SERTIT
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-051 CR Certification Report

Issue 1.0 28 November 2013

Thinklogical VX640 Router KVM Matrix Switch

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

Contents

1 Certification Statement

Thinklogical VX640 Router KVM Matrix Switch is a fiber optic switch that uses multi-mode or single-mode fiber optics to transmit and receive a digital video pulse stream without alteration or interpretation of the original signal.

Thinklogical VX640 Router KVM Matrix Switch has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Rage, Arne Høye Certifier Arne Høye Rage
Quality Assurance	Lars Borgos Quality Assurance Lars Borgos
Approved	Kjell W. Bergan Head of SERTIT Kjell W. Bergan
Date approved	28 November 2013

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
SERTIT	Norwegian Certification Authority for IT Security
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Thinklogical VX 640 Router KVM Matrix Switch Security Target, version 1.4, August 2013.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL4 Evaluation of Thinklogical Router KVM Matrix Switches, Thinklogical MX 48 (SERTIT - 047), Thinklogical VX 80 (SERTIT - 048), Thinklogical VX 320 Audio (SERTIT - 049), Thinklogical VX 320 Video (SERTIT - 050), Thinklogical VX 640 (SERTIT - 051), version 0.5, 28 November 2013.

[8] ALC.DEL_1_0.doc version 1.0 06/01/10

[9] Manual_VX640_Rev_E.pdf, VX640 router KVM Matrix Switch Product Manual, Rev. E September 2013

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thinklogical VX640 Router KVM Matrix Switch to the Sponsor, Thinklogical, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The product evaluated was Thinklogical VX640 Router KVM Matrix Switch (VXR-000640 Rev B)

And Data Input/Output cards:

- Velocity Matrix Router 640 Data Input/Output Card, 20 Ports, SFP+, Multi Mode (VXM-DIOR20 Rev A),

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thinklogical.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

4.3.1 System type and overview

The TOE is a 640 x 640 routing system, which provides connection of 640 optical inputs located on the upper and lower card cage ports to any or all of the 640 optical outputs located on the same upper and lower card cage ports. The TOE consists of 32 Data Input and Output Cards having 20 optical input and output ports. The 32 Data Input and Output Cards installed in the upper and lower card cages can be used to connect any of the 640 Inputs in one direction to any output or multiple outputs. Any combination of Transmitter Port L1 to Receiver Port L1 or Receiver Port L2 to Transmitter Port L2. Each of the 32 Data Input and Output Cards connects to each of the eight 160x160 switch cards through five connections on a passive backplane. The TOE allows for remote operation of shared computers using sets of shared peripherals, dynamically connecting (switching) physical ports on a particular computer to a particular shared peripheral set.

The TOE consists of the following hardware devices:

1. Thinklogical KVM Matrix Switch (VX640 Router)

2. 32 Data Input/Output Cards

Velocity Transmitter Extenders are connected to the input ports of the Data Input and Output Cards located in the upper card cage and to the output ports of the Data Input and Output cards located in the lower card cage of the Switch using optical fibers connections.

Velocity Receiver Extenders are connected to the output ports of the Data Input and Output Cards located in the upper card cage and to the input ports of the Data Input and Output cards located in the lower card cage of the Switch using optical fibers connections.

Each Transmitter and Receiver Port Group is composed of two ports: T port and R port. Two optical cables are then required to connect a Velocity Transmitter or Receiver Extender to a Transmitter or Receiver Port Group on the Switch. One cable is used to transmit data from the Extender to the Switch; the other cable is used to transmit data from the Switch to the Extender. As a result, a bi-directional connection is established, where data can flow in both directions.

All data types, including video, audio and serial data are converted to an optical form and transmitted in a single optical cable.

The purpose of the Switch is to establish logical connections between Transmitter and Receiver Port Groups, while preserving Data Separation Security Function Policy (SFP).

Data Separation Security Function Policy (SFP) states that data shall flow between Transmitter Port A and Receiver Port B if and only if a deliberate logical connection has been established to connect A to B. There shall be no other data flow between a Transmitter Port or a Receiver Port and any other physical port on the Switch.

The use of a restrict or partition table in the system overrides any deliberate logical connection established between Transmitter Port A and Receiver Port B since the restrict policy disallows connection of a higher priority input to a lower priority output and the partition policy disallows connection of an input from one partition going to the output of another partition.

The TOE connections are first controlled by restrict and priority tables and then controlled, if not in conflict with the restrict or partition tables, over the serial RS-232/console interface, a wired 10/100BASE-TX LAN connection.

4.3.2 Physical boundaries

VX 640 Router KVM Matrix Switch is a hardware device. TOE Physical Boundaries then correspond to the physical boundaries of the device enclosure.

4.3.3 Logical boundaries

TOE logical boundaries include all software and firmware components inside the VX 640 Router KVM Matrix Switch.

The following Security Functions are provided by the TOE

- User Data Protection (enforces Data Separation SFP),

This Security Target includes all product security features. There are no security features outside the scope of the evaluation.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 4 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the Security Target [1].

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- Residual data may be transferred between different port groups in violation of data separation security policy.
- State information may be transferred to a port group other than the intended one.

4.9 Threats Countered by the TOE's environment

- The TOE may be delivered and installed in a manner which violates the security policy.
- An attack on the TOE may violate the security policy.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- The switch, the transmitters, the receivers, the optical connections from the Switch to the transmitters and receivers and the wired network connections from the Switch to the administrators are physically secure.

- The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions.
- The TOE is installed and managed in accordance with the manufacturer's directions.
- The TOE users and administrators are non-hostile and follow all usage guidance.
- Vulnerabilities associated with attached devices are a concern of the application scenario and not of the TOE.

4.12 IT Security Objectives

- The TOE shall not violate the confidentiality of information which it processes. Information generated within any peripheral set/computer connection shall not be accessible by any other peripheral set/computer connection.
- No information shall be shared between switched computers and peripheral sets via the TOE in violation of Data Separation SFP.

4.13 Non-IT Security Objectives

- The TOE shall meet the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions.
- The TOE shall be installed and managed in accordance with the manufacturer's directions.
- The authorized user shall be non-hostile and follow all usage guidance.
- The Switch, the transmitters, the receivers, the optical connections from the Switch to the transmitters and receivers and the wired network connections from the TOE to the administrators shall be physically secure.
- Vulnerabilities associated with attached devices or their connections to the TOE, shall be a concern of the application scenario and not of the TOE.

4.14 Security Functional Requirements

- **FDP_ETC.1.1** Enforce the Data Separation Policy when exporting user data, controlled under the SFP, from outside of the TOE.
- **FDP_ETC.1.2** Export the user data without the user data's associated security attributes.
- **FDP_IFC.1.1** Enforce the Data Separation Policy on the set of Transmitter and Receiver Port Groups, and the bi-directional flow of data and state information between the shared peripherals and the switched computers.
- **FDP_IFF.1.1** Enforce the Data Separation Policy based on the following types of subject and information security attributes:
    - Transmitter and Receiver Port Groups (subjects)
    - peripheral data and state information (objects)
    - port group IDs
    - logical connections of Transmitter and Receiver Groups (attributes)
- **FDP_IFF.1.2** Permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

  - peripheral data and state information can only flow between Transmitter and Receiver port groups that have been previously logically connected by the administrator using the TOE management interface
- **FDP_IFF.1.3** Enforce that Transmitter Port Group may be logically connected to multiple Receiver Port Groups, out of which bi-directional information flow will be established only with a single Primary Receiver Port Group selected by the administrator. The remaining Non-Primary Receiver port groups will only receive unidirectional multicast audio and video signals. Any Receiver Port Group may only be logically connected to a single Transmitter Port Group.
- **FDP_IFF.1.5** Explicitly deny an information flow based on the following rules:
  - No data or state information flow shall be allowed between logically unconnected port groups.
  - No data or state information flow shall be allowed between any two Receiver Port Groups.
  - No data or state information flow shall be allowed between any two Transmitter Port Groups.

  No data or state information flow shall be allowed between any Receiver or Transmitter Port Group and any other non-optical physical port on the Switch

- **FDP_ITC.1.1** Enforce the Data Separation Policy when importing user data, controlled under the SFP, from outside of the TOE.
- **FDP_ITC.1.2** Ignore any security attributes associated with the user data when imported from outside the TOE.

4.15 Security Function Policy

The TOE logically connects Transmitter and Receiver Port Groups according to the current switching configuration. The data flows between a particular Transmitter Port Group and a set of Receiver Port Groups if and only if there is an active logical connection connecting these. If there are multiple Receiver Port Groups connected to a Transmitter Port Group, bi-directional information flow will be then established between the Primary Receiver Port Group and the Transmitter Port Group. The remaining Non-Primary Receiver Port Groups will receive uni-directional multi-cast video and audio signals from the Transmitter Port Group.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Norconsult AS Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT on 28.11.2013. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

Thinklogical's delivery procedure [8] describes how the TOE is shipped from Thinklogical's warehouse via Federal Express, UPS or DHL to the customer. The procedure explains that all tracking and shipment information are logged, and upon delivery of the TOE a signature is required. Each shipment is noted with dimension and weight, and hard copies of each shipment are held in Thinklogical's Sales Order folder.

The product manual [9] describes that users has to verify and ensure that all parts of the TOE has been delivered in the correct version. The text states that if the user has ordered an EAL4 certified unit, the user has to verify that he or she has received the proper materials.

5.3 Installation and Guidance Documentation

A description of the secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST [1] can be found in the product manual [9].

The guidance documentation [9] describes the security functionality and interfaces provided by the TSF, it provides instructions and guidelines for the secure use of the TOE, it addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states.

A list of all guidance documents evaluated can be found in Annex A.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Administrators should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance document adequately describes the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions

5.5 Vulnerability Analysis

The evaluators' assessment of potential exploitable vulnerabilities in the TOE has been addressed and shows that the vulnerability analysis is complete, and that the TOE in its intended environment is resistant to attackers with an Enhanced-Basic attack potential.

5.6 Developer's Tests

The evaluators' assessments of the developers' tests shows that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements. The testing performed on the TOE by both the developer and evaluator showed that the EAL 4 assurance components requirements are fulfilled.

5.7 Evaluators' Tests

The evaluator have independently tested the TSFs and verified that the TOE behaves as specified in the design documentation and confidence in the developer's test results is gained by performing a sample of the developer's tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Thinklogical VX640 Router KVM Matrix Switch meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Thinklogical VX640 Router KVM Matrix Switch should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given in Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- Thinklogical VX640 Router KVM Matrix Switch (VXR-000640 Rev B)

and Data Input/Output cards:

- Velocity Matrix Router 640 Data Input/Output Card, 20 Ports, SFP+, Multi Mode (VXM-DIOR20 Rev A)

TOE Documentation

The supporting guidance documents evaluated were:

[a] Cover Page AGD.OPE.3.doc, OPERATIONAL USER GUIDANCE REV. C 01/23/2013

[b] Manual_VX640_Rev_D.pdf, VX640 ROUTER KVM MATRIX SWITCH PRODUCT MANUAL REV. E SEPTEMBER 2013

[c] Manual_X4 Configurator.pdf, X4 CONFIGURATOR PRODUCT MANUAL OCTOBER 2012

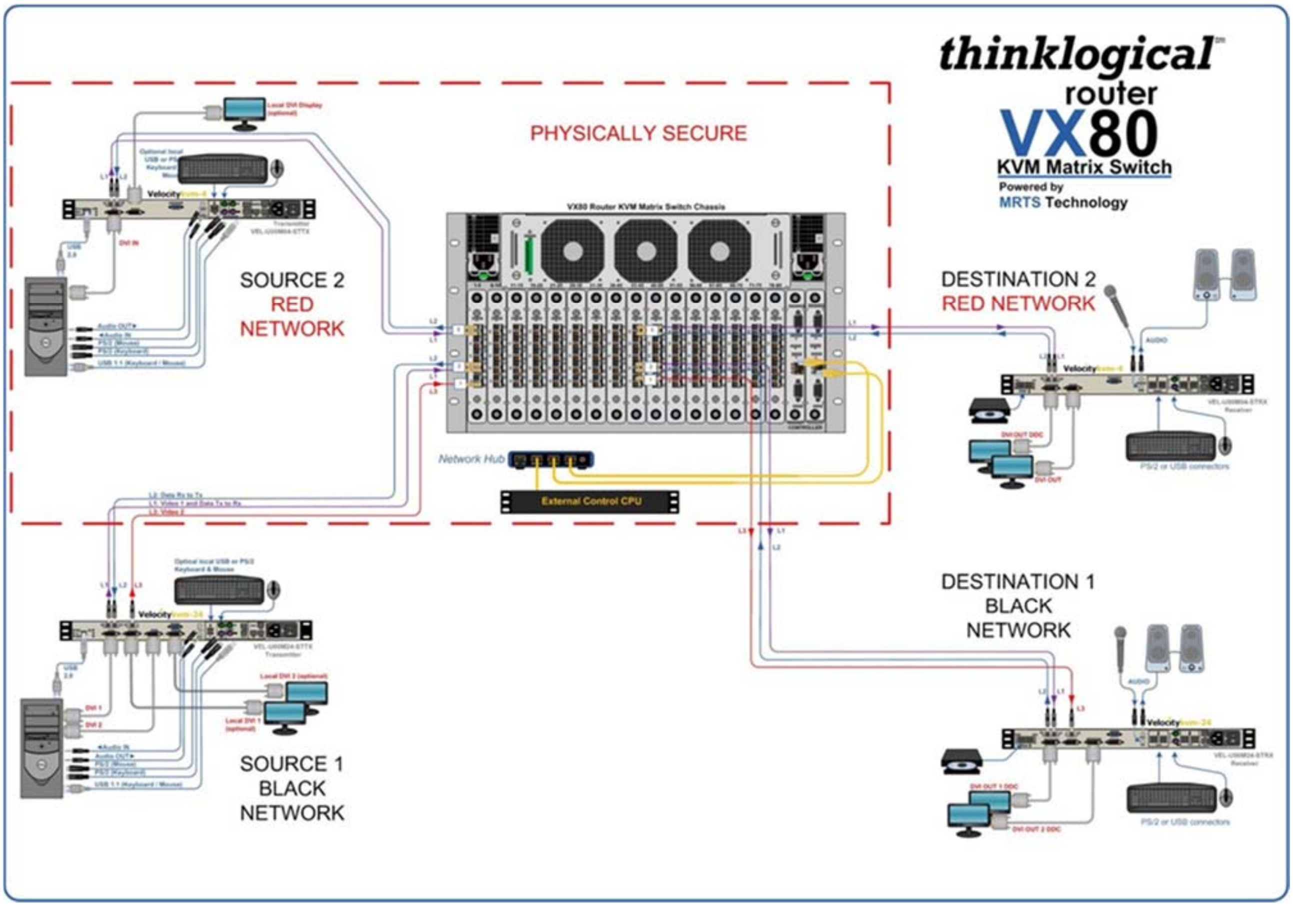
[d] VxRouter-ASCII-API_4_1.pdf, VxRouter ASCII Interface 4.1 24/9-2012

[e] Using-the-ASCII-Interface_4_0.pdf, Using the VxRouter ASCII Interface 4.0 24/9-2012

[f] VX640_VQM-3AV+_VQM-3_VQM-3R_QSG, QUICK-START GUIDE Router VX640 KVM MATRIX Switch As used with Thinklogical's Q-4300 Video Extension System 19/11-2012

TOE Configuration

The following configuration was used for testing:



The figure shows the VX80 Router in an evaluated configuration, however the layout is equivalent for the TOE.

For use in an evaluated configuration, the MX and VX Routers must be located in a physically secure environment to which only authorized administrators has access. Similarly, the server used to manage the MX and VX Routers must be physically protected and have suitable identification/authentication mechanism to ensure that only trusted administrators have access.

Some of the tools used during the evaluation were:

- Microsoft Office 2010
- Nmap port scanning 6.40
- Zenmap (Nmap Security Scanner GUI)
- Microsoft Hyperterminal
- Noyes optical power meter, Model OPM 4-D, Serialnumber 1v52NM024
- Putty Terminal Emulator
- WinSCP
- BusyBox v1.12.1
- Oscilloscope Tektronic TDS6154C, asset number 1054750
- Microsoft Telnet

Environmental Configuration

The TOE is a hardware device. The TOE provides remote connections from a set of shared computers to a set of shared peripherals. The switching capability of the TOE is used to connect ports on a particular computer to a particular peripheral set. The corresponding electronic signal from a computer port is transformed into an optical signal by the Velocity extender, transmitted through an optical fiber, switched by the KVM Matrix Switch to another optical fiber, and then transformed back to an electronic form by the Velocity extender. The resulting signal is used by the shared peripherals.