



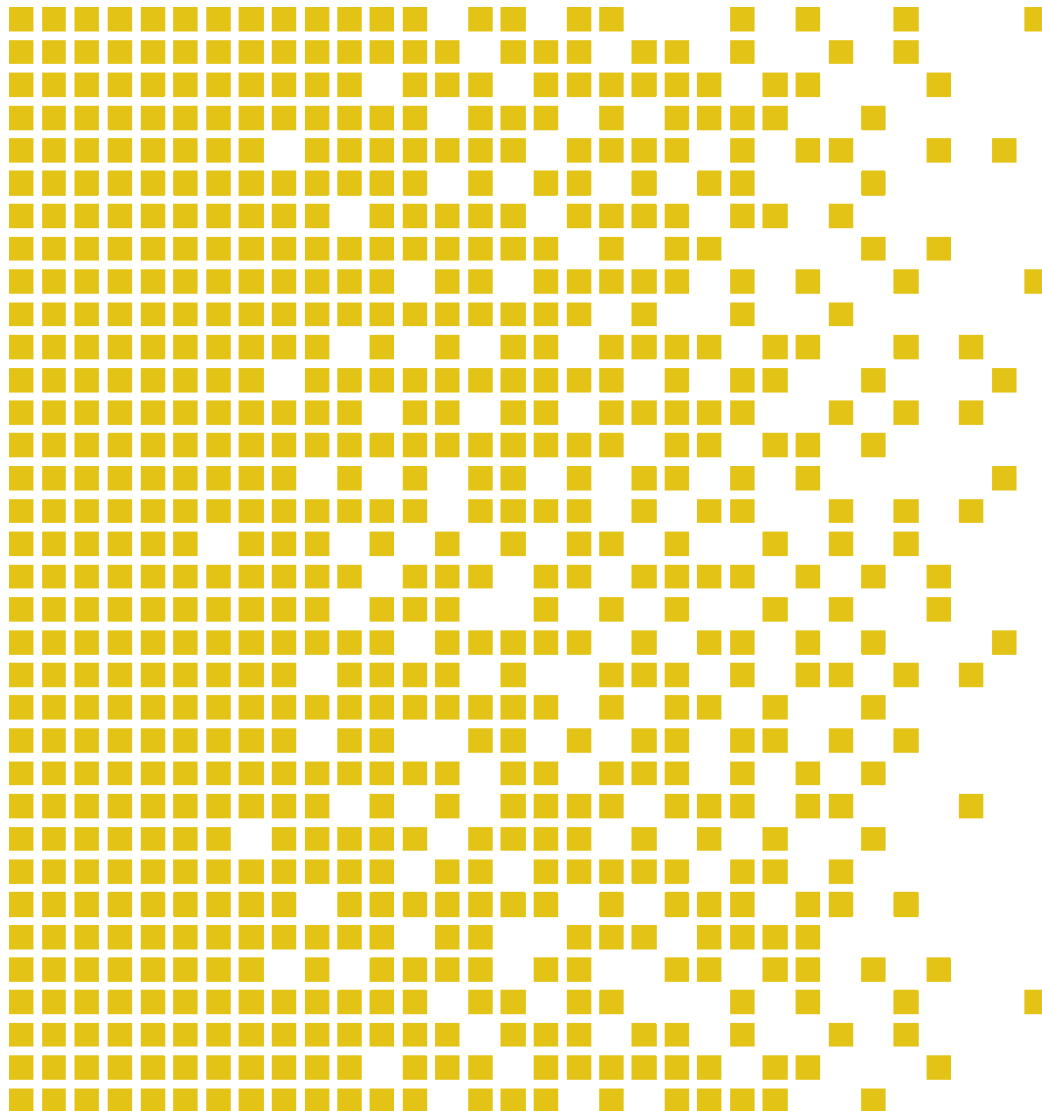
**SERTIT**

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

# SERTIT-100 CR Certification Report

Issue 1.0 19 April 2018

Zyxel ZyWALL VPN Firewall series with ZLD V4.30



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

**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. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC\_FLR CC part 3 components.



**MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY  
EVALUATION CERTIFICATES (SOGIS MRA)**

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

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.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.






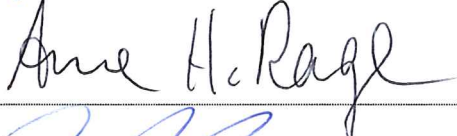
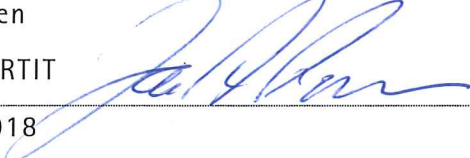
## Contents

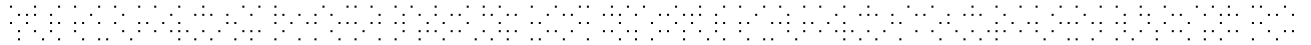
1	Certification Statement	4
2	Abbreviations	5
3	References	6
4	Executive Summary	7
4.1	Introduction	7
4.2	Evaluated Product	7
4.3	TOE scope	7
4.4	Protection Profile Conformance	7
4.5	Assurance Level	7
4.6	Security Policy	7
4.7	Security Claims	8
4.8	Threats Countered	8
4.9	Threats Countered by the TOE's environment	8
4.10	Threats and Attacks not Countered	9
4.11	Environmental Assumptions and Dependencies	9
4.12	IT Security Objectives	9
4.13	Non-IT Security Objectives	10
4.14	Security Functional Requirements	10
4.15	Security Function Policy	11
4.16	Evaluation Conduct	11
4.17	General Points	11
5	Evaluation Findings	12
5.1	Introduction	12
5.2	Delivery	13
5.3	Installation and Guidance Documentation	13
5.4	Misuse	13
5.5	Vulnerability Analysis	13
5.6	Developer's Tests	14
5.7	Evaluators' Tests	14
6	Evaluation Outcome	15
6.1	Certification Result	15
6.2	Recommendations	15
	Annex A: Evaluated Configuration	16
	TOE Identification	16
	TOE Documentation	16
	TOE Configuration	17
	Environmental Configuration	17

## 1 Certification Statement

Zyxel Communications Corporation ZYXEL ZyWALL VPN-Firewall series is a self-contained box consisting of hardware and firmware that provides stateful firewall and VPN-services for IPv4 and IPv6 networks.

ZYXEL ZyWALL VPN-Firewall series version v4.30 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) augmented requirements of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes
	Certifier 
Quality Assurance	Arne Høye Rage
	Quality Assurance 
Approved	Jørn Arnesen
	Head of SERTIT 
Date approved	19 April 2018



## 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
POC	Point of Contact
QP	Qualified Participant
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] Security Target, Zyxel Communications Corporation, Version 1.0, 2018-01-26.
- [2] Common Criteria Part 1, CCMB-2017-04-001, Version 3.1 R5, April 2017.
- [3] Common Criteria Part 2, CCMB-2017-04-002, Version 3.1 R5, April 2017.
- [4] Common Criteria Part 3, CCMB-2017-04-003, Version 3.1 R5, April 2017.
- [5] The Norwegian Certification Scheme, SD001E, Version 10.4, 20 February 2018.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 R5, April 2017.
- [7] Evaluation Technical Report, Version 2.0, 15 February 2018.
- [8] Zyxel ZyWALL VPN/USG/ATP Series CLI Reference Guide, version 4.30 Edition 1, 10/2017.
- [9] Zyxel ZyWALL VPN/USG/ATP Series User's Guide, Version 4.30 Edition 1, 10/2017.
- [10] Zyxel ZYWALL VPN Firewall Series with ZLD V4.30 compliant Firmware Operative and Preparative Guidance, Version 1.0, 26/01/2018.

## 4 Executive Summary

### 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of ZYXEL ZyWALL VPN-Firewall series version v4.30 to the Sponsor, Zyxel Communications Corporation, 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 version of the product evaluated was ZYXEL ZyWALL VPN-Firewall series and version v4.30.

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

The TOE is one of a series of Zyxel ZyWALL VPN Firewalls. Each TOE is a self-contained box consisting of hardware and firmware that provides stateful firewall and VPN-services for IPv4 and IPv6 networks. The ZYXEL ZyWALL VPN-Firewall series are business-grade VPN gateways fine-tuned to deliver the fastest VPN and firewall performance for the most performance-demanding deployments.

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

### 4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.3.1 and 1.3.2.

### 4.4 Protection Profile Conformance

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

### 4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2, augmented by ALC\_FLR.2. 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

There are no Organizational Security Policies or rules with which the TOE must comply.

## 4.7 Security Claims

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

The Security Target[1] defines one extended component: **FDP\_RUL\_EXT.1 Stateful Traffic Filtering**. This component specifies the stateful traffic filtering security function and therefore is a suitable member of the FDP class. It was added to explicitly specify the stateful firewall security function provided by the TOE.

## 4.8 Threats Countered

### ■ T.UNAUTHORIZED\_DATA

An attacker:

- sends data from one network to another network
- accesses services on one network from another network while not authorised to do so

### ■ T.READ\_MODIFY\_DATA

An attacker on a network reads traffic or modifies traffic on that network that comes from or through the TOE, or goes to or through the TOE and this is not desired.

### ■ T.UNAUTHORIZED\_ACCESS

An attacker gains unauthorised access to the TOE itself.

### ■ T.UNDETECTED\_ACTIONS

An attacker may take actions that adversely affect the security of the TOE or the networks it is connected to and these actions remain undetected and thus their effects cannot be effectively mitigated.

### ■ T.TSF\_FAILURE (some models, and only in HA configuration)

The TOE fails, and this causes networks to become unavailable to each other.

## 4.9 Threats Countered by the TOE's environment

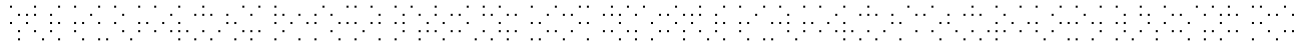
There are 2 threats partly countered by the TOE's environment:

### ■ T.UNAUTHORIZED\_ACCESS

An attacker gains unauthorised access to the TOE itself.

### ■ T.UNDETECTED\_ACTIONS





An attacker may take actions that adversely affect the security of the TOE or the networks it is connected to and these actions remain undetected and thus their effects cannot be effectively mitigated.

#### 4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

#### 4.11 Environmental Assumptions and Dependencies

- A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. Local management shall only take place within this physically secured environment. Any RADIUS and/or Syslog servers shall be similarly protected and their connections with the TOE shall be protected against access by attackers.

- A.SINGLE\_CONNECTION

Information cannot flow among the networks connected to the TOE unless it passes through the TOE.

- A.TRUSTED\_ADMIN

TOE Administrators are trusted to follow and apply

#### 4.12 IT Security Objectives

- O.DATA\_FLOW\_CONTROL

The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination.

- O.ENCRYPT

The TOE is able to protect the authenticity, confidentiality and integrity of traffic from, to or through the TOE by using IPSec- based encryption.

- O.PROTECTED\_MANAGEMENT

The TOE shall allow authenticated administrators to manage the TOE across protected communication channels.

- O.LOGGING

The TOE shall log security-relevant actions and allow only administrators to review them.

- O.HIGH\_AVAILABILITY (some models, and only in HA configuration)

The TOE shall be fault-tolerant.

#### 4.13 Non-IT Security Objectives

- OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. Local management shall only take place within this physically secured environment. Any RADIUS and/or Syslog servers shall be similarly protected and their connections with the TOE shall be protected against access by attackers.

- OE.SINGLE\_CONNECTION

The networks connected to the TOE shall be configured so that information cannot flow among them unless it passes through the TOE.

- OE.TRUSTED\_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

#### 4.14 Security Functional Requirements

- FDP\_RUL\_EXT.1
- FIA\_UID(Network).2
- FIA\_UAU(Network).1
- FTP\_ITC(IPSEC).1
- FMT\_SMF.1
- FMT\_MOF.1
- FTP\_ITC(SSH).1
- FTP\_ITC(HTTPS).1
- FMT\_SMR.1
- FIA\_UID(Management).2
- FIA\_UAU(Management).2
- FDP\_UIT.1
- FAU\_GEN.1
- FAU\_GEN.2
- FAU\_SAR.1
- FAU\_SAR.2
- FPT\_STM.1
- FRU\_FLT.2
- ALC\_FLR.2

#### 4.15 Security Function Policy

The TOE is one of a series of Zyxel ZyWALL VPN Firewalls. Each TOE is a self-contained box consisting of hardware and firmware that provides stateful firewall and VPN-services for IPv4 and IPv6 networks. The TOE resides between one or more internal (virtual) networks (that the TOE is protecting) and an external network such as the Internet.

#### 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 SD001[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 Brightsight Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 15 February 2018. 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 2 assurance package:

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification with complete summary
	ADV_TDS.1	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Production support, acceptance procedures and automation
	ALC_CMS.2	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	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 versions of its components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

## 5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance documents [8][9][10] provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

## 5.4 Misuse

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

The guidance documents adequately describe 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 use the TOE's security functions.

## 5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluator while performing other evaluation activities (ASE, ADV and AGD) considered direct attacks, monitoring and misuse attacks, to identify potential vulnerabilities.

The evaluator also, conducted a public domain vulnerability search to further search for potential vulnerabilities. Both TOE specific and TOE type search terms were used. The evaluator also used a vulnerability scanning tool (Nessus) to identify potential vulnerabilities.

The evaluator assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found however none of them turned out to be possibly exploitable.

## 5.6 Developer's Tests

The developer test plan covers all of the security functions listed in the Security Target [ST]. The test plan of the developer is quite extensive. The developer uses small test case scenarios to test the TOE. These small test cases are then grouped by function into a test suite . The developer has 11 test suites covering the following areas:

- Interface Ethernet testing for IPv4
- Interface Ethernet testing for IPv6.
- VLAN Interface Ethernet testing for IPv4
- VLAN Interface Ethernet testing for IPv6.
- Routing protocols.
- IPsec VPN.
- High Availability.
- Object. (User Authentication, Management Authentication)
- Firewall IPv4.
- Firewall IPv6.
- Logging. (System & Maintenance & Object Reference)

## 5.7 Evaluators' Tests

ATE\_IND.2 tests were performed on the final version of the TOE at Brightsight's Delft premises between 11 December 2017 and 19 January 2018.

The evaluator sampled 3 test cases, based on the claims made in the Security Target. The evaluator devised a subset of 10 tests that focused on the firewall functionality of the TOE and one routing test to be executed on the TOE.



## 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 ZYXEL ZyWALL VPN-Firewall series version v4.30 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on platforms specified in Annex A.

### 6.2 Recommendations

Prospective consumers of ZYXEL ZyWALL VPN-Firewall series version v4.30 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 above under 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.

## Annex A: Evaluated Configuration

### TOE Identification

The TOE consists of:

Hardware	Firmware	Purpose of the model	HA-Pro
USG20-VPN	V4.30(ABAQ.0)	Provides first-line defense to guard small business from network threats from remote access and within the internal network environment.	No
USG40	V4.30(AALA.0)		No
USG60	V4.30(AAKY.0)		No
VPN50	V4.30(ABHL.0)		No
USG110	V4.30(AAPH.0)	Unified Security Gateway integrated with complete, enterprise-level and advanced security solutions designed for Remote office and Small to Medium Business (SMB).	Yes
USG210	V4.30(AAPI.0)		Yes
USG310	V4.30(AAPJ.0)		Yes
ZyWALL 110	V4.30(AAAA.0)	VPN Firewall Gateway integrated with complete, enterprise-level and advanced security solutions designed for Remote office and Small to Medium Business (SMB)	Yes
ZyWALL 310	V4.30(AAAB.0)		Yes
VPN100	V4.30(ABFV.0)		Yes
VPN300	V4.30(ABFC.0)		Yes
USG1100	V4.30(AAPK.0)	Unified Security Gateway integrated with complete, enterprise-level and advanced security solutions designed for enterprise.	Yes
USG1900	V4.30(AAPL.0)		Yes
ZyWALL1100	V4.30(AAAC.0)	VPN Firewall Gateway integrated with complete, enterprise-level and advanced security solutions designed for enterprise.	Yes
USG2200-VPN	V4.30(ABAE.0)		Yes

### TOE Documentation

The supporting guidance documents evaluated were:





- [a] Zyxel ZyWALL VPN/USG/ATP Series CLI Reference Guide , version 4.30 Edition 1, 10/2017.
- [b] Zyxel ZyWALL VPN/USG/ATP Series User’s Guide, Version 4.30 Edition 1, 10/2017.
- [c] Zyxel ZYWALL VPN Firewall Series with ZLD V4.30 compliant Firmware Operative and Preparative Guidance, Version 1.0, 26/01/2018.

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

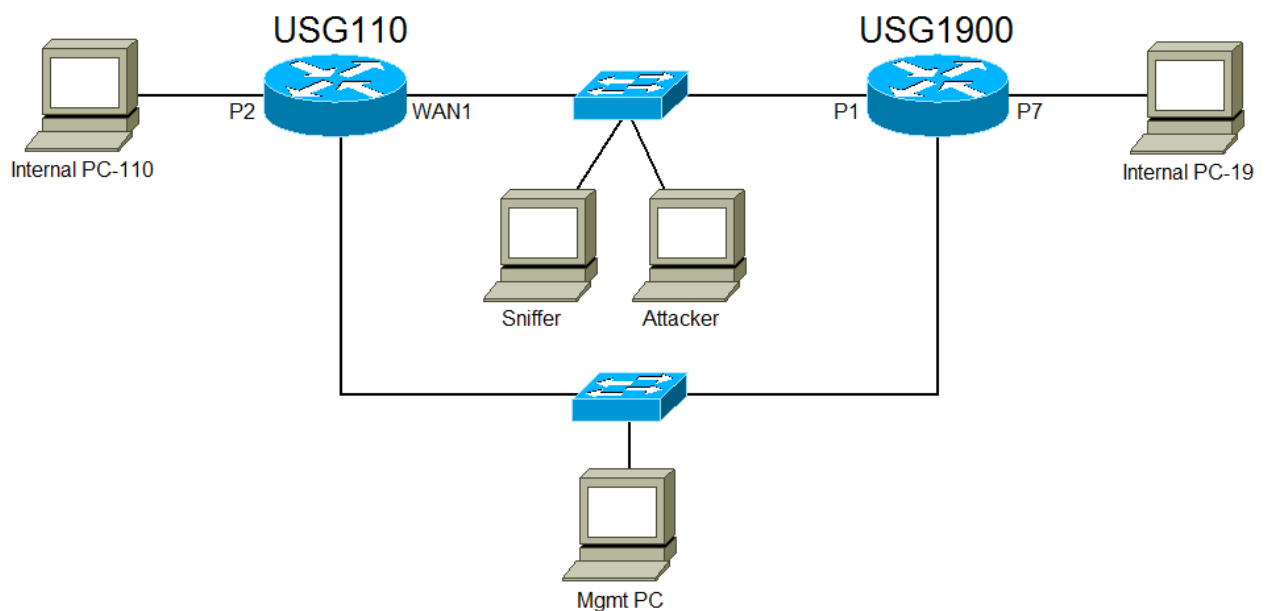
### TOE Configuration

The following configuration was used for testing:

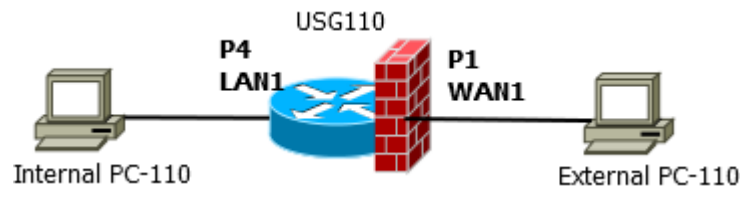
ITEM	IDENTIFIER
HARDWARE	One of the hardware models from each series listed in section TOE Identification
SOFTWARE	V4.30
MANUALS	[8] Zyxel ZyWALL VPN/USG/ATP Series CLI Reference Guide , version 4.30 Edition 1, 10/2017 [9] Zyxel ZyWALL VPN/USG/ATP Series User’s Guide, Version 4.30 Edition 1, 10/2017 [10] Zyxel ZYWALL VPN Firewall Series with ZLD V4.30 compliant Firmware Operative and Preparative Guidance, Version 1.0, 26/01/2018

### Environmental Configuration

The TOE is tested in the following test setups:



**Figure. Network setup for repeat, routing and penetration testing**



**Figure. Network setup for firewall testing**



# Certificate

*The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate.*

*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 Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced.*

*Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects 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 of this certificate. This certificate is not an endorsement of the*

*IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.*

**Product Manufacturer:** Zyxel Communications Corporation

**Product Name:** Zyxel ZyWALL VPN Firewall series

**Type of Product:** Firewall

**Version and Release Numbers:** See Security Target

**Assurance Package:** EAL 2 augmented with ALC\_FLR.2

**Evaluation Criteria:** Common Criteria v. 3.1 R4

**Name of IT Security Evaluation Facility:** Brightsight B.V.

**Name of Certification Body:** SERTIT

**Certification Report Identifier:** SERTIT-100 CR Issue 1.0; 19. April 2018

**Certificate Identifier:** SERTIT-100 C

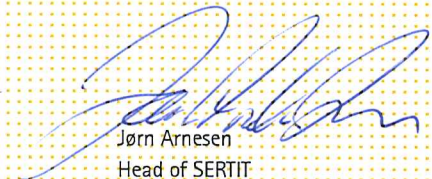
**Date Issued:** 19. April 2018



Kjartan Jæger Kvassnes  
Certifier



Arne Høye Rage  
Quality Assurance



Jørn Arnesen  
Head of SERTIT



CCRA recognition for components up  
EAL 2 and ALC\_FLR only.



SOGIS MRA recognition for  
components up to EAL 4.