC Modus	[RFC3602]	128, 256	Ja	CBC Modus bietet nur Vertraulichkeit, Integritätsschutz erfolgt durch Zeile 19
19		HMAC mit SHA2	[RFC 4868]	256, 384, 512	Ja	Bietet Integritätsschutz für Zeile 18
20	***ESP***					

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*	*Bemerkungen*
21	Vertraulichkeit und Integrität	AES im GCM Modus	[RFC 4106, RFC 6379]	128, 256	Ja	GCM bietet gleichzeitig Vertraulichkeit und Integritätsschutz
22		AES im CCM Modus	[RFC 4309]	128, 256	Ja	CCM bietet gleichzeitig Vertraulichkeit und Integritätsschutz (CBC-MAC)
23		AES im CBC Modus	[RFC 3602]	128, 256	Ja	CBC Modus bietet nur Vertraulichkeit, Integritätsschutz erfolgt durch Zeile 24
24		HMAC mit SHA2	[RFC 4868]	256, 384, 512	Ja	Bietet Integritätsschutz für Zeile 23

Tabelle 3: Kryptografische Funktionen des TOE

2.5 Updatemechanismus

Der TOE verfügt über einen Sicheren Updatemechanismus, der gegebenenfalls notwendige Sicherheitsupdates ermöglicht. Der Prozess ist in Kapitel 6 auf Seite 11 der Cryptographic Specification [09] beschrieben.

2.6 Auflagen und Hinweise zur Benutzung des TOE

Die in Tabelle 2 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des TOE und alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind die Anforderungen an die Einsatzumgebung des TOE aus den Sicherheitsvorgaben zu beachten, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist.

Der Anwender des Produkts muss die Ergebnisse dieser Zertifizierung sowie die zeitliche Begrenzung der Gültigkeit des Zertifikats in seinem Risikomanagementprozess berücksichtigen.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen, wie in Teil B Abschnitt 2.4 dargelegt, muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

3 Definitionen

3.1 Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
ETR	Evaluierungsbericht (Englisch: Evaluation Technical Report)
IT	Informationstechnik (Englisch: Information Technology)
LCOS FX	LANCOM Systems Operating System Firewall Linux
SF	Sicherheitsfunktion (Englisch: Security Function)
ST	Sicherheitsvorgaben (Englisch: Security Target)
SUG	Handbuch zur sicheren Benutzung (Englisch: Secure User Guidance)
TOE	Evaluierungsgegenstand (Englisch: Target of Evaluation)

3.2 Glossar

Evaluierungsgegenstand – Untersuchtes Produkt bzw. untersuchter Teil des Produkts.

Sicherheitsvorgaben - 1In diesem Dokument werden Sicherheitsfunktionalität, Schnittstellen, Einsatzszenario mit Bedrohungsmodell und Umgebung des Evaluierungsgegenstands beschrieben.

3.3 Literaturangaben

[1] BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (BSZ- Produkte) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Produkte.html

[2]BSI-Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (BSZ-Prüfstellen), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Pruefstellen.html

[3] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den TOE relevant sind[8] https://www.bsi.bund.de/bsz

[4] Anerkennungsabkommen: Mutual Recognition Agreement of Cybersecurity Evaluation Certificates issued under a Fixed-time Certification Process, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ/Abkommen_Anerkennung_ANSSI_BSI.pdf

[5] Deutsche IT-Sicherheitszertifikate, periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/bsz

[8] Die für diese Zertifizierung geltenden AIS B:
- AIS B1 Anforderungen an ST und IAR , Version 1.2, 16.06.2023
- AIS B2 Anforderungen an die Evaluierung kryptographischer Mechanismen gemäß BSZ, Version 1.2, 16.06.2023
- AIS B3 Anforderungen an die Benutzeranleitung , Version, 1.2, 16.06.2024
- AIS B4 Anforderungen an die Evaluierung gemäß BSZ , Version 1.2, 16.6.2023
- AIS B5 Anleitung zur Bestimmung des Aufwands für eine BSZ-Evaluierung , Version 1.2, 16.06.2023
- AIS B6 Anforderungen an einen TOE , Version 1.2, 16.06.2023

[6] Sicherheitsvorgaben BSI-DSZ-BSZ-0008-2024, Version 1.6, 06.09.2024, SECURITY TARGET FOR LANCOM R&S®UNIFIED FIREWALL UF-360 WITH LANCOM SYSTEMS OPERATING SYSTEM LCOS FX 10.11 RU4 AND IPSEC VPN, Antragsteller Lancom

[7] Evaluierungsbericht, Version 1.3, 28.05.2024, BSZ Evaluationsreport, Prüfstelle TÜV Informationstechnik GmbH (vertrauliches Dokument)

[8] SUG für den TOE, Version 1.4, 26.07.2024, SECURE USER GUIDANCE FOR LANCOM R&S®UNIFIED FIREWALL UF-360 WITH LANCOM SYSTEMS OPERATING SYSTEM LCOS FX 10.11 RU4, Antragsteller Lancom

[9] Kryptografische Spezifikation, Version 1.2, Datum 08.02.2024, CRYPTOGRAPHIC SPECIFICATION FOR LANCOM R&S UNIFIED FIREWALL UF-360 WITH LANCOM LCOS FX 10.11 RU4 AND IPSEC VPN