Certification Report

Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b)

Sponsor and developer:	***Cisco Systems Inc.*** 170 West Tasman Dr. San Jose, CA 95134 USA
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Reportnumber:	**NSCIB-CC-58905-CR**
Report version:	**1**
Projectnumber:	**NSCIB-CC-58905**
Authors(s):	**Denise Cater**
Date:	07 April 2017
Number of pages:	18
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number
CC-17-58905

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer
Cisco Systems Inc.
170 West Tasman Dr., San Jose, CA 95134, USA

Product and assurance level
Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b),

Assurance Package:

- EAL2

Project number
NSCIB-CC-58905

Evaluation facility
Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. 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 Netherlands scheme for certification in the area of IT security [NSCIB] 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 TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity
Date of issue : **11-04-2017**
Certificate expiry : **11-04-2022**

Registration number
PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

A part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b), which is shortened to “UCS System” in the remainder of this section. The developer of the UCS System is Cisco Systems Inc. located in San Jose, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a unified computing solution, which provides access layer networking and servers. The TOE consists of hardware and software components that support Cisco's unified fabric, which run multiple types of data-center traffic over a single converged network adapter. The UCS features a role based access control policy to control the separation of administrative duties and provide a security log of all changes made.

A single Cisco Unified Computing System scales to up to forty chassis and three hundred twenty blade servers or rack-mount servers, all of which are administered through a single management entity called the Cisco UCS Manager. The Cisco UCS consists of the following primary hardware elements – Cisco UCS 5108 Blade Server Chassis, Cisco UCS Blade Servers (B200 M3, B200 M4, B260 M4, B420 M3, B420 M4, and B460 M4), Cisco UCS Rack Servers (C220 M3, C220 M4, C240 M3, C240 M4, and C460 M4), Virtual Interface Cards (see listing in section 2.6), Cisco UCS Fabric Interconnects (6248UP, 6296UP, 6332, 6332-16UP, and 6324), and Cisco UCS Fabric Extenders (2232PP, 2204XP, 2208XP, and 2304). The Fabric Interconnects and Fabric Extenders are based on the same switching technology as the Cisco Nexus 5000 Series. Fabric Interconnects also provide additional centralized management capabilities that form the basis of the Cisco UCS Manager.

Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. The result of this network unification is a reduction by up to two-thirds of the switches, cables, adapters, and management points. All devices in a system remain under a single management domain, which remains highly available through the use of redundant components.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on April 04 2017 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the UCS System, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the UCS System are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL2augmented (EAL2(+)) assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the UCS System, 3.1(2b) evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b) from Cisco Systems Inc. located in San Jose, USA. Hereinafter the TOE name is shortened to “UCS System”.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Cisco UCS 5108 Blade Server Chassis	n/a
	Cisco UCS Blade Servers (B-Series): Cisco UCS B200 M3, UCS B200 M4, UCS B260 M4, UCS B420 M3, UCS B420 M4, and UCS B460 M4	n/a
	Cisco UCS Rack Servers (C-Series): UCS C220 M3, UCS C220 M4, UCS C240 M3, UCS C240 M4, and UCS C460 M4	n/a
	Virtual Interface Cards compatible with B-series servers: Cisco UCS VIC 1240, Cisco UCS VIC 1280, Cisco UCS VIC 1340, Cisco UCS VIC 1380, Cisco UCS 82598KR-10 Gigabit Ethernet Network Adapter, Cisco UCS M71KR-Q QLogic Converged Network Adapter, Cisco UCS M71KR-E Emulex Converged Network Adapter, Cisco UCS M81KR Virtual Interface Card, Cisco UCS M72KR-Q QLogic Converged Network Adapter, Cisco UCS M72KR-E Emulex Converged Network Adapter, Cisco UCS M61KR-I Intel Converged Network Adapter, Cisco UCS NIC M51KR-B Broadcom BCM57711 Network Adapter	n/a
	Virtual Interface Cards compatible with C-series servers: Cisco UCS VIC 1225, Cisco UCS VIC 1225T, Cisco UCS VIC 1285, Cisco UCS P81E Virtual Interface Card, Emulex OneConnect Universal Converged Network Adapter, QLogic QLE8152 Dual Port 10 Gb Ethernet to PCIe Converged Network Adapter, Cisco UCS X520 Intel Converged Network Adapter, Broadcom NetXtreme II 5709 Quad Port Ethernet PCIe Adapter Card with TOE and iSCSI HBA, Broadcom NetXtreme II 57711 Dual Port 10 Gb Ethernet PCIe Adapter Card with TOE and iSCSI HBA, Emulex LightPulse LPe11002 4 Gbps Fibre Channel PCI Express Dual Channel HBA, QLogic SANblade QLE2462, Dual Port 4 Gbps Fibre Channel to PCI Express HBA	
	Cisco UCS Fabric Interconnects: Cisco UCS 6248UP, UCS 6296UP, UCS 6332, UCS 6332-16UP, and UCS 6324	n/a

	Cisco UCS Fabric Extenders: Cisco Nexus 2232PP, UCS 2204XP, UCS 2208XP, and UCS 2304	n/a
Software	Cisco Unified Computing System (UCS) Manager: Unified Computing System (UCS) Complete Software Bundle version 3.1(2b) which includes Cisco UCS Manager 3.1(2b), and the UCSM Client GUI Java-based applet	3.1(2b)

To ensure secure usage a set of guidance documents is provided together with the UCS System. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TOE are:

- The TOE provides the ability to audit the actions taken by authorized administrators. Audited events include start-up and shutdown, configuration changes, administrative authentication, and administrative log-off. With the exception of failed attempts to connect to the TOE via SSHv2[2], all audit data is stored locally. Regardless of standalone or clustered configuration, the TOE may be configured to send records to an external syslog server
- The TOE supports two methods of authenticating administrator logins on the Cisco UCS Manager: a local user database of passwords (and optionally SSH keys) or a remote authentication server accessed either via LDAP, RADIUS, or TACACS+.
- The TOE can be managed using the graphical user interface (over TLS1.0/1.1/1.2), the command line (over SSHv2 or by local console access via the RS-232 port), or by manipulating an XML API. The TOE provides administrative services to:
  - Manage UCS hardware
  - Manage UCS resources
  - Perform server administration, network administration and storage administration tasks within a CISCO UCS Instance
- The TOE provides network separation based on policies configured for VLANs and VSANs
  - VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN.
  - Virtual SAN (VSAN) technology partitions a single physical Storage Area Network (SAN) into multiple VSANs. VSAN capabilities allow the Cisco UCS 6200 Series Fabric Interconnect Hardware to logically divide a large physical fabric into separate isolated environments to improve SAN scalability, availability, manageability, and network security. Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups.
  -
- The TOE provides role based access control to restrict/authorize system access for different administrative user types. These are based on Privileges, roles and Locales:
  - Privileges give their holder access to specific system resources and permission to perform specific tasks. Privileges can be added to the default roles (except the

[2] Failed attempts to connect to the TOE via SSHv2 are only logged to a remote syslog server.

    - 'Administrator' and 'Read-Only' roles), and new custom roles can be created with custom-defined sets of privileges.
    - User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles.
    - A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access is limited to the organizations specified in the locale. Access control based on locales is enforced on all roles, including the full access Administrator role. A locale without any organizations may be created, this grants unrestricted access to system resources in all organizations.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 3.1 and 3.2 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.4 Architectural Information

The general architecture consists of four subsystems:

- The Fabric Interconnect (FI) subsystem providing:
    - Unifying up to 320 servers within a single system domain
    - Connecting every server resource in a system
    - An execution platform for the UCS Manager server software that provides:
        - General OS functionalities.
        - Security audit
        - Cryptography
        - Data protection by using role-based access control and information flow control
        - Identification and authentication
        - User management
        - Protection of the TSF
- The Fabric Extender (FEX) subsystem providing:
    - Traffic aggregation/de-aggregation between FI and servers
- The Processing Node subsystem in which only CMIC chip and vNIC are part of the TOE:
    - CIMC monitors physical state of the servers' hardware.
    - CIMC supports OS independent/pre-OS management.
    - vNIC (Virtual network interface card) sends/receives information to the FI and user traffic to FI.
- The UCS Manager Client Subsystem which is a java-based application running in a non-TOE browser on a non-TOE workstation:
    - It is used to connect to the UCS Manager server running on the FI and perform management operations.
    - The UCS Manager Client Subsystem makes no decision as the FI subsystem decides whether actions are allowed.

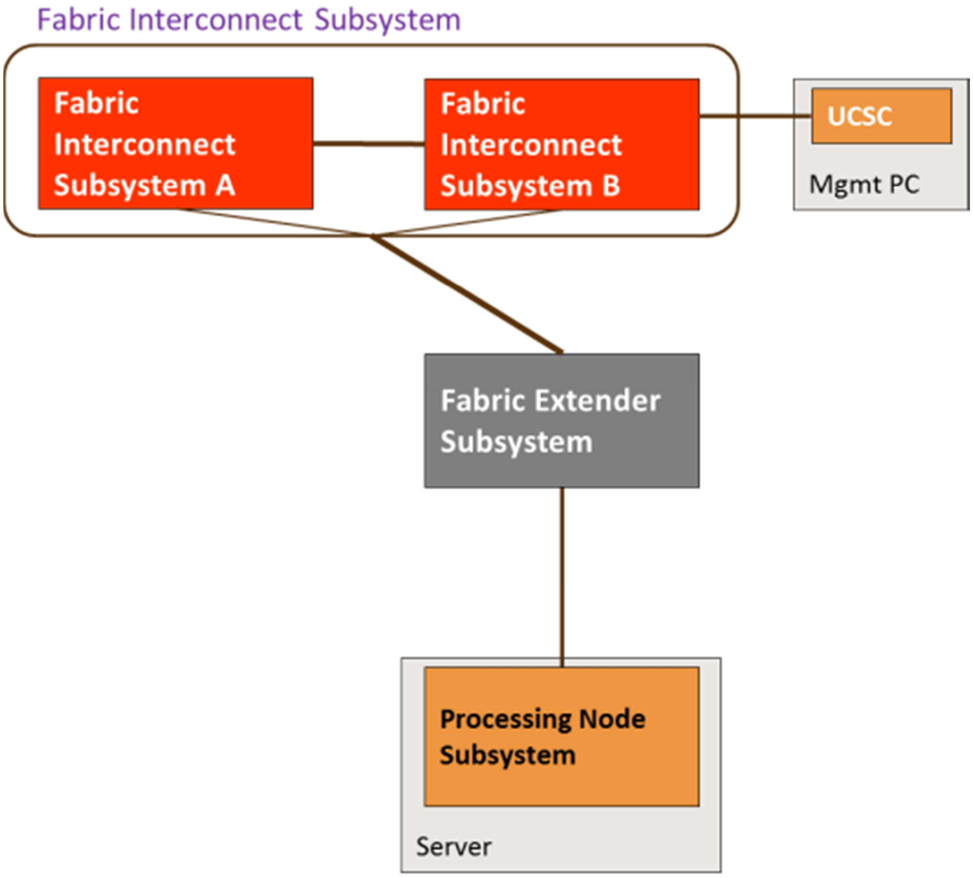
Fabric Interconnect Subsystem
Fabric Interconnect Subsystem A
Fabric Interconnect Subsystem B
UCSC
Mgmt PC
Fabric Extender Subsystem
Processing Node Subsystem
Server

Figure 1 TOE Architecture

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Cisco Unified Computing System (UCS), version 3.1(2b) Common Criteria Operational User Guidance and Preparative Procedures	1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer tests consist of forty-two (42) tests, some of which were quite extensive. These tests cover all TSFI and all SFRs and include both positive and negative tests. Brightsight repeated eight (8) of the forty-two developer tests.

In addition to the developer tests, the evaluator derived and executed nine (9) additional functional tests.

2.6.2 Independent Penetration Testing

The evaluators performed twenty-one (21) penetration tests. These were derived from a vulnerability analysis comprised of 3 parts:

1. Public domain vulnerability analysis of TOE specific vulnerabilities (vulnerabilities specific for Cisco UCS 3.1(2b));
2. Public domain vulnerability analysis of TOE-type vulnerabilities (vulnerabilities that are generic for switches and management of switching components, including VLAN switching, VSAN switching, SSH and TLS);
3. Analysis of TOE deliverables (AGD, FSP, TDS etc.);
4. Execution of vulnerability scanning tool to identify additional potential vulnerabilities.

The evaluators considered the potential vulnerabilities in the context of the attack paths identified (as shown in Figure 2 below):

- ➢ Attacks on the Fabric Interconnects
- ➢ Attacks on the infrastructure to the servers (downlinks)
- ➢ Attacks on the Fabric Interconnects management interface
- ➢ Attacks on the links between the FI and FEX (or between the FIs)

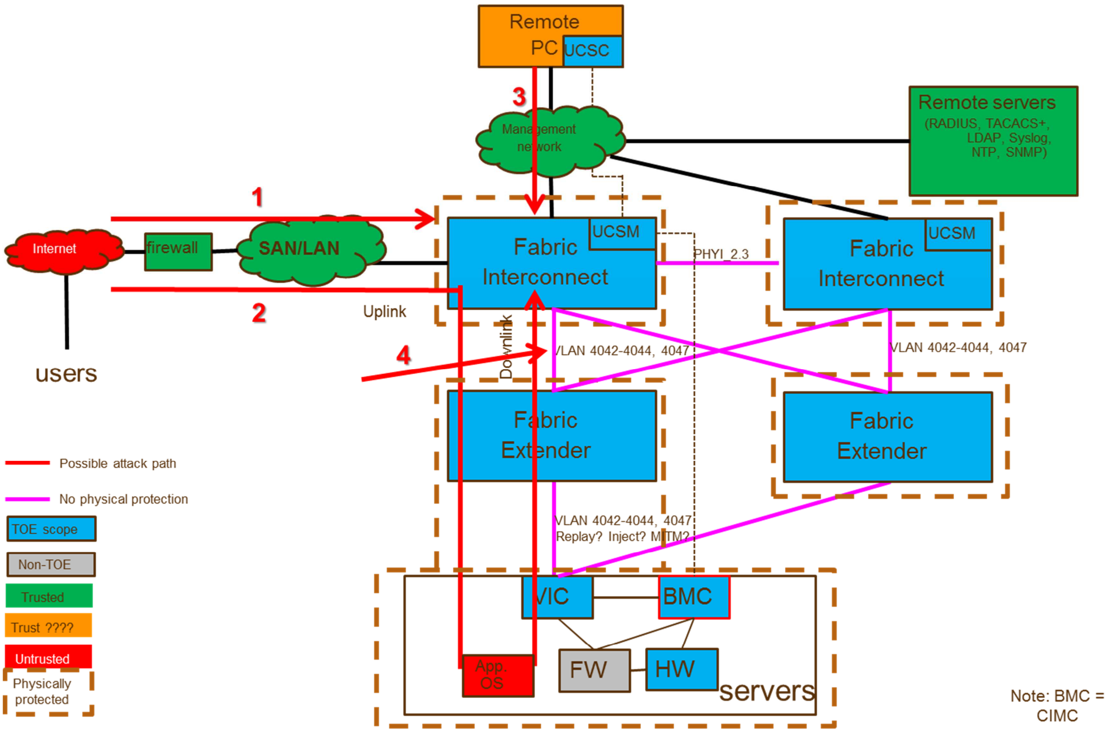

Figure 2 Attack paths

2.6.3 Test Configuration

The network diagram in Figure 3 describes the overall setup of the lab used for developer and evaluator testing. Ports are labelled as follows:

Port	Type	Description	Purpose
Management PC (environment)			
SER	Console	A standard RS-232 serial port for CLI management	For serial command line testing UCS Manager CLI.
EH	Ethernet	Management port	UCS Manager GUI (UCSC)
UCS-FI-6248UP (TOE hardware)			

Port	Type	Description	Purpose
CO	Console	A standard RS-232 serial port for CLI management	For serial command line testing - UCS Manager CLI.
FM	Ethernet	Management port	UCS Manager GUI (UCSC)
UPLINK	SFP	Ethernet port 1/18 to Catalyst 3850	Acting as the upstream network
LD	SFP	Ethernet port 1/1 and 1/2 configured as a server port	Testing VLAN configuration via fabric extender
MA	SFP	Monitoring port	VLAN monitoring
N2K-C2232PP (TOE hardware)			
LU	SFP	Uplink port 1/1 and 1/2	To extend the FI's I/O module managed by UCS-FI-6248UP.
LS	SFP	Downlink port	To extend the FI's I/O module managed by UCS-FI-6248UP.
UCSC-C220-M3 (TOE hardware)			
UC	SFP (vNIC 1225T)	A Cisco VIC 1225T vNIC connected to the Fabric Extender	Testing VLAN configuration. Provides access to the virtual machines
Catalyst 3850 (environment switch)			
3K	Ethernet	Ethernet port to UCS-FI-6248UP	Upstream network testing
AK	Ethernet	Ethernet port to 'attacker-2'	Upstream network testing
'attacker-2' (environment)			
EA	Ethernet	Ethernet port to Catalyst 3850	Upstream network testing
Testing PC (environment)			
TD	SFP	Monitoring port	VLAN monitoring

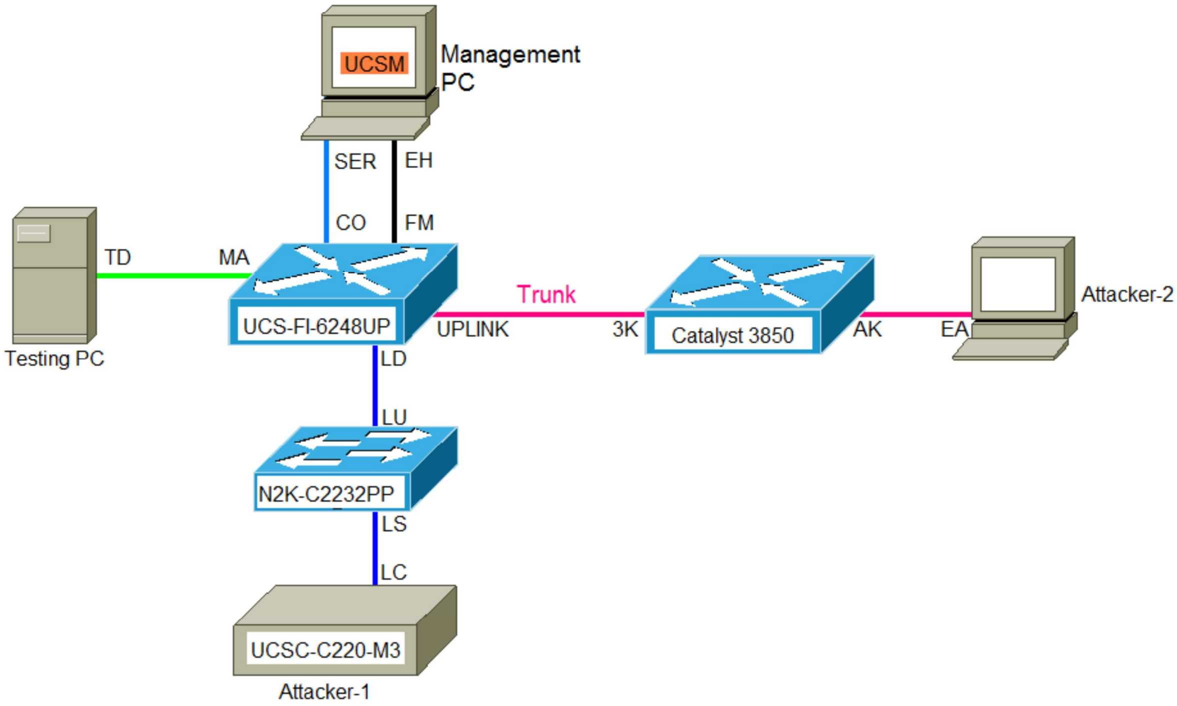

Figure 3 Test Configuration

Test cases load a baseline configuration (verified to match the security guidance provided in [AGD]) on the TOE before configuring the TOE into the state necessary for the test case to proceed. The baseline configuration has been created by the Evaluator and saved in flash memory on the TOE.

Device	Software Version
UCS-FI-6248UP	3.1(2b)
N2K-C2232-PP	N/A
UCSC-C220-M3	3.1(2b)c[3]

The following tools were used for testing:

Description	Package Name	Platform	Version	Related test cases
Management PC				
Operating system	Windows 7 professional SP1	X86_64	6.1.7601	All (testing environment)
Terminal	putty	X86_64	2011-1’2-1’9:r9371	All (testing environment)
Web browser	Firefox	X86_64	50.0	All (testing environment)
Java	Java	X86_64	8 update 101, (build 1.8.0_101-b13)	All (testing environment)
Java JRE	Java	X86_64	1.7.0_79	All (testing environment)
Snmp MIB browser	iReasoning MIB browser	X86_64	11.0 (build 4010)	2.1.8

[3] UCS 3.1(2b) software packages contain 3 bundles: A bundle for the fabric interconnect, B bundle for the B series servers, and C bundle for the C series servers. The suffix “c” here indicates the C bundle running on the UCSC-C220-M3 server because it is a C series server.

Description	Package Name	Platform	Version	Related test cases
SSH Client	bitvise SSH client.	X86_64	6.31	3.3.3
XML API	UCSMSDK	X86_64	0.9.2.0	2.2.7
'attacker-1' (UCSC-C220-M3)				
Operating system	Kali	X64	Linux version 4.6.0-kali1-amd64	All (testing environment)
VLAN hopping	Python-scapy	X64	2.2.0-1'kali1	3.2.1, 3.2.2
VLAN hopping	Yersinia framework	X64	0.7.3	3.2.1, 3.2.2
Packet capture	Tcpdump	X64	4.6.2	All (testing environment)
Packet capture	Wireshark	X64	2.2.0	All (testing environment)
Complier	gcc	X64	5.4.0 20160609	All (testing environment)
'attacker-2' PC				
Operating system	Kali	X64	Linux version 4.6.0-kali1-amd64	All (testing environment)
VLAN hopping	Python-scapy	X64	2.2.0-1'kali1	3.1.4, 3.1.5, 3.3.11
Packet capture	Tcpdump	X64	4.6.2	All (testing environment)
Packet capture	Wireshark	X64	2.2.0	All (testing environment)
Complier	gcc	X64	5.4.0 20160609	All (testing environment)
SSH Client Software	openssh-client	X64	6.7p1	All (testing environment)
Python dependency	python-pexpect	X64	3.2-1'	All (testing environment)
Python dependency	python-scapy	X64	2.2.0-1'kali1	All (testing environment)
ARP spoofing	arpspoof	X64	2.4	3.1.2
MAC flooding	dsniff	X64	2.4	3.1.3
MAC flooding	macof	X64	1.0	3.1.3
Firefox	Mozilla Firefox	X64	45.3.0	All (testing environment)
Network enumeration	nmap	X64	6.49BETAA4	3.3.1
XSS vulnerabilities	XSSer	X64	3.0.0.a2	3.3.4
IP stack integrity checker	isic	X64	0.07	3.3.7
Password attacks	Hydra	X64	8.1	3.3.5
Vulnerability scan tool	Nessus	X64	6.5.2	2.2.8
Fast SSL/TLS scanner	sslscan	X64	1.10.5-static	3.3.2
Cryptography toolkit	Openssl	X64	1.0.2e-dev	All (testing environment)
Hypertext transfer protocol server	Apache	X64	2.0	3.3.1
Web Application vulnerability scanner	Zap-proxy	X64	2.4.1	3.3.1
Web Application	Burp	X64	1.6.01	3.3.1

Description	Package Name	Platform	Version	Related test cases
vulnerability scanner				
Web Application Attack and audit framework	W3af	X64	1.6.54	3.3.1
Open source web application security platform	vega	X64	1.0	3.3.1
Testing PC				
Operating system	Debian 8 (Jessie)	X64	Linux kernel 3.16	All (testing environment)
Packet capture	Tcpdump	X64	4.6.2	All (testing environment)
Ethernet Bridging	bridge-utils	X64	1.5-9	3.4.1

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b). Details of the hardware models included in the TOE are provided in Section 2.1.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[4] which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C-Series Rack-Mount Servers, 2200/2300 Series Fabric Extenders, and 6200/6300 Series Fabric Interconnects with Unified Computing System (UCS) Manager 3.1(2b), to be CC Part 2 conformant, CC Part 3 conformant, and to meet the requirements of EAL 2.This implies that the product satisfies the security technical requirements specified in Security Target Cisco Unified Computing System (UCS) Security Target, v1.0, 06 April 2017.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

The customer is responsible for configuring secure connections between the TOE and any time, authentication and syslog servers, as described in the user guidance. Furthermore, the customer is responsible for ensuring **all** components of the TOE, the UCS System, are to be located in the same physically protected area.

[4] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The TOE supports additional protocols to those that are enabled in the evaluated configuration. Enabling these additional protocols may lead to the TOE no longer meeting the SFRs.

Although all login attempts for GUI and CLI are logged, only successful login attempts are logged in the local audit log and can be viewed on the TOE. Failed authentication attempts are not logged to the local audit log but sent to an external Syslog only. The failed attempt of using SSH to login the CLI is also only logged to an external syslog server only. Therefore if the user needs to review the failed login attempts, an external syslog is required.

It should be noted that when a user's privilege is modified while that user is still logged in, the change is not take effect until the user is re-logged in. Therefore the administrator needs to make sure if the privilege of a user is changed, this user must be logged off.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

3 Security Target

The Security Target Cisco Unified Computing System (UCS) Security Target, v1.0, 06 April 2017 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

ACL	Access Control List
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LAN	Local Address Network
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
RBAC	Roles-Based Access Control (management)
SSH	Secure Shell
TOE	Target of Evaluation
VLAN	Virtual LAN
VSAN	Virtual SAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III version 3.1, revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.
[ETR]	Evaluation Technical Report Cisco Unified Computing System (UCS) - EAL2, 17-RPT-110, Version 3.0, 07 April 2017.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[ST]	Cisco Unified Computing System (UCS) Security Target, v1.0, 06 April 2017.

(This is the end of this report).