Zywall VPN Client

Customization Qualification Tests Specifications

Zywall IPSec VPN Client 3.6.204.61.04

WebSite :	http://www.thegreenbow.com
Contact :	support@thegreenbow.com

TABLE OF CONTENT

1 How to use the Qualification Test Specification 3
1.1 Header / Footer 3
1.2 Qualification tests 3
1.3 Qualification environment 4
2 Qualification Tests 4
2.1 Installation / Uninstallation 4
2.1.1 Platform 4
2.1.2 Relevant documentation 4
2.1.3 Acronyms used in this chapter 5
2.1.4 Scripts used to check file versions 5
2.2 Installation 5
2.2.1 Platform 5
2.3 Activation / Reset 7
2.4 Upgrade 8
2.5 Uninstallation 8
2.6 VPN Configuration Server 10
2.6.1 VPN Configuration Server Interface 10
2.6.2 Zyxel Specific Tests 13
3 Annex 18
3.1 Customization values 18
4 Version number control 19
5 General Tests for Customisations 19

1 How to use the Qualification Test Specification

1.1 Header / Footer

Header and footer must be filled in for each page

Version field shows the version tested.
OS field shows the operating system used for tests.
Date field shows the beginning date of the testing session
Tester fields is filled with the tester initials.

1.2 Qualification tests

All tests need to be performed sequentially in an exhaustive manner, as each test describes a specific functionality of the VPN Client.

Each test is defined with the following informations:

- An operating mode
- An expected result
- An actual result filled in by the tester: **OK**, **TGB OK** (Tested with TGB VPN), **NOK**, **NA** (Not Applicable)

If the actual result of a test is **NOK**, the issue must be accurately described and may be added in a separate document from this one.

1.3 Qualification environment

1 test computer with Windows (the windows version must be indicated in the header of this document), **without any previous installation of the software**.

The registry key **HKEY_LOCAL_MACHINE \ Software \ ZyXEL \ ZyWALL IPSec VPN Client** should not exist (if it exists, it must be removed)

1 VPN Client setup. This setup will be run not from the test computer (it should be run from a server, another computer, a CD, etc...)

Environment diagram:

2 Qualification Tests

2.1 Installation / Uninstallation

2.1.1 Platform

PC with no VPN Client installed.

2.1.2 Relevant documentation

1	RN VPN 5.1	On the partner area.

2.1.3 Acronyms used in this chapter

[VPNSETUP.EXE]	ZyWALL_IPSec_VPN_Client.exe
[Company]	ZyXEL
[Product]	ZyWALL IPSec VPN Client

[INSTALLDIR]	64bit	C:\Program Files (x86)\[Company]\[Product]
	32bit	C:\Program Files\[Company]\[Product]
[SYSTEM32]	64bit	C:\Windows\SysWOW64
	32bit	C:\Windows\System32
[PROGRAMDATA]	C:\ProgramData\[Company]\[Product]	
[TGBCODE_XY.DAT]	The file "tgbcode_201_*uuu*.dat" where "*uuu*" is the Windows User Name	
[TGBPARAM_XY.DAT]	The file "tgbparam_201_*uuu*.dat" where "*uuu*" is the Windows User Name	
[PRODACT.DAT]	"C:\Users*uuu*\Documents\prodact.dat" where "*uuu*" is the Windows User Name	
[HKLMTGBIKEKEY]	Registry key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\TgbIke.exe	
[HKLMTGBKEY]	64bit	HKLM\ SOFTWARE \Wow6432Node\[Company]\[Product]
	32bit	HKLM\SOFTWARE\[Company]\[Product]
[OSAURLKEY]	Registry key: [HKLMTGBKEY]\OSAUrl (REG_SZ)	
[OSAPORTKEY]	Registry key: [HKLMTGBKEY]\OSAPort (REG_SZ)	
[OSACERTKEY]	Registry key: [HKLMTGBKEY]\cert (REG_SZ)	
[NOACTIVWINKEY]	Registry key: [HKLMTGBKEY]\NoActivWin (REG_BINARY)	
[AUTOACTIVKEY]	Registry key: [HKLMTGBKEY]\AutoActiv (REG_BINARY)	
[LANGUAGEKEY1]	Registry key: [HKLMTGBKEY]\Language (REG_SZ)	
[LANGUAGEKEY2]	Registry key: HKCU\Software\[Company]\[Product]\Language (REG_SZ)	
[HKLMTGBSERVMP]	Registry folder: HKLM\System\CurrentControlSet\services\TGBVPNVirtM	
[HKLMTGBSERVENUM]	Registry folder: HKLM\System\CurrentControlSet\services\TGBMPEnum	
[HKLMTGBSERVXP]	Registry folder: HKLM\System\CurrentControlSet\services\TGBVPN	
[HKLMTGBSTARTER]	Registry folder: HKLM\System\CurrentControlSet\services\TgbIke Sarter	
[HKLMRUN]	Registry folder: HKLM\Software\Microsoft\Windows\CurrentVersion\Run	
[HKLMTGBRUN]	Registry key: [HKLMRUN]\TgbVpn (REG_SZ)	
[IKESTARTKEY]	Registry key: [HKMLTGBIKEKEY]\IkeStart (REG_SZ)	

2.1.4 Scripts used to check file versions

1	File Version Check Script	\\Gillespie\Produits\VPN\Qualif\TgbValidation\Tools\TGBfileCheckAllOSCustoV51.vbs To be compared with the file versions from Versionning.xlsx

2.2 Installation

2.2.1 Platform

PC/VM **with no previous installation**, these tests must be passed on each platform Seven 32/64

N°	BT	Action	Expected results	Status
		Run [VPNSETUP.EXE]	The language selection is displayed	OK
			The icon on the left of this dialog is the customized icon.	OK
			The languages available are consistent with the customization specification.	OK
			The language selected by default is the language of the OS	OK
		Select the default language and click Ok	The welcome step is displayed	OK
			The Right column of the dialog is customized	OK
			The bitmap (Left side of the dialog) is customized	OK
			The name of the software is customized	OK
		Click on Next	In the software license agreement, the name of the company and the name of the product are customized.	OK
		Click on I Agree	The default install dir is [INSTALLDIR]	OK
		Click on Next (choose the default install dir)	The shortcut name is customized	OK
		Click on Install	Step progress bar is displayed	OK
			Popup Windows for the installation of the "miniport" driver is displayed. It identifies the signature is Ok	OK
		Click on Ok	Popup Windows for the installation of the "Enum" driver is displayed. It identifies the signature is Ok	OK
		Click on Ok	Progress bar ends	OK
			Step "Finish" is displayed	OK
		Click on "Finish"	The installation closes	OK
		Start the VPN Client, check-in the “Evaluate” radio button and click on “Next” button		
		Execute the script [File Version Check]	All the listed files are correct, and none is missing	OK
			All the versions are correct vs [TRN VPN 5.1]	OK
		Open the registry (1), goto [HKLMRUN]	[HKLMTGBRUN] exists and is set to: "[INSTALLDIR]\vpnconf.exe"	OK
		Open [HKLMTGBKEY]	"GuiDefs" exists and is not empty	OK
			[LANGUAGEKEY1] is set to 3 characters (2)	OK
			[MENUITEMKEY] is set to 1F	OK
			[OSAURLKEY] is set to "tgbosa.com/activation.php"	NA
		Open [HKLMTGBIKEKEY]	[IKESTARTKEY] is set to 0	OK

			"Path" is set to [INSTALLDIR]	OK
			"NoCaCertReq" is set to 1	OK
		Open the folder [PROGRAMDATA]	[TGBPARAM_XY.DAT] is present	OK
		Reboot the computer and open the Windows session.	The customized VPN Client starts automatically or not, depending of the customization specification. *(Check StartMode in Annex table)*	OK
		Visualize the Windows desktop	The evaluation/activation dialog is displayed.	OK
			The evaluation period is 30 days (*)	OK
			The software icon and the name of the icon are customized	OK
		Click on "buy" (or equivalent depending on the language)	The buy website opens *(Check url buy in Annex table)*	NA
		Click on "evaluate" (or equivalent depending on the language)	The software is running (no problem with TgbIke)	OK
			The header banner of the software is customized	OK
			The name of the software is customized	OK
			The systray icon is customized	OK
		Open the control panel and select the menu "add/remove program"	The customized VPN Client appears in the installed software list.	OK
		Open the directory "Program Files"	The customized directory [INSTALLDIR] owns the VPN Client software	OK
		click on the "?" menu" then select "support"	The customized "support" url opens *(Check url support in Annex table)*	NA
		Select "help"	The customized "help" url opens *(Check url help in Annex table)*	NA
		Select "check for update"	The customized "update" url opens. *(Check url update in Annex table)*	NA
		Create a VPN Configuration used for further test, and click on "save & apply"	"VPN ready" is displayed on GUI	OK
		In VPN Configuration panel	IKE V1 and IKE V2 branches are presents. SSL branch is not available *(Check Protocol in Annex table)*	

2.3 Activation / Reset

PC with VPN Client installed, not activated, not running
PC is connected to the network (Internet)
Test licenses: available at: \\GILLESPIE\Produits\Licences TGBTEST\TGBTEST Licences.xls

N°	BT	Action	Expected results	Status
		Run the VPN Client	1st page of the Activation Wizard is displayed	OK
		Enter License number and email and Click on "Next"	Step 2 of the Activation Wizard displays "Activation successful"	OK
		Quit the VPN Client. Restart the VPN Client	The software is activated	OK
		Reboot the PC. Run the VPN Client	The software is activated	OK
		Uninstall the VPN Client	Verify if activation reset has been processed in activation server	OK
		Install the VPN Client and proceed a manual activation	The software is activated	OK

2.4 Upgrade

PC with previous version of VPN Client installed, activated and with a VPN configuration
PC is connected to the network (Internet)
Test licenses: available at: \\GILLESPIE\Produits\Licences TGBTEST\TGBTEST Licences.xls

N°	BT	Action	Expected results	Status
		Install previous version of VPN Client > Activate the license > Import a configuration		
		Proceed an upgrade to the current version	Upgrade passes correctly	OK
		Run the VPN Client	Previous VPN configuration imported successfully	OK
			License number and Email imported successfully	OK

2.5 Uninstallation

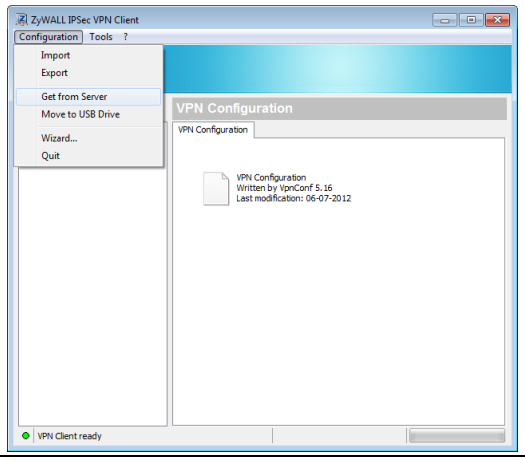
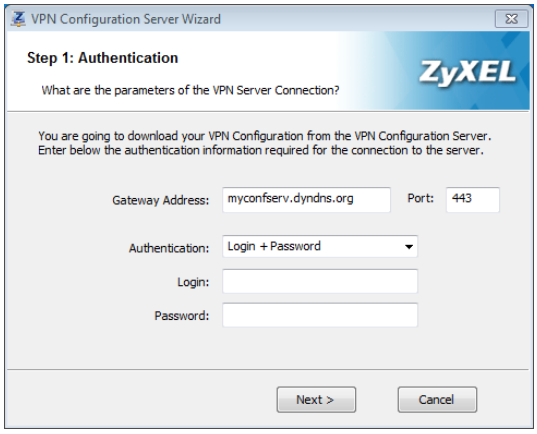
N°	BT	Action	Expected results	Status
		Open Windows Start Menu > Control Panel > Program > Programs & Features		
		Select the customized VPN Client and click on "uninstall"	Welcome popup is displayed	OK
		Click on "Yes" (ack the uninstall)	The uninstall ends successfully	OK
		Open Windows desktop	The application icon is removed	OK
		Open Windows start menu	[Product] folder is removed	OK
			[HKLMTGBIKEKEY] is removed	OK
			[HKLMTGBKEY] is removed	OK

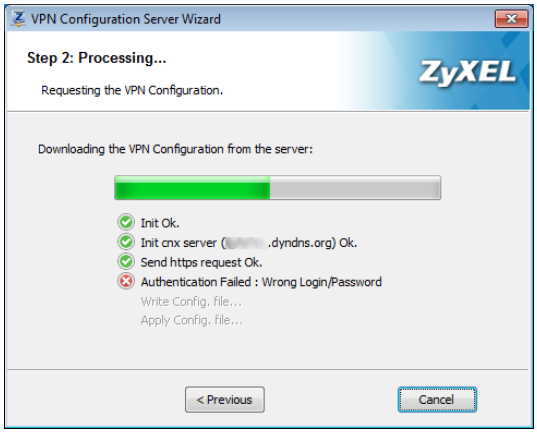
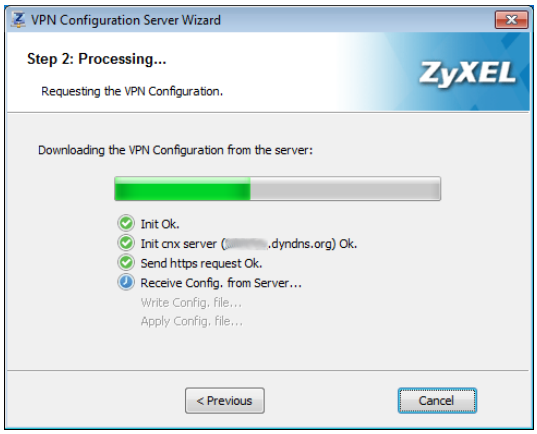
			[INSTALLDIR] is removed	**OK**
			[PROGRAMFILES]\[Company] folder is removed	**OK**
		Open [SYSTEM32]	Tgb_configmode.dll is removed	**OK**
			Vpncfg.dll is removed	**OK**
			Tgbstarter.exe is removed	**OK**
		Open [SYSTEM32]	TgbCredProv.dll is removed	**OK**
		Open [PROGRAMDATA]	[TGBPARAM_XY.DAT] is still there	**OK**
			[TGBCODE_XY.DAT] is removed	**OK**

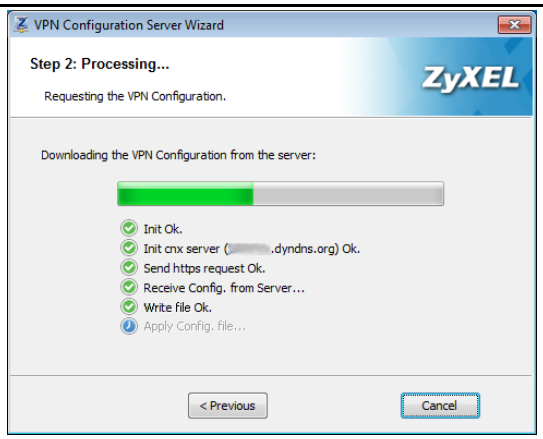
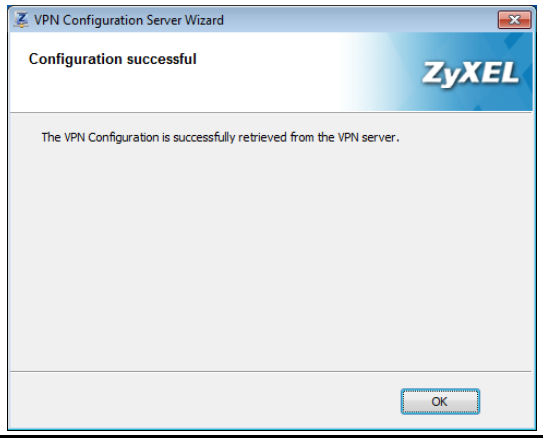
2.6 VPN Configuration Server

Router : Zywall USG1000 – Configure to provide VPN Configuration using Provisional feature.
(ZyWall > Configuration > VPN > IPSec VPN > Configuration Provisioning)
VPN Configuration with 0.0.0.0 is assigned to the User.
Two VPN profiles should have been setup on VPN Gateway for test purpose:
-one with Pre-Shared Key (PSK) for IKE
-one with Certificate for IKE
The certificate used for IKE authentication when connecting to gateway has to be available in Windows Personal Certificate Store of the workstation where the VPN Client is installed.

2.6.1 VPN Configuration Server Interface

N°	BT	Action	Expected results	Status
		Run the VPN Configuration Server by going through VPN Client menu **Configuration** > **Get from Server**.  	VPN Configuration Server Wizard "**Step 1: Authentication**" is displayed  	**OK**
		Fill in a wrong address and/or port for Gateway Address. Click on **Next** button.	Wizard "**Step 2: Processing**" is displayed with an error in 3rd listed item:"" "**Server not found ! (check the server address/port)**"	**OK**

		Click on Previous button, fill in the right Gateway Address/Port. Type a wrong Login and/or Password. Click on **Next** button	Wizard "**Step 2: Processing**" is displayed with an error in 4th listed item: "**Authentication Failed : Wrong Login/Password**" 	**OK**
		Click on **Previous** button. Type in the right Login and/or Password. Click on **Next** button.	Wizard "**Step 2: Processing**" is displayed and all items are validated. 	**OK**

				
			In case of a certificate defined in gateway VPN IKE configuration, VPN Configuration Server Wizard display "**Step 3: Certificate Choice**". Select the right certificate in displayed list. Click on **Next** button. 	
			VPN Configuration Wizard ends successfully. 	OK

2.6.2 Zyxel Specific Tests

N°	BT	Action	Expected results	Status
	3371	31 characters in any phase name	Tgblke does not crash when opening tunnel using such long phase name.	**OK**
	3342 3230	Gateway Phase-1 and Phase-2 names with dash sign "-"	VPN Configuration Wizard imports Phase-1 and Phase-2, replacing dash sign "-" by underscore sign "_"	**OK**
	3268 3076	When VPN Client Trace Mode is ON (Ctrl+Alt+D), Configuration Server will write its log in "C:\ProgramData\[Company]\[Product]\LogFiles" in file named "YYYY-MM-DD-VpnCfgSrv.log"	Check log is created when VPN Client trace mode is ON.	
	3232	ZyXEL gateway send configuration with Local-ID filled.	Local-ID information is not used when VPN Client virtual IP is 0.0.0.0	
	3073	Retrieving a VPN configuration from gateway while at least one VPN configuration already exist in VPN Client Tree list	VPN Client must prompt customer with Information window asking "**Do you want to add this configuration or to replace the current configuration?**", buttons **Add**, **Replace** and **Cancel** being the different choices available.	**OK**
	2773	Gateway Configuration with Certificate	VPN Configuration Wizard asks for a certificate to be chosen from the Windows Personal Certificate Store	**OK**
	2764	VPN Configuration Server should provide different error message when not being able to retrieve VPN configuration from gateway.	401 -> Authentication Failed: Wrong Login/Password 403 -> Server does not enable the service of VPN configuration provisioning. 404 -> Server Not Found! (check the server address/port) 500 -> Server has internal error! Downloading process failed!	**OK**
		Install the VPN Client in Russian Language > Execute VPN Client and the Wizard Get from server	Wizard language is in Russian	**OK**
		Re-install the customized VPN Client		
		Open the "startup" menu	The website link doesn't appear in the menu "startup > ZyXEL"	
		Run the software	The "buy" button of the evaluation/activation dialog doesn't appear.	**OK**
			The string mentioning the ability to buy ("Buy a software license (...)") doesn't appear	**OK**
		Click on "evaluate" then open the "?" menu of the main GUI.	The items "Online support", "Help" and "Check for update" doesn't appear	**OK**
		Open the "About" dialog	The specific ZyXEL software version is displayed (e.g. "1.0.204.61")	**OK**

		Open the parameters page	The miscellaneous retransmissions value is set to 2.	OK
		Open Configuration panel	SSL Branch doesn't exist in VPN Client	OK
		Create an IKEv1 tunnel	Configuration created	OK
		Open the IKEv1 tunnel	Tunnel opened and traffic passes through the tunnel	OK
		Create an IKEv2 tunnel	Configuration created	OK
		Open the IKEv2 tunnel	Tunnel opened and traffic passes through the tunnel	OK
		Import an IKEv2 tunnel	Configuration created	OK
		Open the IKEv2 tunnel	Tunnel opened and traffic passes through the tunnel	OK
		Close the IKEv2 tunnel	Tunnel closed	OK
	4931	Create an IKEV2 configuration with PSK and Check the option "Request configuration from Gateway"	An alert displayed that it is not allowed and no changes to the configuration	OK
	4931	Create an IKEV2 configuration with Certificate and Check the option "Request configuration from Gateway"	An alert displayed that it is not allowed and no changes to the configuration	OK
	4931	Create an IKEV2 configuration > new VPN Gateway	PSK is selected by default	OK
		Create New VPN Connection under above config	"Request config from gateway" is unchecked.	OK
		Select EAP and Check the option "Request configuration from Gateway"	No alert / Popup	OK
	4931	Go to Phase1 and change EAP to PSK	An alert displayed that it is not allowed and no changes to the configuration	OK
	4931		EAP is always selected	OK
	4931	Go to Phase1 and change EAP to Certificate	An alert displayed that it is not allowed and no changes to the configuration	OK
			EAP is always selected	OK
	4824	Open an IKEV1 IPv4 tunnel in non NATed environment and PFS = None	Tunnel opens and traffic passes to remote network	OK(1)
	4826	In IKV2 IPv6 configuration	Child SA shows 'Prefix Length' instead of 'Subnet Mask'.	OK
	4841	Create an IKEV2 tunnel	Phase1 name is Ikev2Gateway Phase2 name is Ikev2Tunnel	OK
	4837	In an IKEv2 certificate configuration > Click on View Certificate	Certificate information window appears	OK
	4836	Save an IKEv2 configuration with Presharedkey	PSK Configuration saved properly	OK

		by leaving the mouse curser in Confirm field		
	4834	Open an IKEv1 tunnel with Phase1 algorithms as 'Auto'	Tunnel opens and traffic passes to remote network	**OK**
	4833	Open an IKEv2 IPv4 tunnel with empty local & remote ID	Tunnel opens and traffic passes to remote network	**OK**
	4833	Open an IKEv2 IPv6 tunnel with empty local & remote ID	Tunnel opens and traffic passes to remote network	**OK**
	4829	Right click on 'VPN Configuration' root menu	New Phase1 button is not shown	**OK**
	4828	Open an IKEV2 IPv4 tunnel with PFS = None	Tunnel opens and traffic passes to remote network	**OK**
	4827	Switch between PSK and EAP in an IKEv2 configuration	Configuration switches properly	**OK**
	4825	Open an IKEv1 tunnel with Xauth Popup	Popup appears and tunnel opens	**OK**
	4823	Open VPN Configuration panel	SSL branch is not shown	**OK**
		Import a SSL configuration	Configuration is not imported	**OK**
	5010	Open an IKEv2 tunnel with range address	Tunnel opens	**OK**
			Configured range address is used for the tunnel	**OK**
	5012	Open an IKEv2 tunnel with empty Remote ID but configure Remote ID in Gateway	Tunnel opens	**OK**
	4965	Import an IKEv2 configuration which configured with IKEv2 and Certificate	Configuration imported	**OK**
	4839	Open an IKEv2 tunnel with Host address in P2	Tunnel opens	**OK**
		Open an IKEv2 tunnel with Subnet in P2	Tunnel opens	**OK**
		Open an IKEv2 tunnel with Range address in P2	Tunnel opens	**OK**
		Open an IKEv2 tunnel with Config Payload and Host address in P2	Tunnel opens	**CP works only with EAP and EAP works only with Certificate**
		Open an IKEv2 tunnel with Config Payload and Subnet in P2	Tunnel opens	**CP works only with EAP and EAP works only with Certificate**
		Open an IKEv2 tunnel with Config Payload and Range address in P2	Tunnel opens	**CP works only with**

				EAP and EAP works only with Certificate
	4838	Open VPN Client configuration panel, Phase1 of IKEv2 configuration	IPV4/Auto/IPV6 buttons are not available	**OK**
	4822	Create VPN Configuration > Change the Gateway name or address > Enter the Presharedkey > Enter wrong Confirm PSK > Press Ctrl+S to save	Wrong Presharedkey warning appears	**OK**
	5014	Open an IKEv2 tunnel without CA certificate	Tunnel opens	**OK**
	5024	Open an IKEv1 auto tunnel with P1: DES/MD5/DH1 and P2:DES/MD5	Tunnel opens	**OK**
		Open an IKEv1 auto tunnel with P1: AES128/SHA1/DH5 and P2:AES256/SHA256	Tunnel opens	**OK**
	5025	Open an IKEv1 tunnel using Certificate and Email as remote ID	Tunnel opens	**NOK**
004				
	5113 5118	Open an IKEv2 tunnel using Certificate with gateway. In Gateway, Local ID type = Email. In VPN Client, Remote ID is not configured	Tunnel opens	**OK**
	5113 5118	Open an IKEv2 tunnel using Certificate with gateway. In Gateway, Local ID type = DNS. In VPN Client, Remote ID is not configured	Tunnel opens	**OK**
	5113	Open an IKEv2 tunnel using Certificate with gateway. In Gateway, Local ID type = IP. In VPN Client, Remote ID is not configured	Tunnel opens	**OK**
	5117	Create an IKEv2 tunnel > Import a Certificate > Open Advance tab	Remote ID is empty	**OK**
005				
	5120 5139	Import a Self signed certificate to Windows Certificate store > Open an IKEv2 tunnel using Windows certificate	Tunnel opens	**OK**
006				
	5168	Open VPN Client > Create or Edit IKEv2 configuration > Select EAP	Multiple Auth Support check box is not available	**OK**
007				
	5211	Open IKEv1 tunnel with Xauth popup	Xauth login window text shows 'Enter Authentication login and password to open the tunnel'	**OK**

		Open IKEv2 tunnel with EAP popup	EAP login window text shows 'Enter Authentication login and password to open the tunnel'	**OK**
	5191	Import Windows Certificate to Certificate store (Root and User) > Create an IKEv2 configuration with the certificate from Store > Save the configuration	Configuration saved sucessfully and no error appear in VPN Console	**OK**
3.5.204.61.05				
	5275	Open a tunnel with USG40 using Zyxel1 Certificate and using attached BT configuration file	Tunnel opens	**OK**
3.5.204.61.11				
	5427	Open an IKEv1 tunnel > Wait for key renewal > Open Console log	Initial contact is not sent	**OK**
3.6.204.61.01				
	5332	Install VPN Client in Windows 10 32Bits > Activate the software License > Uninstall the VPN Client	Software installed , activated and Uninstalled properly	**OK**
		Install VPN Client in Windows 10 64Bits > Activate the software License > Uninstall the VPN Client	Software installed , activated and Uninstalled properly	**OK**
3.6.204.61.04				
		Open IKEv2 configuration	Presharedkey's 'Confirm' word shown in interface	**OK**

3 Annex

3.1 Customization values

Item	Value	Status
OEM	**ZyXEL**	
Vendor Code	**24**	
Setup Name	ZyWALL IPSec VPN Client.exe	
Registry Path	HKEY_LOCAL_MACHINE\SOFTWARE\ ZyXEL\ ZyWALL IPSec VPN Client	
Install Path	C:\Program Files\ ZyXEL\ ZyWALL IPSec VPN Client	
Desktop Shortcut	ZyWALL IPSec VPN Client	
Start Program	Programs\ZyXEL\ ZyWALL IPSec VPN Client \ ZyWALL IPSec VPN Client	
Uninstall Name	ZyWALL IPSec VPN Client	
Bmp setup 1	Customs\ZyXEL\103.bmp	
Bmp setup 2	Customs\ZyXEL \10551.bmp	
Company Name	ZyXEL	
Product	ZyWALL IPSec VPN Client	
Icone Application	App	
Icone systray 1	Systray1	
Icone systray 2	Systray2	
url company	www.zyxel.com	
url support	Disabled	
url help	Disabled	
url buy	Disabled	
url update	Disabled	
Banner	Banner	
Header	Header	
Logo	Logo	
About	About	
StartMode	Logon	
Protocol	IKEv1, IKEv2	

4 Version number control

				RESULT
Mode	**Platform**	**Executable**		
User / Appli	**All**	VPNConf.exe	**3.6.204.61**	OK
		TgbLogonUI.exe	**3.6.204.61**	OK
		TgbStarter.exe	**4.3.0.1**	OK
		TgbIkeNG.exe	**6.30.0.1**	OK
		VpnCfg.dll	**3.5.0.1**	OK
		VpnToken.dll	**2.1.0.1**	OK
		ComLib.dll	**4, 1, 0, 1**	OK
		tgblibeay32.dll	**0.9.8.31**	OK
		ssleay32.dll	**0.9.8.31**	OK
		DrvVista.dll	**4, 0, 0, 1**	OK
		[lng].dll	**3.0.1.1;** **Esp, Fre, Ptg: 3.0.1.2**	
	x64	TgbCredProv.dll	**6.3.0.1001**	OK
	x64 only	DrvVista.exe	**4, 0, 0, 1**	OK
Kernel / Drivers	**w32**	TGBMPEnum.sys	**2.0.1.3**	OK
	x64	TGBMPEnum.sys	**2.0.2.3**	OK
	w32	TGBVPNVirtM.sys	**2.5.3.1**	OK
	x64	TGBVPNVirtM.sys	**2.5.4.1**	OK

5 General Tests for Customisations

General Tests are to be conducted from the file CDR 6.10