Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	07/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/04/2023/RC, v1.0
Decorrenza *(Date of 1st Issue)*	22 agosto 2024
Nome e Versione del Prodotto *(Product Name and Version)*	OPSWAT NetWall Optical Diode OD-101 v1.0.1
Sviluppatore *(Developer)*	OPSWAT Inc.
Tipo di Prodotto *(Type of Product)*	Dispositivi e sistemi di protezione perimetrale (Boundary Protection Devices and Systems)
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.2, ALC_DVS.2 and AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 22 agosto 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

Firmato digitalmente da:
Andrea Billet
Data: 22/08/2024 18:59:06

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

OPSWAT NetWall Optical Diode OD-101 v1.0.1

OCSI/CERT/CCL/04/2023/RC

Versione 1.0

22 agosto 2024

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	22/08/2024

2 Indice

3 Elenco degli acronimi

3.1 Schema Nazionale

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
RFV	Rapporto Finale di Valutazione
TDS	Traguardo di Sicurezza

3.2 CC e CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Altri acronimi

API	Application Programming Interface
CLI	Command Line Interface
CM	Configuration Management
GUI	Graphical User Interface
REST	Representational State Transfer
RX	Reception
SFP	Security Functional Policy
SKU	Stock Keeping Unit
SSL	Secure Socket Layer
SQL	Structured Language Query
TX	Transmission
UI	User Interface
WebUI	Web User Interface

4 Riferimenti

4.1 Riferimenti normativi e documenti dello Schema nazionale

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Documenti tecnici

[AGD] AGD Documentation OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.5, 04 April 2024

[INST_GUIDE] OPSWAT NetWall OD-101 Common Criteria Evaluated Configuration Guide v1.3, Version: 1.3, 18 January 2024

[RFV2] Evaluation Technical Report OPSWAT NetWall Optical Diode OD-101 v1.0.1, OPSWATEVOD-038_ETR_v2, CCLab Software Laboratory, 09 April 2024

[RFV5] Evaluation Technical Report Veritas NetBackup v9.1.0.1, VERITAS-025_ETR_v2, CCLab Software Laboratory, 05 March 2024

[TDS] Security Target OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.7, 22 May 2024

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione, fino a EAL4 incluso, per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA fino al livello di garanzia EAL4.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (*Common Criteria Recognition Arrangement*, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA fino a EAL2 con la sola aggiunta di ALC_FLR.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "**OPSWAT NetWall Optical Diode OD-101 v1.0.1**", sviluppato da OPSWAT Inc.

L'ODV è costituito da un modulo TX che si collega a una rete di invio (o affidabile) e da un modulo RX che si collega a una rete di ricezione (o non affidabile). Entrambi i moduli applicano in hardware una politica di controllo del flusso di informazioni unidirezionale sul traffico di rete che scorre attraverso l'ODV. Questi moduli sono in esecuzione su un sistema basato su Linux sia sui dispositivi TX che RX.

La connessione tra il modulo TX e il modulo RX è costituita da un cavo di collegamento ottico.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo "*Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione*" ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica (OCSI), istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 Revisione 5 per il livello di garanzia EAL4 con l'aggiunta di AVA_VAN.5, ALC_DVS.2 e ALC_FLR.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in "Appendice B - Configurazione valutata" di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione *Common Criteria* – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal *Common Criteria Recognition Arrangement* [CCRA] e che nessuna vulnerabilità sfruttabile con il potenziale di attacco dichiarato è stata trovata. Tuttavia, l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "NetWall Optical Diode OD-101 v1.0.1" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	OPSWAT NetWall Optical Diode OD-101 v1.0.1
Traguardo di Sicurezza	Security Target OPSWAT NetWall Optical Diode Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5, Version: v1.7, 22 May 2024
Livello di garanzia	EAL4 con l'aggiunta di ALC_FLR.2, ALC_DVS.2 e AVA_VAN.5
Sviluppatore	OPSWAT Inc.
Committente	OPSWAT Inc.
LVS	CCLab – The Agile Cybersecurity Laboratory (sede di Budapest)
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna
Data di inizio della valutazione	1 giugno 2023
Data di fine della valutazione	10 aprile 2024

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le assunzioni sull'ambiente di esercizio descritte nel Traguardo di Sicurezza [TDS] e nella configurazione riportata nell' "Appendice B – Configurazione valutata" di questo Rapporto di Certificazione.

7.3 Prodotto valutato

In questa sezione vengono riepilogati i principali requisiti funzionali e di sicurezza dell'ODV. Per una descrizione dettagliata, fare riferimento al Traguardo di Sicurezza [TDS].

L'Oggetto della Valutazione (ODV) è un *software gateway* di sicurezza unidirezionale, che utilizza diodi ottici per il trasferimento dati, e che è costituito da un modulo TX e da un modulo RX che impongono nel software e nell'hardware un flusso di dati unidirezionale. Il modulo TX si collega alla rete di invio o attendibile e un modulo RX si collega alla rete di ricezione o non attendibile.

La connessione tra il modulo TX e il modulo RX è costituita da un cavo di collegamento ottico.

L'ODV consente di trasferire informazioni quali dati di controllo di processo in tempo reale, registrazioni di eventi *syslog* o file, da reti con sistemi di controllo industriale alla rete aziendale, tramite una connessione dedicata e protetta. L'ODV impedisce che qualsiasi dato ritorni alla rete industriale e impedisce che le informazioni identificative della rete sorgente quali indirizzo IP e indirizzo MAC dei sistemi nelle reti industriali vengano trasferite alla rete di destinazione. Viene trasferito solo il payload dei dati. La rete di invio è completamente protetta da qualsiasi attacco informatico avviato sulla rete ricevente, poiché nessun dato può essere inviato dalla rete ricevente alla rete di invio.

Uno scenario di utilizzo tipico è costituito da una rete sorgente che rappresenta una rete di controllo industriale e una rete ricevente che rappresenta la rete aziendale. Le informazioni possono essere condivise dalla rete industriale alla rete aziendale senza che la rete aziendale si connetta direttamente alla rete di controllo industriale, impedendo un attacco dalla rete esterna che potrebbe influire sulla integrità del sistema protetto o causare mancanza di disponibilità (*denial of service*). L'ODV consente, dunque, alle informazioni di fluire dalla rete industriale alla rete aziendale, impedendo al contempo che qualsiasi informazione rifluisca attraverso il diodo dati alla rete industriale. Ciò serve a prevenire un'ampia gamma di attacchi *online*.

Un secondo utilizzo tipico è quello di spostare in modo sicuro le informazioni da una rete non attendibile a una rete protetta o attendibile. Ad esempio, reti classificate nel dominio dell'*intelligence* o della Difesa che devono ricevere informazioni da una rete a classifica inferiore (o completamente inaffidabile, come Internet), mantenendo al contempo l'isolamento della rete ad alta classifica da quella a classifica inferiore. In questo scenario, L'ODV è configurato in modo tale che il Server di destinazione si connetta alla rete di sicurezza più elevata.

In associazione all'ODV c'è un'applicazione Web che consente a un utente (con ruolo di amministratore dell'ODV - *admin*) di configurare l'ODV per connettersi ai sistemi nelle reti di origine e destinazione e configurare il tipo di dati che viene trasferito dall'ODV. L'applicazione Web è accessibile tramite un browser che visualizza la Web App GUI.

Oltre alla Web App GUI è disponibile una interfaccia a linea di comando (CLI) per la configurazione di sistema. La Web App GUI e la CLI non fanno parte dei confini dell'ODV e il loro uso è raccomandato solo per la fase di configurazione iniziale e solo con una connessione locale in cui il computer con la CLI e/o la Web App GUI è direttamente collegato con l'ODV.

OPSWAT TX Connector (non facente parte dell'ODV) è un software che può essere eseguito sullo stesso dispositivo in cui si trova il modulo OPSWAT TX o su un server nel dominio di invio. OPSWAT TX Connector inoltra dati specifici del protocollo tra i server di rete di invio e inoltra queste informazioni al modulo OPSWAT TX per la consegna all'altro dominio. I protocolli attualmente supportati sono:

- Modbus
- OPC UA
- SMTP
- IEC 104
- DNP3
- MQTT
- OSI-PI

Sul lato ricevente, OPSWAT RX Connector (non facente parte dell'ODV) è un software che può essere eseguito sullo stesso dispositivo in cui si trova il modulo OPSWAT RX o su un server nel dominio ricevente. OPSWAT RX Connector inoltra dati specifici del protocollo tra il modulo OPSWAT RX verso un server sullo stesso dispositivo o a un server nel dominio ricevente.

Per una descrizione approfondita dell'ODV si faccia riferimento alla sezione 1.3 e 1.4 del Traguardo di Sicurezza [TDS].

7.3.1 Architettura dell'ODV

OPSWAT NetWall OD-101 si basa sull'infrastruttura hardware illustrata in Figura 1. Utilizza un *transceiver* unidirezionale TX con sola capacità trasmissiva sul server di invio e un *transceiver* RX con sola capacità di ricezione sul server di destinazione con un cavo ottico per collegare il lato TX al lato RX. Questi *transceiver* ottici sono stati modificati proprio al fine di consentire solo la trasmissione sul lato TX e solo la ricezione sul lato RX. Altri percorsi di trasmissione sono fisicamente disabilitati.

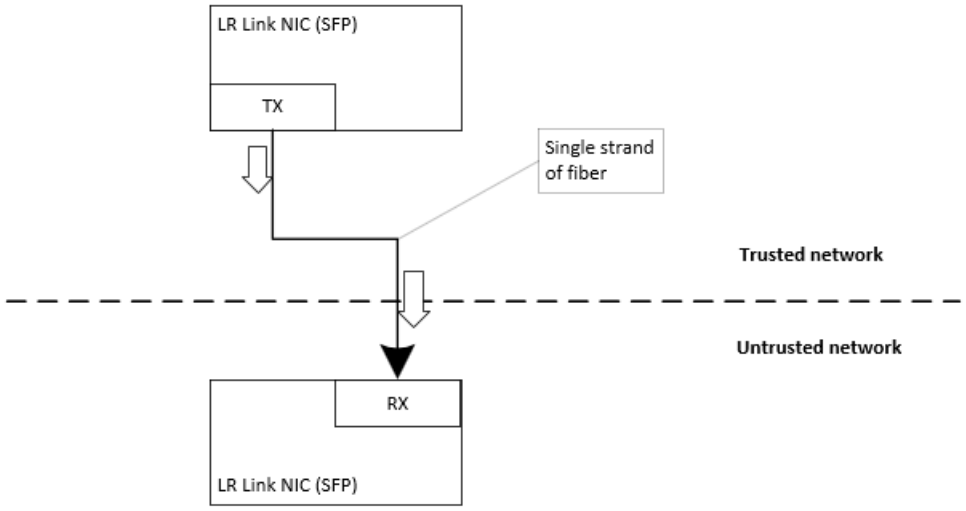

Figura 1 - Descrizione schematica dell'ODV

Questo approccio consente un trasferimento dati unidirezionale forzato a livello fisico senza possibilità di avere canali di ritorno. L'ODV OPSWAT NetWall OD-101 supporta la connessione ottica ridondante, offrendo un livello più elevato di garanzia di distribuzione dei dati. L'ODV è diviso in due moduli diversi, modulo OPSWAT TX e modulo OPSWAT RX (Figura 2).

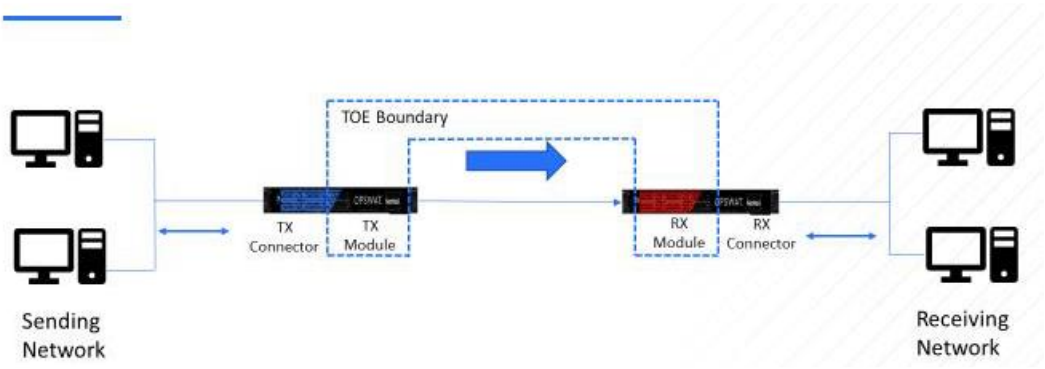

Figura 2 - Confini fisici dell'ODV

La Figura 3 mostra l'architettura dell'ODV includendo anche le componenti esterne alla valutazione. I riquadri blu e rossi indicano i confini dell'ODV. La TSFI è mostrata con gli elementi di colore verde e bianco (all'interno dei riquadri DiodeSend e DiodeReceive).

DiodeSend, SFPTX1 e SFPTX2 nel modulo TX e DiodeReceive, SFPRX1 e SFPRX2 costituiscono il confine dell'ODV. I moduli OPSWAT TX e OPSWAT RX sono posizionati negli apparati fisici identificati come BLUE e RED.

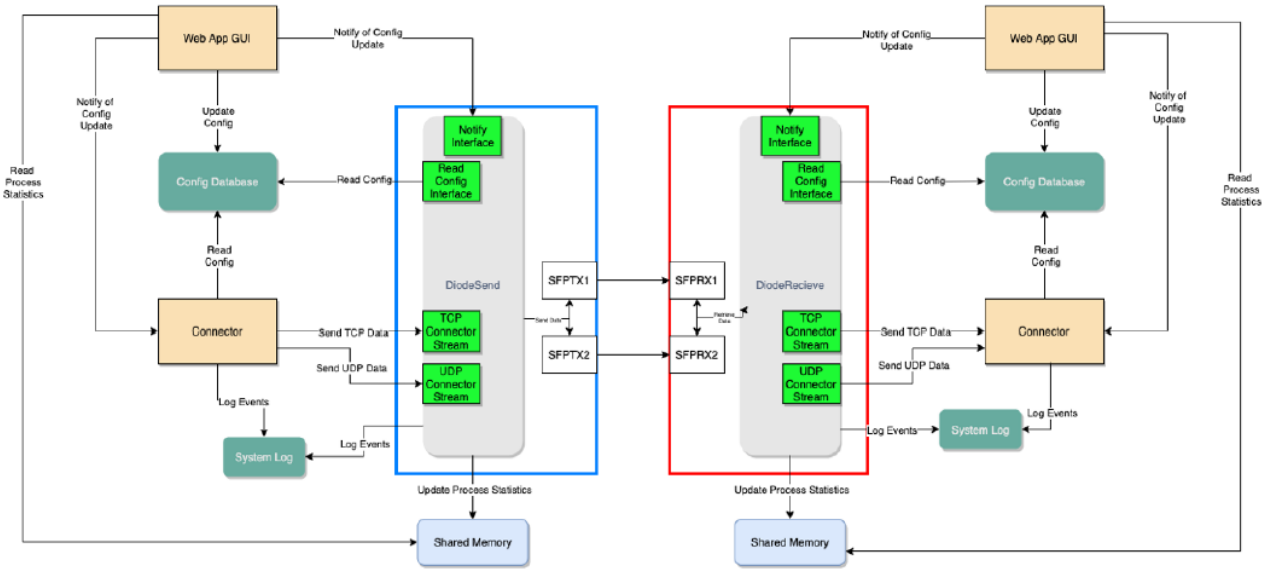

Figura 3 – Architettura dell'ODV

L'ODV è un componente software parte di un prodotto più grande denominato OPSWAT NetWall Optical Diode e composto da due apparati, identificati come BLUE e RED ed equipaggiati con il Sistema Operativo Linux. Il software in esecuzione negli apparati fornisce i seguenti servizi:

Componenti dell'ODV:

- TX Module
- RX Module

Componenti non parte dell'ODV:

- Web App GUI
- Config Database

- Connector
- System Log
- Shared Memory

7.3.2 Caratteristiche di sicurezza dell'ODV

Le assunzioni, le minacce e gli obiettivi di sicurezza sono definiti nelle sezioni 3 e 4 del Traguardo di Sicurezza [TDS].

Le principali caratteristiche di sicurezza dell'ODV sono riassunte di seguito:

1) Protezione dei dati utente

L'ODV è implementato in due moduli indipendenti (hanno fonti di alimentazione indipendenti e interfacce ottiche indipendenti) modulo OPSWAT TX e modulo OPSWAT RX. L'hardware non consente altri modi per trasmettere segnali elettronici o ottici oltre alle interfacce descritte. Il modulo OPSWAT TX è collegato solo alla rete di invio tramite il connettore OPSWAT TX (esterno all'ODV) e il modulo TX non è collegato alla rete di ricezione. Il modulo OPSWAT RX è collegato solo alla rete di ricezione tramite il connettore OPSWAT RX (esterno all'ODV).

Flusso TCP/UDP

Il connettore OPSWAT TX (Connector) si interfaccia con i dati specifici del protocollo tra i server di rete di invio e inoltra queste informazioni al modulo OPSWAT TX. Il modulo OPSWAT TX rimuoverà tutte le informazioni extra-protocollo (instradamento, ecc.) dai dati ricevuti dall'OPSWAT TX Connector prima di inviarli al modulo OPSWAT RX, eseguendo a tutti gli effetti un "*protocol break*".

Un cavo in fibra ottica collega i moduli TX e RX. Il cavo in fibra ottica può essere reso ridondante, fornendo un livello più elevato di garanzia di trasmissione dei dati. I transceiver all'interno dell'ODV (SFPTX1, SFPTX2, SFPRX1 e SFPRX2) sono stati modificati fisicamente per supportare solo la comunicazione in una singola direzione, dal modulo TX al modulo RX. SFPTX1 e SFPTX2 non dispongono di ottica e circuiti necessari per ricevere i dati. SFPRX1 e SFPRX2 non dispongono di ottica e circuiti necessari per inviare i dati. Ciò garantisce che tutte le informazioni che fluiscono attraverso l'ODV vengano trasferite tramite una connessione unidirezionale tra i moduli TX e RX implementata anche in modo fisico a supporto della SFP unidirezionale.

Il modulo TX è collegato alla rete di invio tramite il connettore OPSWAT TX utilizzando interfacce RJ45 standard. Il modulo TX non può leggere informazioni dalla rete di ricezione perché le sue interfacce di rete sono collegate solo alla rete di invio. Il modulo TX converte la comunicazione in arrivo in una trasmissione dati basata su fibra ottica utilizzando un transceiver in fibra ottica. Questo transceiver è stato modificato fisicamente per supportare solo la trasmissione dati, implementando l'isolamento galvanico.

Un cavo in fibra ottica collega il dispositivo BLUE al dispositivo RED e costituisce l'unica connessione tra questi due componenti. Il cavo in fibra ottica può essere reso ridondante, fornendo un livello più elevato di garanzia di trasmissione dei dati. Questo cavo in fibra ottica si collega alla porta ottica del modulo RX. Il modulo OPSWAT RX converte i dati ottici in arrivo in segnali elettronici utilizzando un transceiver in fibra ottica. Questo transceiver è stato modificato fisicamente per supportare solo la ricezione dei dati, implementando l'isolamento galvanico.

Il modulo RX è collegato alla rete ricevente tramite il connettore OPSWAT RX utilizzando interfacce RJ45 standard. Il modulo OPSWAT RX trasmette i dati ricevuti dal modulo TX al connettore OPSWAT RX e, da lì, alle stazioni e ai server nella rete ricevente. Il modulo RX non può trasmettere

informazioni alla rete di invio perché le sue interfacce di rete sono collegate solo alla rete ricevente evil transceiver ottico nel modulo RX è stato modificato fisicamente per supportare solo la ricezione dei dati.

Gestione della sicurezza

Solo un amministratore con credenziali valide e in possesso di un dongle di sicurezza (vedere la sezione 10.1) può modificare i dati di configurazione e gli attributi sicuri all'interno del database in entrambi i lati, Invio (TX) e Ricezione (RX). I dati di configurazione e gli attributi sicuri dell'ODV non possono essere modificati dall'ODV.

Lettura della configurazione (Read Config)

Una volta che l'amministratore esegue modifiche sui dati di configurazione e/o sugli attributi sicuri all'interno del database utilizzando la Web App GUI e/o la CLI, l'ODV verrà informato della modifica tramite la funzione Notifica della funzione "Config Update". Una volta ricevuto la notifica, l'ODV leggerà i nuovi dati di configurazione tramite la funzione "Read Config".

Per una descrizione dettagliata delle funzionalità di sicurezza dell'ODV, si faccia riferimento alle sezioni 1.4 e 6 del Traguardo di Sicurezza [TDS].

7.4 Documentazione

La documentazione specificata in "Appendice A - Indicazioni per l'uso sicuro del prodotto " viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel paragrafo di 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun profilo di protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono tratti da CC Part 3 [CC3] e sono derivati dal pacchetto di garanzia EAL 4, con l'aggiunta dei componenti ALC_FLR.2, ALC_DVS.2 e AVA_VAN.5, sempre tratti dalla parte 3 dei CC.

Tutti i requisiti funzionali di sicurezza (SFR) sono stati selezionati dalla Parte 2 dei CC [CC2].

È possibile fare riferimento al Traguardo di Sicurezza [TDS] per la descrizione completa di tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i requisiti funzionali di sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab – The Agile Cybersecurity Laboratory (Sede di Budapest).

L'attività di valutazione è terminata in data 10 aprile 2024 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione approvato [RFV2]. A seguito di alcuni chiarimenti richiesti dall'Organismo di Certificazione in fase di redazione del rapporto di certificazione, l'RFV è stato ulteriormente rivisto con l'emissione di una versione definitiva ([RFV5]).

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in "Appendice B – Configurazione valutata".

I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

L'organismo di certificazione raccomanda di rivedere le ipotesi nella sezione 3.3 del [TDS], che sono condizioni necessarie da implementare per la sicurezza dell'ODV:

- *A.ADMIN - Personnel with authorized physical access to the appliances where the TOE is placed, will not attempt to circumvent the TOE's security functionality or perform any malicious action.*
- *A.PHYSICAL - Appliances (including TOE, Fiber cable and Web App GUI console) will be located within secure and controlled access facilities, preventing unauthorized access.*
- *A.NETWORK - TOE will be the only communications channel between sending and receiving networks*.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali ed effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV2] prodotto CCLab – The Agile Cybersecurity Laboratory (Sede di Budapest) e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, l'OCSI è giunto alla conclusione che l'ODV "OPSWAT NetWall Optical Diode OD-101 v1.0.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4 con l'aggiunta di ALC_DVS.2, ALC_FLR.2 e AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in "Appendice B - Configurazione valutata".

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4 con l'aggiunta di ALC_DVS.2, ALC_FLR.2 e AVA_VAN.5 (i componenti aggiunti sono in *corsivo* nella Tabella 1).

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	*ALC_DVS.2*	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo

Classi e componenti di garanzia		Verdetto
Well-defined development tools	ALC_TAT.1	Positivo
Flaw reporting procedures	*ALC_FLR.2*	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: basic design	ATE_DPT.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	*AVA_VAN.5*	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "NetWall Optical Diode OD-101 v1.0.1" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nella sezione 4 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le assunzioni descritte nel par. 3.3 del Traguardo di Sicurezza [TDS].

Come anticipato nella sezione 7.8 del presente rapporto di certificazione, l'Organismo di Certificazione raccomanda di tenere in considerazione le assunzioni introdotte dal Traguardo di Sicurezza [TDS] alla sezione 3.3. Tali assunzioni sono condizioni necessarie da implementare per la sicurezza dell'ODV e vengono qui ripetute, per comodità:

- *A.ADMIN - Personnel with authorized physical access to the appliances where the TOE is placed, will not attempt to circumvent the TOE's security functionality or perform any malicious action.*
- *A.PHYSICAL - Appliances (including TOE, Fiber cable and Web App GUI console) will be located within secure and controlled access facilities, preventing unauthorized access.*
- *A.NETWORK - TOE will be the only communications channel between sending and receiving networks*.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella sua configurazione valutata. In particolare, l'"Appendice A - Indicazioni per l'uso sicuro del prodotto" del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione, alla configurazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([INST_GUIDE], [AGD]).

9 Appendice A - Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna dell'ODV

Di seguito sono riportati i passaggi procedurali che definiscono come l'ODV viene configurato e consegnato al cliente:

1. Ricezione Ordine - L'ordine di acquisto (PO) viene ricevuto nel reparto di evasione degli ordini di OPSWAT.
2. Rivedi Ordine - Verifica che gli SKU degli articoli nel PO siano corretti.
   i. Risoluzione eventuali dubbi ed errori connessi all'ordine, se necessario.
3. OPSWAT recupera e assembla l'hardware necessario per completare l'ordine di acquisto.
4. Controlla e segnala il livello delle scorte per la gestione dell'inventario.
5. Passa le informazioni sul numero di serie per la registrazione.
6. Controlla e verifica l'elenco delle parti.
7. Verifica che gli strumenti software siano aggiornati e che gli archivi software siano corretti.
8. Sono eseguite ispezioni sull'hardware.
9. Sono completate le configurazioni hardware.
10. Completa la *build* del software secondo i passaggi richiesti per ogni SKU.
11. Verifica le versioni software di avvio.
12. Verifica il corretto spegnimento.
13. Applica le marcature.
14. Effettua la pulizia delle unità.
15. Prepara per l'imballaggio il materiale di spedizione OPSWAT.
16. Componenti e articoli vari, sono controllati per ogni prodotto così come imballato.
17. Inserisce il materiale OPSWAT nelle scatole imballate.
18. Prepara le etichette di spedizione/reso con sigillo di sicurezza.

Il Cliente può controllare nella fattura il numero di serie (Serial Number) degli apparati che gli sono stati inviati. Questo numero di serie è anche indicato in un'etichetta aggiunta agli apparati. Allo stesso modo, gli slot Small Form-Factor Pluggable (SFP) hanno un'etichetta che indica il numero di serie.

Il numero di serie sugli apparati può essere confrontato con quello indicato nella fattura. Per quanto riguarda il software, OPSWAT rende nota agli utenti l'esatta versione che deve essere installata, per essere conforme alla certificazione corrente, in "OPSWAT NetWall Data Diode OD-101 Common Criteria Evaluated Configuration Guide" [INST_GUIDE]. Il documento, insieme al documento [AGD] e al Manuale Utente, sarà disponibile su https://docs.opswat.com/netwalldiode/netwall-diode con i corrispondenti valori *hash* per la protezione dell'integrità.

I clienti potranno controllare i diversi hash dei pacchetti di aggiornamento che OPSWAT fornisce loro confrontandoli con la versione consigliata nella documentazione. In questo modo, il cliente può controllare se il software installato è quello corretto.

Ogni documentazione relativa al prodotto è disponibile tramite la pagina "Documentazione tecnica" per i prodotti OPSWAT (https://docs.opswat.com/netwalldiode), dove viene sempre pubblicata la documentazione più recente. La pagina è gestita tramite DeveloperHub e, al fine di proteggere l'integrità dei file, lo strumento è disponibile solo per le persone con i diritti di accesso e le credenziali appropriate.

9.2 Installazione, configurazione e utilizzo sicuro dell'ODV

Per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV è necessario attenersi alle istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, i documenti [INST_GUIDE] e [AGD] contengono informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e l'utilizzo sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS].

10 Appendice B - Configurazione valutata

I Valutatori hanno seguito i passaggi di preparazione definiti nei documenti [INST_GUIDE] e [AGD] per ottenere l'ODV nella configurazione attesa.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con la versione numero 1.0.1. La valutazione dell'ODV è stata condotta nella configurazione 1.5.0. Il nome, la versione e il numero di configurazione identificano in modo univoco l'ODV e l'insieme dei suoi sottosistemi, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori al momento dell'esecuzione dei test e alla quale vengono applicati i risultati della valutazione.

L'ODV è costituito solo dai moduli TX e RX. Questi sono responsabili della comunicazione del flusso di dati unidirezionale. TX e RX sono abbreviazioni di *Transmit* e *Receive*. Pertanto, l'ODV è composto solo dai due pacchetti software:

- NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE
- NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED

Il prodotto viene consegnato con tutti i componenti software necessari già installati, ma il cliente può scaricare la versione valutata dell'ODV dalla pagina https://my.opswat.com/portal/products e l'integrità dei file scaricati può essere convalidata utilizzando i valori *hash* disponibili per ogni versione. Il pacchetto scaricato può essere installato utilizzando la funzione di "Aggiornamento software".

La Tabella 2 riporta una lista dei possibili dispositivi hardware su cui può essere installato l'ODV. L'ODV è il medesimo per entrambi i dispositivi fisici che differiscono solamente per il livello di prestazioni erogate in termini di capacità.

Dispositivo fisico	**Numero di serie**	**Versione Software**	**Pacchetto di installazione**	**HASH**
NetWall BLUE 1U	NW202300019	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE	SHA256: d2d2d225832486f85358e3fefe84b97b05401321a9bc0896879448f4055fc28c
NetWall RED 1U	NW202300020	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED	SHA256: e1be95643a2c6c8548ce4096c1bacfd3aa43d8ec6621b1ac96b49b2e826b826a
NetWall BLUE DIN rail	LR202207015043	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1963_BLUE	SHA256: d2d2d225832486f85358e3fefe84b97b05401321a9bc0896879448f4055fc28c
NetWall RED DIN rail	LR202207015044	OD-101: 1.0.1 Config: 1.5.0	NetWall_OD-101_1.0.1_Config_1.5.0.1965_RED	SHA256: e1be95643a2c6c8548ce4096c1bacfd3aa43d8ec6621b1ac96b49b2e826b826a

Tabella 2 – Identificazione della versione valutata dell'ODV

Gli elementi descritti nella sezione 10.1 “Ambiente operativo dell’ODV” devono essere predisposti prima di eseguire l’installazione.

10.1 Ambiente operativo dell’ODV

In associazione con l’ODV viene fornita un'applicazione Web che consente all'utente di configurare le connessioni ai sistemi nelle reti di origine e destinazione e configurare il tipo di dati che viene trasferito dall’ODV. Gli amministratori dell’ODV possono accedere all'applicazione Web tramite un *browser* in esecuzione su un elaboratore connesso localmente al dispositivo “Optical Diode”. Il browser consente di visualizzare la Web App GUI.

Oltre all'applicazione Web, è disponibile un'interfaccia a riga di comando (CLI) che può essere utilizzata anche per configurare il sistema (sempre ad uso esclusivo degli amministratori). L'applicazione Web di configurazione e la CLI non sono parte dell’ODV.

Due dispositivi USB (*dongle* di sicurezza) sono forniti da OPSWAT e sono impiegati agiscono come un secondo fattore per l'autenticazione, ossia è necessario siano presenti per consentire l’accesso.

OPSWAT crittografa ogni dongle con informazioni univoche per il sito del cliente. I dongle sono crittografati e configurati in modo che non sia possibile accedervi da un computer con mezzi normali.

Ogni dongle contiene le seguenti informazioni che sono univoche per ogni cliente:

- una Site Key che identifica il sito dell'organizzazione del cliente. Questa chiave è la stessa su tutti i dongle dell'organizzazione.
- una chiave di sicurezza univoca per ogni dongle.

Questi due dongle sono preregistrati. Se l'organizzazione ha bisogno di dongle extra, questi devono essere registrati tramite la CLI per funzionare correttamente. L'utente ha bisogno delle credenziali di amministratore per accedere alla CLI.

11 Appendice C – Attività di test

Questa appendice descrive le attività fatte dal laboratorio di valutazione (LVS) e dallo Sviluppatore durante i test.

11.1 Configurazione per i test

Il valutatore ha condotto i test in ambiente locale. La configurazione di test è stata installata dal valutatore che ha seguito i passaggi descritti nei documenti [AGD] e [INST_GUIDE].

11.2 Test funzionali svolti dallo Sviluppatore

11.2.1 Approccio adottato per i test

I test sono stati eseguiti utilizzando tre reti. Una rete sorgente (BLUE), una rete ricevente (RED) e una rete di accesso. Le reti sorgente e ricevente non erano in grado di comunicare tra loro. La rete di accesso aveva accesso alle reti sorgente e ricevente per la configurazione e il test. Un server Ubuntu (mittente) è stato configurato sulla rete sorgente e un server Ubuntu (destinazione) è stato configurato sulla rete ricevente. I server erano dotati del pacchetto *netcat openbsd* installato.

11.2.2 Copertura dei test

I Valutatori hanno verificato la copertura completa tra i casi di test nella documentazione di test fornita dallo Sviluppatore e le interfacce TSFI descritte nelle specifiche funzionali. I Valutatori hanno verificato che i casi di test sono sufficienti per dimostrare il comportamento interno e le proprietà della TSF.

11.2.3 Risultati dei test

I risultati effettivi di tutti i test dello Sviluppatore sono stati coerenti con quelli attesi.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

11.3.1 Approccio adottato per i test

A causa delle dimensioni relativamente ridotte del campione, tutti i test dello Sviluppatore sono stati ripetuti dai Valutatori per confermare la validità dei risultati attesi. I test in questione sono:

- Caso di test 1 – Configurazione flusso UDP modulo TX
- Caso di test 2 – Configurazione flusso UDP modulo RX
- Caso di test 3 – Invio dati UDP
- Caso di test 4 – Configurazione flusso TCP modulo TX
- Caso di test 5 – Configurazione flusso TCP modulo RX
- Caso di test 6 – Invio dati TCP
- Caso di test 7 – Inizializzazione DiodeSend
- Caso di test 8 – Inizializzazione DiodeReceive

I Valutatori hanno inoltre creato cinque casi di test aggiuntivi per testare specificamente la funzionalità unidirezionale fornita dall'ODV.

11.3.2 Risultati dei test

Tutti i test dello Sviluppatore sono stati eseguiti con successo e i Valutatori hanno verificato il corretto comportamento delle TSFI e delle TSF e la corrispondenza tra i risultati attesi e i risultati raggiunti per ogni test.

Tutti i casi di test ideati dai Valutatori sono stati superati con successo e tutti gli esiti dei test sono risultati coerenti con gli esiti attesi.

11.4 Analisi delle vulnerabilità e test di intrusione

Per lo svolgimento di tali attività, i Valutatori hanno lavorato con l'ODV già utilizzato per le attività di test funzionale e verificato che l'ODV e l'ambiente di test fossero correttamente configurati.

I Valutatori hanno progettato i seguenti scenari di attacco:

- *injection attacks (Cross-Site Scripting* e *SQL injection);*
- *information leak over OSI layers in network packets;*
- vulnerabilità SSL*;*
- *password brute-force authentication attack;*
- modifica di *cron jobs scripts;*
- *buffer overflow;*
- *file upload;*
- *man-in-the-middle attack;*
- *escape from restricted CLI;*
- modifica non autorizzata di parametri dell'ODV*;*
- *information leak on REST API* in assenza di autenticazione;
- flusso informazioni non consentito *(over one-way transmission).*

I Valutatori hanno concluso che l'ODV è resistente a un potenziale di attacco di livello ALTO nell'ambiente operativo previsto.