Zyxel ZyWALL VPN Firewall series with ZLD V4.30 compliant firmware

Security Target

/

Document history

Version	Date	Comment
0.1	31-5-2017	First draft
0.2	07-06-2017	Second version, release to Zyxel
0.3	16-06-2017	Based on Zyxel comments and first evaluation round
0.4	15-08-2017	Removed IP Options from FDP_RUL and further on Added that IPsec also provides authenticity
0.5	11-09-2017	Corrected firmware versions, removed PVLANs.
0.6	19-10-2017	Update Physical scope
0.7	22-01-2018	Updated according to evaluator comments
1.0	26-01-2018	Change version to 1.0

Distribution list

- Zyxel
- SERTIT
- Brightsight

/

Contents

/

1 Security Target Introduction

1.1 Identifiers

ST Title	Zyxel ZyWALL VPN Firewall series with ZLD V4.30 compliant firmware Security Target
ST Version	See Document History
ST Date	See Document History
TOE Identification	Zyxel ZyWALL VPN Firewall series with ZLD V4.30 compliant firmware
Developer	Zyxel
TOE Type	VPN Firewall

1.2 TOE Overview

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. An example may be found in Figure 1.

.

Figure 1 The Zyxel USG1900 (front and back view).

/

The TOE resides between one or more internal (virtual) networks (that the TOE is protecting) and an external network such as the Internet. An example setup, with two TOEs, each protecting a network may be found in Figure 2.

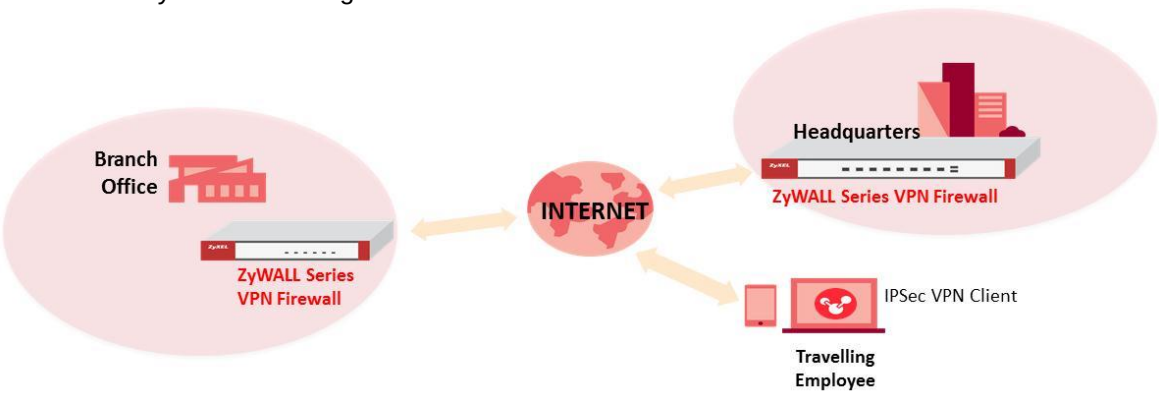


Figure 2 A typical setup

Businesses deploy network security appliances for two main purposes: to protect company resources against a multitude of threats and to enable secured communications between multiple locations via Virtual Private Network (VPN). For many years, Zyxel's highly-acclaimed Unified Security Gateway (USG) Series has helped businesses satisfy all these demands. Fortifying businesses against a new generation of threats, Zyxel is offering a new line of Next Generation Unified Security Gateways that deliver unmatched capacity, performance and protection for businesses of all sizes.
On the other hand, business operations today are more mobile, more global, and more dynamic than ever. This, combined with the use of advanced or bandwidth consuming applications in the workplace, has created great demand for even faster VPN and firewall performance. To satisfy this demand, Zyxel has introduced the all-new ZyWALL Series VPN Firewalls. Zyxel's new ZyWALL VPN Firewalls are business-grade VPN gateways fine-tuned to deliver the fastest VPN and firewall performance for the most performance-demanding deployments.

The TOE provides the following major security features:

- Firewall
- User authentication
- IPSec VPN
- Secure Management
- Management Authentication
- Secure Routing
- VLANs
- Logging
- IPv4/IPv6
- High Availability (not all models)

/

1.2.1 HW/SW required by the TOE

The TOE requires the following hardware/software to be available in its environment

Component	Required	Usage/Purpose Description for TOE performance
Local Console	At least one of these three is required	A console that is directly connected to the TOE via the Console Port
Management Workstation with SSH Client		A workstation with an SSH client that supports SSHv2 and is (in)directly connected to the TOE via a network port.
Management Workstation with HTTPs browser		A workstation with a browser supporting HTTPs and is (in)directly connected to the TOE via a network port.
Syslog Server	No	A syslog server to which the TOE can transmit syslog messages.
RADIUS Server	No	A RADIUS server that provides authentication services.

1.3 **TOE Description**

1.3.1 Physical Scope

1.3.1.1 List of TOE parts

The TOE consists of different hardware models, each with its own firmware[1]. The model-firmware combinations are listed below. Some of the models support a feature called HA-Pro (High Availability), and this is also noted in the table[2].

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	Yes
ZyWALL 310	V4.30(AAAB.0)		Yes

[1] Each firmware version is different, because functionality that is not supported by a model is not compiled into the firmware and because drivers are different for different hardware models. As far as the security functionality described in this ST is concerned, all firmware versions are equivalent (with the exception of the HA functionality).

[2] The remainder of this ST will state that HA is "not available in all models". Use this table to determine which models do and which models do not support HA.

VPN100	V4.30(ABFV.0)	advanced security solutions designed for Remote office and Small to Medium Business (SMB)	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

The TOE hardware can be ordered from Zyxel headquarters or resellers and is delivered by a courier, and all the firmware are provided together with the TOE hardware. Or the user needs to register their products and create an account at myzyxel.com to download the latest version of the firmware.

Guidance
Zyxel ZyWALL VPN/USG/ATP Series CLI Reference Guide , version 4.30 Edition 1, 10/2017
Zyxel ZyWALL VPN/USG/ATP Series User's Guide, Version 4.30 Edition 1, 10/2017
Zyxel ZYWALL VPN Firewall Series with ZLD V4.30 compliant Firmware Operative and Preparative Guidance, <Version 1.0, 26/01/2018>

All the manuals are provided in the PDF format, and can be downloaded from the Zyxel website (http://www.zyxel.com)

1.3.2 Logical Scope

The TOE offers the following security features (on IPv4 and IPv6, all security claims apply equally to both):

Firewall

Administrators can provide rules to be used by the TOE to restrict the flow of traffic between the various networks connected to the TOE. Rules can be based on various traffic properties such as source and/or destination address, source and destination ports etc.

User authentication

The TOE can force users to authenticate themselves (with username and password) before they can establish sessions through the TOE. Web requests of unauthenticated users are redirected to a login page, all other traffic of unauthenticated users is simply dropped. Once the user has authenticated himself, traffic goes through normally (subject to other firewall rules).

IPSec VPN

/

The TOE can initiate and/or accept IPSec connections for traffic that needs authenticity, confidentiality and integrity protection.

Secure Management

The TOE can be managed by administrators as follows:

- CLI through the console port
- CLI over SSHv2
- Web interface over HTTPs

Management Authentication

Managers must authenticate themselves by:

- Username/password, using:
  - Local authentication, or
  - An external RADIUS server
- Certificates

before they can use the TOE

Authenticated Routing

The TOE supports authenticated routing for the following protocols:

- RIPv2
- OSPFv2
- BGPv4

VLANs

The TOE supports VLANs.

Logging

The TOE can be configured to log a wide range of events. These can be stored in memory, written to an external USB-device or to an external syslog server

HA-Pro (High Availability)

Two copies of the TOE can be placed in parallel, such that if one copy fails, the other automatically takes over, thereby guaranteeing much higher availability. This functionality is not available in some models.

/

2 Conformance claims

The TOE and ST conform to the Common Criteria (CC) Version 3.1, Revision 5, dated April 2017. The TOE and ST CC Part 2 extended and CC Part 3 conformant. The TOE and ST are EAL2 package-augmented with ALC_FLR.2.

No conformance is claimed to any Protection Profile.

/

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- Threats that must be countered by the TOE or its environment

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name.

3.1 **Assumptions**

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Definition
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 all administrator guidance in a trusted manner.

3.2 **Threats**

The following table lists the threats addressed by the TOE and its environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
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.

/

Threat	Threat Definition
T.TSF_FAILURE (some models, and only in HA configuration)	The TOE fails, and this causes networks to become unavailable to each other.

/

4 Security Objectives

4.1 Security Objectives for the TOE

Objective	Definition
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.

4.2 Security Objectives for the Operational Environment

Objective	Definition
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.

/

5 Security Functional Requirements

Notes:

- Selections and assignments have been underlined.
- Various refinements have been made in the requirements (**in bold**). In general these were meant to improve readability. In other cases, the reason for the refinement is indicated.
- Iterations have been indicated by adding a part to the requirement name (in brackets).

5.1 **Firewall**

5.1.1 FDP_RUL_EXT.1 Stateful Traffic Filtering

FDP_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FDP_RUL_EXT.1.2 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- ICMPv4 (Type, Code)
- ICMPv6 (Type, Code)
- IPv4 (Source Address, Destination Address, Transport Layer Protocol)
- IPv6 (Source Address, Destination Address, Transport Layer Protocol)
- TCP (Source Port, Destination Port)
- UDP (Source Port, Destination Port)

and

- distinct interface
- authentication status (if applicable)

and

- **VLAN ID**[3]

FDP_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules:

- Allow
- Deny

FDP_RUL_EXT.1.4 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

FDP_RUL_EXT.1.5 The TSF shall:
a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols:
TCP, UDP based on the following network packet attributes:

1. TCP: source and destination addresses, source and destination ports, sequence number, Flags;
2. UDP: source and destination addresses, source and destination ports;

b) Remove existing traffic flows from the set of established traffic flows based on the following:

- session inactivity timeout,

[3] This refinement was added to capture VLANs in the filtering requirement.

/

- completion of the expected information flow.

FDP_RUL_EXT.1.6 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:
a) The TSF shall drop packets which are invalid fragments;
b) The TSF shall drop fragmented packets which cannot be re-assembled completely;
c) The TSF shall drop packets where the source address of the network packet is:
- on a broadcast network
- on a multicast network ;
- a loopback address

d) The TSF shall drop network packets where the source or destination address of the packet is:
- unspecified[4]
- reserved for future use[5]

FDP_RUL_EXT.1.7 The TSF shall drop network packets where
a) the source address of the network packet is equal to the address of the network interface where the network packet was received;
b) the source or destination address of the network packet is a link-local address;
c) the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.

FDP_RUL_EXT.1.8 , The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

FDP_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FDP_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped.

5.2 **User Authentication**

5.2.1 FIA_UID(Network).2 User identification before any action

FIA_UID(Network).2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 FIA_UAU(Network).1 Timing of authentication

FIA_UAU(Network).1.1 The TSF shall allow [sessions that do not require user authentication] on behalf of a user to be performed before the user is authenticated.

FIA_UAU(Network).1.2 The TSF shall require each user to be successfully authenticated before **allowing sessions that require user authentication**.

5.3 **IPSec VPN**

5.3.1 FTP_ITC(IPSEC).1 Inter-TSF trusted channel

[4] Such as 0.0.0.0
[5] Such as 240.0.0.0/4 (as specified in RFC5735)

/

FTP_ITC(IPSEC).1.1 The TSF shall provide a**n IPSec** channel between itself and **IPSec clients and/or servers** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC(IPSEC).1.2 The TSF shall permit the TSF **and IPSec clients** to initiate communication via the **IPSec** channel.

FTP_ITC(IPSEC).1.3 The TSF shall initiate communication via the **IPSec** channel for outgoing sessions that require IPSec.

5.4 **Secure Management**

5.4.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: see the table below].

SFR	**Management action**
FDP_RUL_EXT.1	Create, modify and delete firewall rules
FIA_UAU(Network).1	Create, modify and delete accounts of non-admin users
FTP_ITC(IPSEC)	Determine which connections will be IPSec-encrypted
FIA_UAU(Management).2	Create, modify and delete accounts of administrators
FDP_UIT.1	Create, modify secrets for authenticated routing
FAU_GEN.1	Set/modify what events are logged
FPT_STM.1	Set/change the time

5.4.2 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behavior of **all functions** to **administrators**.

5.4.3 FTP_ITC(SSH).1 Inter-TSF trusted channel

FTP_ITC(SSH).1.1 The TSF shall provide a communication channel between itself and **an SSH client** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC(SSH).1.2 The TSF shall permit **the SSH client** to initiate communication via the trusted channel.
FTP_ITC.1.3(SSH) -[6]

5.4.4 FTP_ITC(HTTPS).1 Inter-TSF trusted channel

FTP_ITC(HTTPS).1.1 The TSF shall provide a communication channel between itself and **an HTTPS client** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[6] Refined away.

/

FTP_ITC(HTTPS).1.2 The TSF shall permit **the HTTPS client** to initiate communication via the trusted channel.
FTP_ITC.1.3(HTTPS) -.[7]

5.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles administrator, non-admin user.
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.5 Management Authentication

5.5.1 FIA_UID(Management).2 User identification before any action

FIA_UID(Management).2.1 The TSF shall require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **administrator**.

5.5.2 FIA_UAU(Management).2 User authentication before any action[8]

FIA_UAU(Management).2.1 The TSF shall require each **administrator** to be successfully authenticated **by: password or certificate**
residing

- **on the TSF, or**
- **on an external RADIUS server**

before allowing any other TSF-mediated actions on behalf of that **administrator**.

5.6 Authenticated Routing

5.6.1 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall[9] transmit and receive **routing** data in a manner protected from modification, insertion and replay errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of **routing** data, whether modification, insertion or replay has occurred.

5.7 Logging

5.7.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) -[10]
c) [see the table below].

---

[7] Refined away
[8] This requirement has been refined to show the method of authentication and the location of the authentication data.
[9] The reference to policies was deleted, as the entire policy is captured inside this requirement.
[10] Completed to "not specified" and then refined away.

/

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) -[11].

SFR	Associated events
FDP_RUL_EXT.1	Modification of the rules Dropping of a packet (and why it was dropped)
FIA_UAU(Network).1	(Un)successful authentication attempts of a web user
FTP_ITC(IPSEC)	(Un)successful establishment of an IPSec connection Termination of an IPSec connection
FTP_ITC(SSH).1	(Un)successful establishment of an SSH connection
FTP_ITC(HTTPS).1	(Un)successful establishment of an HTTPS connection
FIA_UAU(Management).2	(Un)successful authentication attempts of an administrator
FDP_UIT.1	Receipt of a routing packet with integrity issues
FAU_GEN.1	Modification of what events are logged
FPT_STM.1	Changing the time by an administrator
FRU_FLT.2	A change-over of the TOE in HA mode (in some models, and only in HA configuration)

5.7.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.7.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide administrators with the capability to read all information from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.7.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.7.5 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.8 **High Availability (some models, and only in HA mode)**

5.8.1 FRU_FLT.2 Limited fault tolerance

[11] Completed to "none" and then refined away.

/

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: one of the TOEs in a HA configuration becomes unresponsive.

/

6 Security Assurance Requirements

This Security Target claims conformance to EAL2, augmented with ALC_FLR.2. This assurance level was chosen to ensure that:

- the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.
- Any remaining security flaws in the TOE that are brought to the notice of Zyxel will be remediated

/

7 Extended Component Definition

7.1 FDP_RUL_EXT[12] Stateful Traffic Filter Firewall

Family Behavior

The component in this family is used to specify the behavior of a Stateful Traffic Filter Firewall. The network protocols that the TOE can filter, as well as the attributes that can be used by an administrator to construct a ruleset are identified in this component. How the ruleset is processed (i.e., ordering) is specified, as well as any expected default behavior on the part of the TOE.

Component leveling
There is only one component

Management: None

Audit: None

FDP_RUL_EXT.1 Stateful Traffic Filtering
Hierarchical to: No other components
Dependencies: None

FDP_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FDP_RUL_EXT.1.2 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields:

- ICMPv4 (Type, Code)
- ICMPv6 (Type, Code)
- IPv4 (Source Address, Destination Address, Transport Layer Protocol)
- IPv6 (Source Address, Destination Address, Transport Layer Protocol)
- TCP (Source Port, Destination Port)
- UDP (Source Port, Destination Port)

and

- distinct interface
- authentication status (if applicable)

FDP_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Stateful Traffic Filtering rules:

- Allow
- Deny

FDP_RUL_EXT.1.4 The TSF shall allow the Stateful Traffic Filtering rules to be assigned to each distinct network interface.

FDP_RUL_EXT.1.5 The TSF shall:
a) accept a network packet without further processing of Stateful Traffic Filtering rules if it matches an allowed established session for the following protocols:
TCP, UDP based on the following network packet attributes:

1. TCP: source and destination addresses, source and destination ports,

[12] This family definition is based on the FFW_RUL family in the Stateful Traffic Firewall cPP.

sequence number, Flags;

2. UDP: source and destination addresses, source and destination ports;

b) Remove existing traffic flows from the set of established traffic flows based on the following:

- session inactivity timeout,
- completion of the expected information flow.

FDP_RUL_EXT.1.6 The TSF shall enforce the following default Stateful Traffic Filtering rules on all network traffic:

a) The TSF shall drop packets which are invalid fragments;

b) The TSF shall drop fragmented packets which cannot be re-assembled completely;

c) The TSF shall drop packets where the source address of the network packet is:

- on a broadcast network
- on a multicast network ;
- a loopback address

d) The TSF shall drop network packets where the source or destination address of the packet is:

- unspecified[13]
- reserved for future use.[14]

FDP_RUL_EXT.1.7 The TSF shall drop network packets where

a) the source address of the network packet is equal to the address of the network interface where the network packet was received;

b) the source or destination address of the network packet is a link-local address;

c) the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.

FDP_RUL_EXT.1.8 , The TSF shall process the applicable Stateful Traffic Filtering rules in an administratively defined order.

FDP_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FDP_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped.

[13] Such as 0.0.0.0

[14] Such as 240.0.0.0/4 (as specified in RFC5735)

/

8 TOE Summary Specification

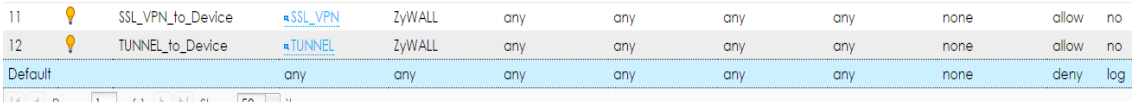
8.1 Firewall

FDP_RUL_EXT.1

The TOE allows administrators to define a set of filtering rules. The filtering rules are defined in a sequence: rules at the start are applied first, rules lower in the sequence are applied later.

Packets entering the TOE have these rules applied to them one by one, with the following results:

- The packet matches the rule, and the rule says “Allow”. No further rules are applied and the packet is passed through the TOE.
- The packet matches the rule, and the rule says “Deny”. No further rules are applied and the packet is not passed through (deleted).
- The packet does not match the rule, in which case the packet is moved to the next rule.
- By default, the last line matches all packets with a “Deny”. This line cannot be deleted, but an administrator could modify it if he wanted.



11	SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no
12	TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no
Default		any	any	any	any	any	any	none	deny	log

Rules can be based on various network protocol fields

- ICMPv4 (Type, Code)
- ICMPv6 (Type, Code)
- IPv4 (Source Address, Destination Address, Transport Layer Protocol)
- IPv6 (Source Address, Destination Address, Transport Layer Protocol)
- TCP (Source Port, Destination Port)
- UDP (Source Port, Destination Port)

Rules can also be based on the interface a packet comes in (or is supposed to go out).
There can also be rules that the user must first be authenticated (see section 8.2).

The TOE also supports VLANs (IEEE 802.1Q) and these may cause further filtering.

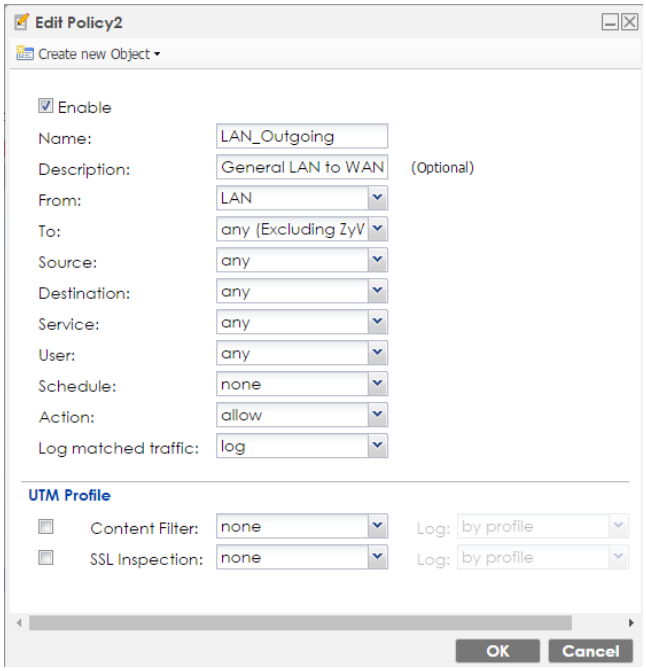
For efficiency reasons, the TOE also supports sessions: traffic flows that have already been processed by the rules, and each packet in that session does not have to through all rules again, but uses the same result as all earlier packets in that session.

The TOE will also drop packets that may have security problems such as packets:

- which are invalid fragments
- that cannot be reassembled completely that have source addresses that are a loopback address, unspecified, reserved for future use, a link-local address on a broadcast or multicast network, equal to the address of the network interface where the packet was received, does not belong to the networks associated with the network interface where the network packet was received
- that have destination addresses that are unspecified, reserved for future use or a link-local address;

/

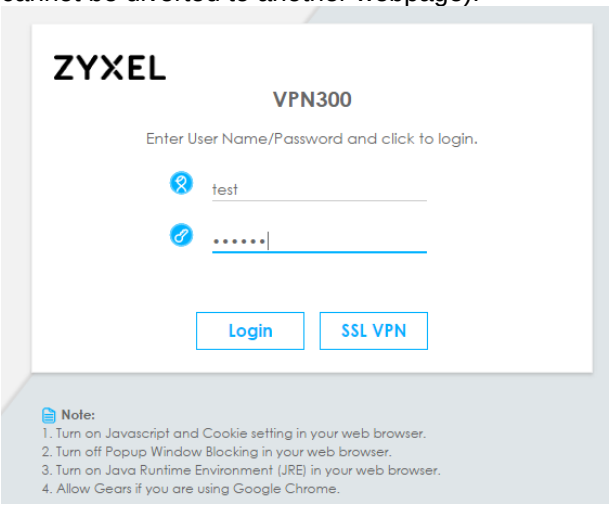
Finally, the TOE will also restrict the number of half-open TCP connections and drop all new TCP connections once this limit has been reached, as this may indicate a DoS attack.



8.2 User Authentication

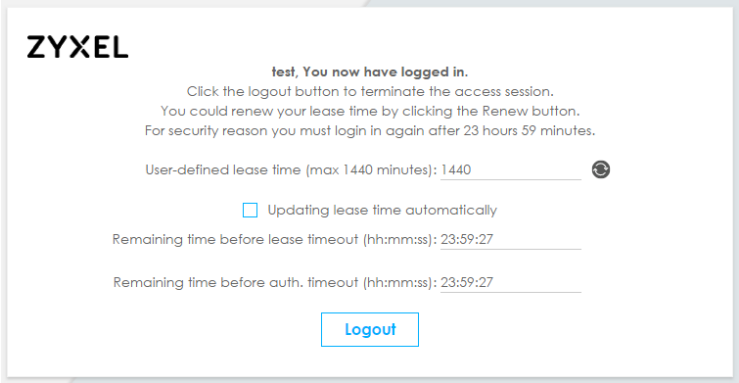
FIA_UID(Network).2, FIA_UAU(Network).2, FMT_SMR.1

If the TOE is configured to require web authentication, and it received a web request from a certain IP-address and this IP-address has not been authenticated, the web request is diverted to a login page.
If the TOE receives any other request from an unauthenticated IP-address, it is dropped (it cannot be diverted to another webpage).



The user then has to input a valid username/password combination and this authenticates his IP-address.

/



Subsequent web requests and other requests are then passed on normally (subject to other rules).

8.3 IPSec VPN

FTP_ITC(IPSEC).1
The TOE supports IPSecv3 (RFC4301-4303) in both transport mode and tunnel mode, in combination with IKEv2 (RFC5996)

The TOE can act as an IPSec server (allowing external entities to set up IPSec connections with the TOE) and as an IPSec client (where the TOE sets up IPSec connections with external entities).

For IPSec-ESP the TOE supports[15] AES-CBC-128 and AES-CBC-256 (both specified by RFC 3602), while for IKEv2 the TOE supports DH5, DH14, AES-CBC-128 and AES-CBC-256.

The TOE can be configured to limit SA lifetimes by setting a maximum amount of time it can be active.

8.4 Secure Management

FMT_SMF.1, FMT_MOF.1
The TOE has a wide range of management options: this ST includes only a few of the options that are relevant to the other security requirements. An administrator must authenticate himself to get access to these management interfaces (either web or CLI).

From there he can (among others):

- Create, modify and delete firewall rules
- Create, modify and delete accounts of users and other administrators
- Determine which connections will be IPSec-encrypted
- Create, modify secrets for authenticated routing
- Set/modify what events are logged

[15] The TOE can be configured to support more cypher-suites for both ESP and IKE, but these are outside the evaluated configuration

- Set/change the time

FTP_ITC(SSH).1
In order for managers to access the CLI of the TOE, the TOE supports SSH v2 (RFC 4250-4254). Administrators wishing to access the TOE should use the following settings:

- SSH v2
- DiffieHellman-Group-14-SHA-1
- SSH-RSA
- AES-128-CBC or AES-256-CBC
- HMAC-SHA1 or HMAC-SHA1-96

SSH automatically rekeys every 2^31 packets.

FTP_ITC(HTTPS).1
In order for managers to access the web interface of the TOE, the TOE supports HTTPS (RFC2818) in conjunction with TLS v1.2 (RFC5246). The TOE rejects TLS v1.1 and 1.0.

For TLS, the TOE validates certificates according to RFC 5280. The certificate path must terminate with a trusted CA certificate.to validate the certificate. If the validity of the certificate cannot be established, the connection fails.

The TOE supports the following[16] TLS v1.2 cypher-suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

8.5 Management Authentication

FIA_UID(Management).2, FIA_UAU(Management).2, FMT_SMR.1
The TOE enforces authentication of administrators before they can perform any management action. This authentication can be done by username/password.

The authentication data needed to authenticate administrators can be stored:

- On the TOE itself
- On an external RADIUS server: the TOE communicates with this server according to RFC 2865-2866 across a secure connection (see OE.PHYSICAL)

8.6 Authenticated Routing

FDP_UIT.1
The TOE also acts as a router, and therefore requires routing information from other routers to ensure that it routs traffic to the correct network interface. As attackers could conceivably

[16] The TOE can be configured to support more cypher-suites, but these are outside the evaluated configuration

interfere with this routing information, this could cause the TOE to rout information towards the wrong network interface, thereby possibly allowing undesired traffic flows.

To prevent this, the TOE supports authenticated routing, whereby it shares a secret key with adjacent routers, and uses MD5-hashes based on this key to protect the authenticity and integrity of each routing packet.

This is described in more detail in:

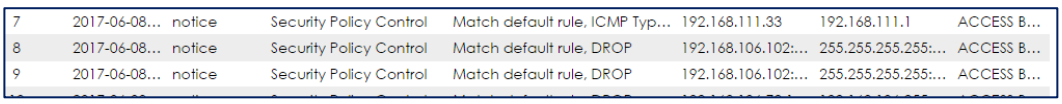
- RFC2082 for RIPv2
- RFC2328 for OSPFv2
- RFC2385 for BGPv4

8.7 **Logging**

FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FPT_STM.1

The TOE can log a large amount of different events. This Security Target only includes only the following subset, that is relevant to the other security requirements:

- Starting and stopping of the logging (so one can determine that when an event is not logged, that this was due to the TOE being off, rather than the event not occurring)
- Modification of the firewall rules, or the rules for logging of events
- Dropping of packets
- (Un)successful authentication attempts of both administrators and web users
- (Un)successful establishment of an IPSec, SSH or HTTPS connection
- Termination of an IPSec connection
- Receipt of a routing packet with integrity issues (the md5 hash does not correspond to the packet)
- Changing of the time by an administrator
- A change-over of the TOE in HA mode (in some models, and only in HA configuration)



7	2017-06-08...	notice	Security Policy Control	Match default rule, ICMP Typ...	192.168.111.33	192.168.111.1	ACCESS B...
8	2017-06-08...	notice	Security Policy Control	Match default rule, DROP	192.168.106.102:...	255.255.255.255:...	ACCESS B...
9	2017-06-08...	notice	Security Policy Control	Match default rule, DROP	192.168.106.102:...	255.255.255.255:...	ACCESS B...

Where possible, the TOE also logs the identity of the administrator or the web user that caused the event (or other identifiers like the IP-address).

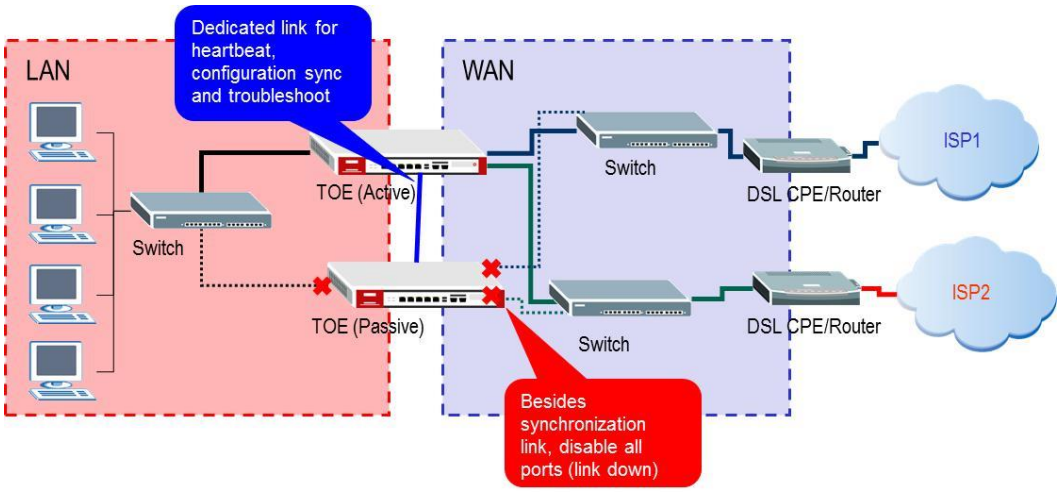
Access to the audit records is only possible through the CLI or web interface, which is only accessible by authenticated administrators. Authenticated administrators have access to all the audit information.

Finally, the TOE maintains an internal clock so that it can log the correct time that events occurred. It is possible to synchronise this clock through NTP, but this is outside the scope of the evaluation.

/

8.8 **High Availability (some models, and only in HA mode)**

Two copies of the TOE can be configured in parallel to provide protection against failure of one copy.



One TOE is active, the other TOE is passive: all of its ports are closed except a dedicated port for heartbeat, synchronisation of configuration (if an admin manages the active TOE, all changes are also made to the passive TOE) and troubleshooting. If the heartbeat port of the passive TOE no longer receives a signal, the passive TOE switches to active, so that the services are still continued. (FRU_FLT.2)

/

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of two parts:

- A rationale that the security objectives uphold all assumptions
- A rationale that the security objectives counter all threats

Assumption	Rationale
A.PHYSICAL	This assumption is upheld by OE.PHYSICAL, which restates the assumption.
A.SINGLE_CONNECTION	This assumption is upheld by OE.SINGLE_CONNECTION, which restates the assumption.
A.TRUSTED_ADMIN	This assumption is upheld by OE.TRUSTED_ADMIN, which restates the assumption.

Threat	Rationale
T.UNAUTHORIZED_DATA	This threat is countered by O.DATA_FLOW_CONTROL, which directly restates the threat.
T.READ_MODIFY_DATA	This threat is countered by O.ENCRYPT stating that the TOE can use IPSec-based encryption to protect the traffic flows
T.UNAUTHORIZED_ACCESS	This threat is countered by • O.PROTECTED_MANAGEMENT specifying that only authenticated managers can remotely access the TOE, and only through protected channels • OE.PHYSICAL specifying that the TOE itself is physically protected, as is local management • OE.TRUSTED_ADMIN specifying that all administrators are trusted
T.UNDETECTED_ACTIONS	This threat is countered by: • O.LOGGING specifying that actions are logged and managers can review them • OE.TRUSTED_ADMIN specifying that all administrators will follow the guidance on checking the log
T.TSF_FAILURE (some models, and only in HA configuration)	This threat is directly countered by O.HIGH_AVAILABILITY, which directly restates the threat

/

9.2 **Security Requirements Rationale**

This rationale shows that all security objectives for the TOE are upheld by the security functional requirements.

Objective	**Rationale**
O.DATA_FLOW_CONTROL	This objective is met by: • FDP_RUL_EXT.1: which specifies a stateful firewall that is able to mediate traffic based on rules defined by administrators (FMT_SMF.1 • FIA_UID(Network).2 and FIA_UAU(Network).1: which specify that for users additional authentication may be required • FDP_UIT.1 specifying secure routing, which would prevent the TOE from receiving wrongful routing information, which may then allow unauthorized traffic flows.
O.ENCRYPT	This objective is met by FTP_ITC(IPSEC).1 specifying that the TOE can setup IPSec channels with other IPSec clients and servers.
O.PROTECTED_MANAGEMENT	This objective is met by: • FMT_SMF.1: which specifies the security management functions relevant to this ST • FMT_MOF.1: restricting this management to administrators • FIA_UID(Management).2 and FIA_UAU(Management).2 specifying that managers must be identified and authenticated before allowing access • FTP_ITC(SSH).1: allowing remote administrators to use SSH for management • FTP_ITC(HTTPS).1: allowing remote administrators to use HTTPS for management NB: Local administration is handled by OE.PHYSICAL
O.LOGGING	This objective is met by: • FAU_GEN.1 specifying which events to log • FAU_GEN.1 and FAU_GEN.2 specifying what to log about each event • FAU_SAR.1 allowing administrators to read the log • FAU_SAR.2 allowing nobody else to do so. • FPT_STM.1 providing reliable time stamps, so that it is known when events happened.
O.HIGH_AVAILABILITY	This objective is met by FRU_FLT.2 specifying that in case of failure of one of the two TOEs in a HA configuration, the other TOE shall ensure that all of its capabilities continue.

/

9.3 **Dependency Rationale**

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	**Dependency**	**Rationale**
FDP_RUL_EXT.1	None	-
FIA_UID(Network).2	None	-
FIA_UAU(Network).1	FIA_UID.1	Met by FIA_UID(Network).2
FTP_ITC(IPSec).1	None	-
FMT_SMF.1	None	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Met Met
FTP_ITC(SSH)	None	-
FTP_ITC(HTTPS)	None	-
FMT_SMR.1	FIA_UID.1	Met by FIA_UID(Management).2
FIA_UID(Management).2	None	-
FIA_UAU(Management).2	FIA_UID.1	Met by FIA_UID(Management).2
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	Not met, since the policy reference was refined away Not met, as a full trusted path or channel is not necessary: integrity and authenticity are important, but confidentiality is not
FAU_GEN.1	FPT_STM.1	Met
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Met Met by FIA_UID(Management).2
FAU_SAR.1	FAU_GEN.1	Met
FAU_SAR.2	FAU_SAR.1	Met
FPT_STM.1	None	-
FRU_FLT.2	FPT_FLS.1	Not met, the requirement is unnecessary since FRU_FLT describes already what the secure state is.
EAL2	All dependencies of an EAL are addressed within that EAL	
ALC_FLR.2	None	-