speedtouch™

SpeedTouch™ IPSec VPN to Alcatel OmniPCX Office(OXO) and Enterprise(OXE)

Author: Willem Naudts, Jan Wuyts, Sascha Peckelbeen

Date: April 2006

Version: v1.0

Abstract: The SpeedTouch™620 Business DSL router can extend the reach of a network built around the Alcatel OmniPCX Office (OXO) or Enterprise(OXE) to remote locations connected to the public internet. At such a remote location all the features of the OmniPCX can be made available. Both voice and data services are supported. Through the use of IPSec, a high level of security is guaranteed on the internet connection. IPSec creates a VPN tunnel between the two locations. The OmniPCX Office (OXO) incorporates an IPSec gateway. The OmniPCSX Enterprise (OXE) on the other hand makes use of an external IPSec Gateway, in this case the Fortigate Fortinet 200A. This Application Note describes an easy install procedure for the SpeedTouch™620 that establishes VPN connectivity between a SpeedTouch™620 and the Alcatel OmniPCX. A PC-based installation wizard guides the user through the various configuration steps. It is assumed that the reader is familiar with the various parameters required to complete the SpeedTouch™620 configuration.

The first part of the document describes the connection to the Alcatel OmniPCX Office (OXO). In section 1, the intended application scenario is explained and a reference network is presented. In section 2, the SpeedTouch™ external setup wizard is described. In section 3, the configuration procedures for the most important network components are described. The use of the SpeedTouch™ setup wizard is described in detail. Specific configuration templates are provided that guide you through the process. In section 4, a similar deployment scenario is described to extend the reach of the Alcatel OmniPCX Enterprise (OXE). As this equipment does not support IPSec, a Fortinet IPSec gateway is introduced. The use of the dedicated configuration template is described in section 4.

In a number of appendices, more detailed information can be found on specific topics.

This document does not provide background information about VPN tunnels or technical details of IPSec. For extra information the related Application Notes can be consulted.

Applicability: This application note applies to following products:

- The SpeedTouch™620 Business DSL Router.
  Minimum required system software release 5.4.014, or higher.
- The Alcatel OmniPCX
  - Tests are made against release R4.1 / 023.005
  - Voice Management tool versions: PM5 V210.25.2 and PM5 V210.37.0

For more information on the Alcatel OmniPCX and Fortinet Fortigate, please refer to your local vendor or Alcatel support. THOMSON does not provide technical support in case of configuration problems on the OXO or Fortinet.

Updates: THOMSON continuously develops new solutions, but is also committed to improve its existing products.

For more information on THOMSON's latest technological innovations, documents and software releases, visit us at http://www.speedtouch.com

CONTENTS

1 VPN TUNNEL ACCESS TO ALCATEL OXO

Application

A network built around the Alcatel OmniPCX Office (OXO) can be extended to remote locations connected to the internet. At the remote location, a SpeedTouch™620 is used to establish a secure VPN tunnel through the internet to the OXO. In this way, users at a remote office experience the same data and voice services as users that are locally connected to the OXO. For example, VoIP telephone sets can be connected at the remote location to gain access to the IP telephony service of the OXO.

In the following section a reference network is described that can be used to demonstrate the interoperability of the SpeedTouch™620 and the OXO. While representing a realistic situation, a number of assumptions are made which may differ from a real-world deployment.

Network Overview

The figure below shows the reference network used throughout this document. It consists of an Alcatel OXO and its local terminals located in a main office. It is assumed that the Alcatel OXO is directly connected to the Internet via its WAN interface.

It is possible to connect to the internet via a SpeedTouch™620. Information regarding such a configuration can be found in other Application Notes.

At the remote office, a SpeedTouch™620 is connected to a DSL line to provide internet access for its internal users, which can be both PCs and IP telephones. In the reference configuration, Alcatel Reflex IP telephone sets are used.

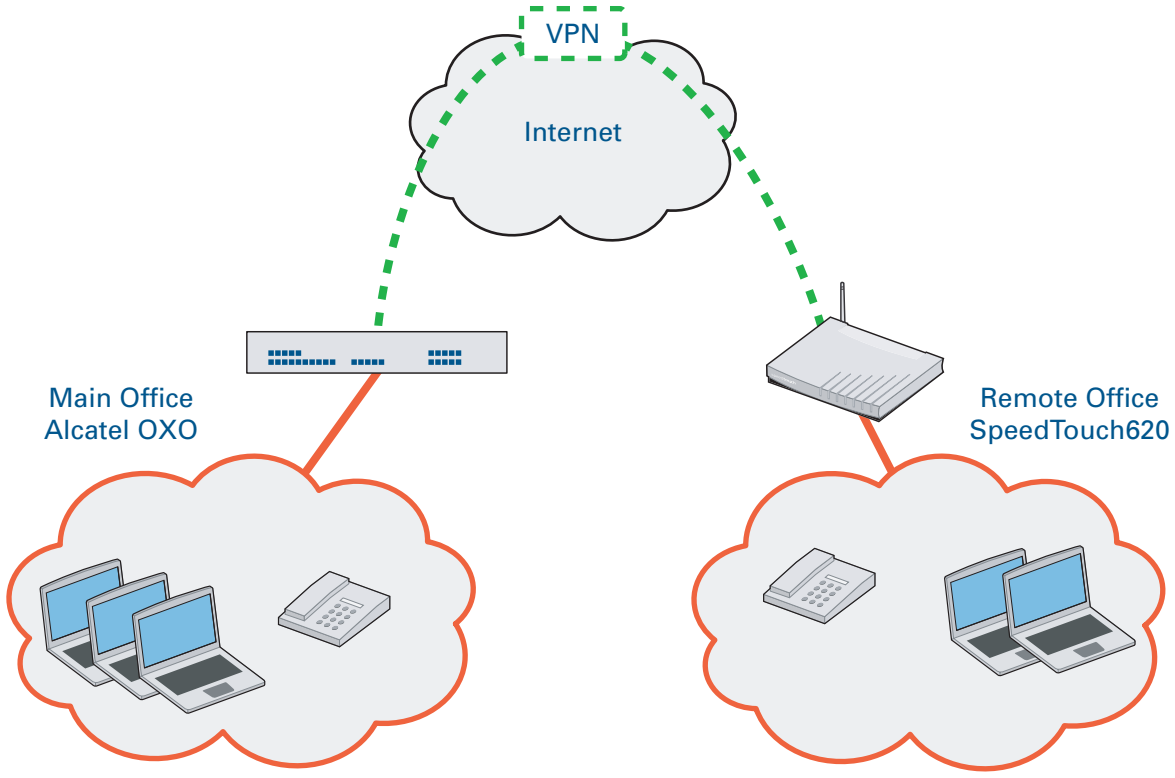


Figure 1: Network overview Alcatel OXO- SpeedTouch™620

Details of the reference network

The OXO has a valid public IP address on its WAN interface, also called its “Black IP address”. It is assumed that a fixed IP address is attributed to the WAN interface. On the LAN side, the OXO serves a private IP address range to interconnect local devices; this is called the “Red IP address range”. For security reasons, this address range is not visible from the public internet.

On the SpeedTouch™620 a DSL line is the WAN interface to the Internet. The public IP address of this WAN interface is its “Black IP address”. It is assumed that a fixed IP address is assigned by the ISP. At the LAN side, the SpeedTouch™620 serves a private local network, also called the “Red IP address range”. For security reasons, this address range is not visible from the public internet.

An IPSec VPN tunnel is established between both sides. This tunnel provides confidential and authenticated communication between the remote office red IP range and the main office red IP range. This application is also known as LAN extension.

The authentication method for the IPSec connection is assumed to make use of pre-shared keys. As a default key, in this document the following key is used: **speedtouch123**. The pre-shared key is configurable by the user and must be set to an identical value at both sides of the connection. More information about the pre-shared key value is found in “ Pre-shared key” on page 20.

Connectivity between the 192.168.92.0/24 and 192.168.1.0/24 IP address ranges is enabled through the secured tunnel.

In this reference network it is preferred to work with statically assigned public IP addresses. This makes the configuration easier. (Dynamically assigned public IP addresses may cause unexpected loss of VPN connectivity.)

In this reference network it is assumed that the LAN’s address ranges are statically assigned.

Parameters of the reference network

The following table lists the main configuration parameters applicable to the reference network proposed in this document.

	Alcatel OXO	SpeedTouch™620
Public IP address	Fixed, provided by ISP	Fixed, provided by ISP
Private IP address range	192.168.92.0/24	192.168.1.0/24
Default pre-shared key	speedtouch123	speedtouch123

VPN Network split tunnelling <> all-in-one

The SpeedTouch™ router supports two alternative approaches to handle internet traffic in combination with VPN traffic.

- With “Split tunnelling” the remote office is capable to directly access the Internet while the VPN connection to the central office is operational. Only the traffic to/from the Main Office is forwarded through the secured tunnel. The advantage of this approach is that non-business related traffic is not interfering with the business-related traffic.

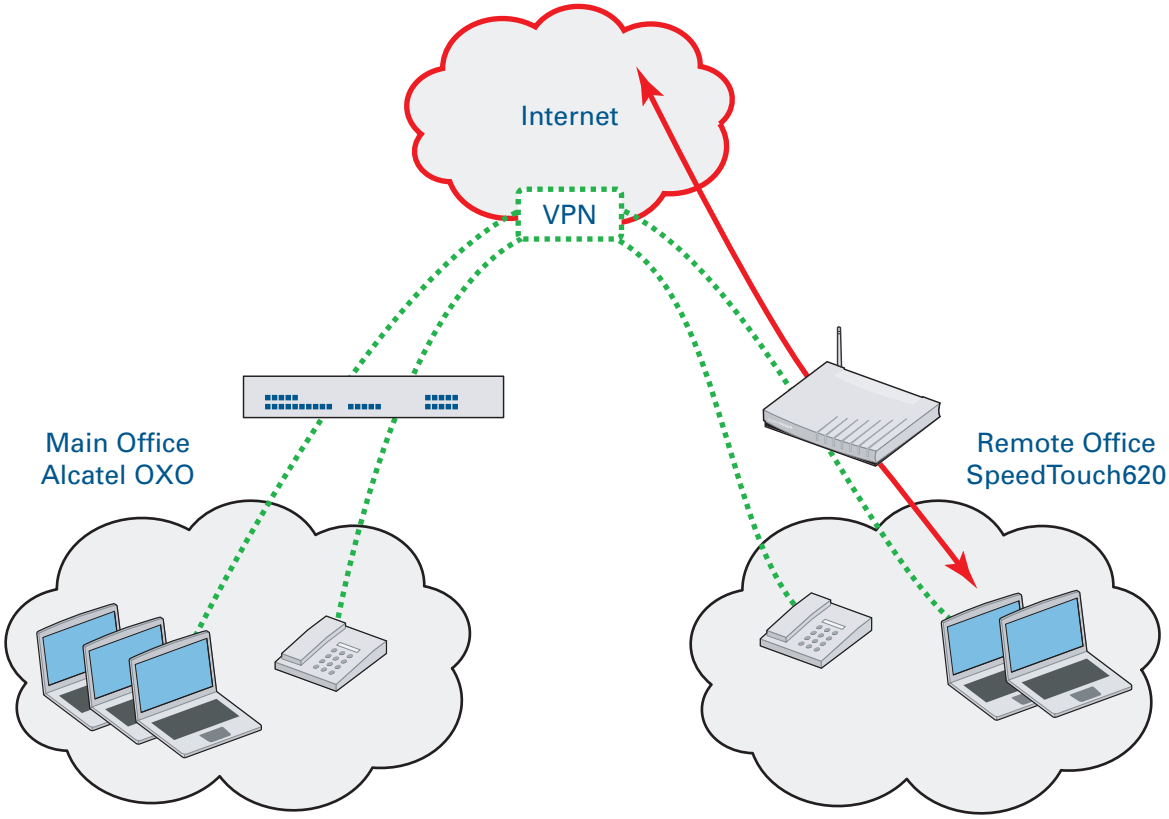


Figure 2: VPN Network, split tunnelling

“Split tunnelling” is selected by default.

- On the other hand, it is possible to route all traffic via the Main Office in order to increase the security of the Office Network: One centralized firewall, Proxy-Server, DMZ …

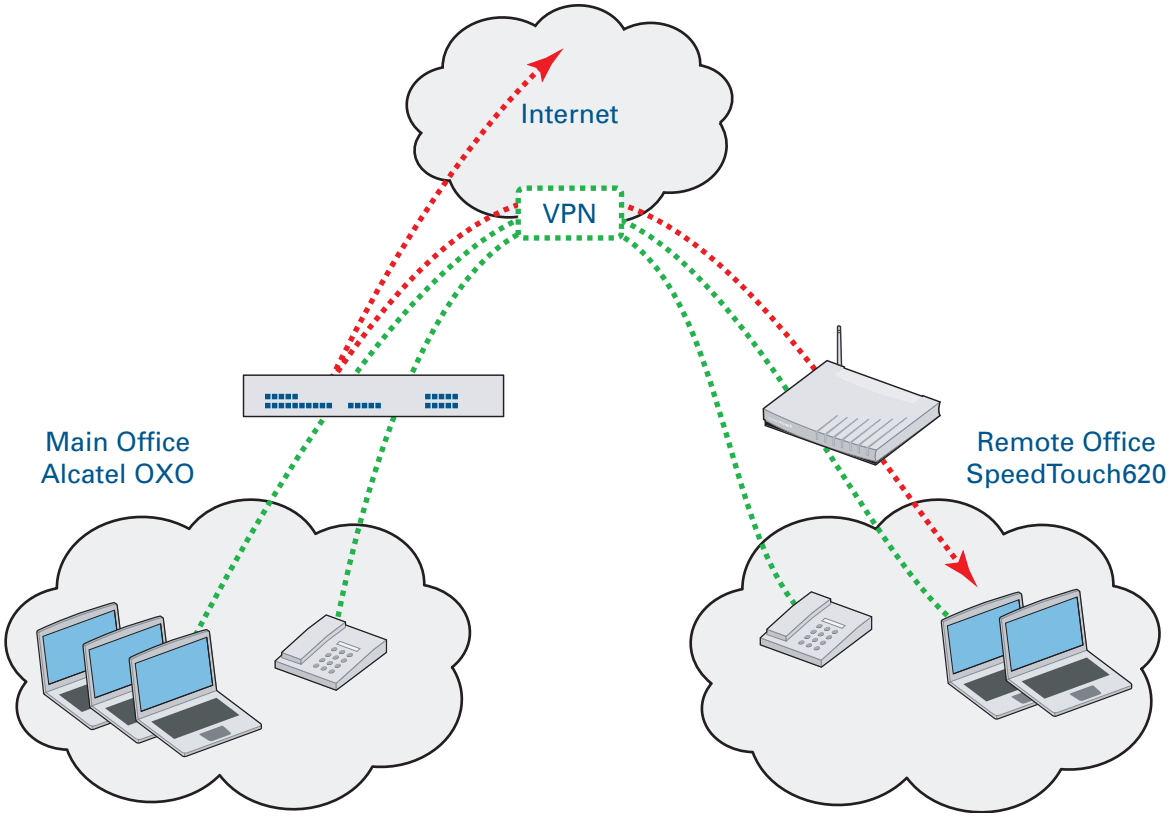


Figure 3: VPN Network, all-in-one

2 SPEEDTOUCH™ INSTALL WIZARD

What is the SpeedTouch™ Install Wizard

The SpeedTouch™ Install Wizard is an application that guides the user through the configuration procedure of the SpeedTouch™ in an easy way, in order to download a specific configuration to the router. The SpeedTouch™ Install Wizard runs on a PC (MS Windows operating system) connected to the local network of the SpeedTouch™ (preferably directly connected to an Ethernet interface of the SpeedTouch™). This setup wizard makes use of a configuration template that presents to the user only the variable configuration parameters relevant to the intended application. All other (fixed) parameters are embedded in the template and are not accessible for the user. A complete configuration is downloaded to the SpeedTouch™ in the final execution step of the wizard.

How to run the SpeedTouch™ Install Wizard

To run the Install Wizard, proceed as follows:

1. Insert the SpeedTouch™ Installation CD ROM.
2. Browse to **SpeedTouch Maintenance -> Reconfigure my SpeedTouch**.
3. Fill out the presented screens as explained in detail below.

Use the SpeedTouch™ Install Wizard to provision a VPN connection to the Alcatel OXO

The templates described in this document configure the SpeedTouch™ for operation in a network environment similar to the reference network described above:

- It can connect to a remote OXO via a VPN tunnel in order to provide VPN services to data and voice terminals locally connected to the SpeedTouch™ router.
- This VPN connection uses IPSec for encryption and authentication.
- The wizard builds SpeedTouch™ configurations that comply with the capabilities of the Alcatel OXO.
- Either split tunnelling is selected at the remote office or access to the internet is through the main office.

SpeedTouch™ Install Wizard templates

Three templates are defined for this type of application:

1. Basic VPN mode.
   This template builds a basic VPN to OXO configuration suitable when PPP is used on the access line of the remote office. PPPoE or PPPoA is user-selectable. Minimal configuration knowledge required for maximum security. Only limited configuration choices are presented to the user. Some advanced settings are preset in the template and can not be altered via the wizard.
2. Advanced VPN mode (PPP).
   This template gives a complete overview of all possibilities for experts. Use this template to build enhanced VPN to OXO configurations suitable when PPP is used on the access line of the remote office. PPPoE or PPPoA is user-selectable. Advanced settings are under control of the user.
3. Advanced VPN mode (IPoA).
   This template gives a complete overview of all possibilities for experts. Use this template to build enhanced VPN to OXO configurations suitable when IPoA is used on the access line of the remote office. Advanced settings are under control of the user.

The templates can only be used via the Install Wizard on the PC, NOT via the embedded Easy Setup Wizard on the SpeedTouch™620.

Quality of Service

In all templates IPQoS is enabled by default. This means that priority is given to specific traffic. Voice traffic for example is attributed a high priority level. This feature is used to enhance the perceived service of the telephone sets. Voice services are sensitive to propagation delay and its variation.

Priority scheduling for traffic coming from LAN-interfaces on the uplink is based on:

- IP Precedence bit (e.g priority level 7 for voice traffic)
- DSCP
- Management: ICMP/IKE/DNS
- Interactive protocols: TELNET/SMTP/IMAP3/IMAP2/POP3/POP2/HTTPPROXY/1080/WWW-HTTP/ESP
- TCP-ACK prioritization

The Alcatel OXO offers the possibility to impose to the client terminals to use priority level 7. In the SpeedTouch™, traffic with priority level 7 is processed with the highest priority. This offers the best possible service to the Alcatel OXO client terminals.

Firewall profiles

The templates described in this application note use the pre-defined firewall levels of the SpeedTouch™. These pre-defined firewall settings are intended to protect the SpeedTouch™ and the private network served by it.

Remote Modem Management Firewall Rules

To allow remote access for SpeedTouch™ management via WAN and/or IPSec, you have to enable the corresponding **SpeedTouch Services**.

More information is found in the SpeedTouch™ User's Guide.

3 CONFIGURATION OVERVIEW

3.1 OXO Configuration

Basic OXO configuration

The OXO can be configured with the web wizards on the OXO. The configuration process is not explained in this document. WAN and LAN connectivity needs to be configured. The WAN-IP address is required as BLACK-IP address for this node. The LAN IP address range is used as the RED-IP address range of the OXO.

Some basic support information about the OXO configuration can be found in the Appendix A and B of this document:

- Appendix A: Overview screen of OXO configuration Wizards
- Appendix B: To check and manipulate the OXO VPN settings

OXO configuration: requirements for VPN connection to SpeedTouch™620

In the OXO configuration, some parameters need to be configured in accordance with the remote side of the VPN connection.

- Remote WAN IP address:
  Check with the ISP that provides DSL access at the remote office, or read it from the SpeedTouch™620 router configuration at the remote office.
- Remote LAN IP range:
  This value depends upon the LAN network connected to the SpeedTouch™620 router at the remote office.

  For example: in the reference network of this document, the remote LAN IP range is 192.168.1.0/24.
- VPN peer authentication:
  In this document it is assumed that pre-shared key authentication is used. In the SpeedTouch™ Install Wizard, a default key is preset, using the following password: **speedtouch123**. If this default value is used in the SpeedTouch™620, it should also be set in the OXO configuration.
- VPN security profile:
  Select either **Standard Security** or **High Security** in the OXO.

3.2 SpeedTouch™ Install Wizard Configuration Procedure

3.2.1 Main Configuration Steps

The External Wizard guides the user through all the configuration steps of the SpeedTouch™ router. In this section the main steps are indicated. The detailed configuration procedure and the structure of the configuration screens are explained in subsequent sections:

1. Start the SpeedTouch™ Install Wizard
2. Detection Process
3. Select your SpeedTouch™
4. Select your Service
5. Complete the various configuration windows
6. Download Configuration
7. Close the External Wizard

3.2.2 Start the SpeedTouch™ Install Wizard

Start procedure

Proceed as follows:

1. Insert the CD-Rom in a PC that is located in the LAN network of the SpeedTouch™ that needs to be configured
2. Open the **Run** dialog window on the PC.
3. Browse to **SpeedTouch Maintenance -> Reconfigure my SpeedTouch**.

   When the Wizard starts up, the application starts a pop-up window that will guide you through the configuration steps. The first screen is the welcome screen.
4. Click **Next** to continue the configuration process. This action automatically starts the SpeedTouch™ detection process.

Welcome window

When the Install Wizard starts up, the application starts a pop-up window that will guide you through the configuration steps. The first window is the welcome screen shown below.

Figure 4: Install Wizard Welcome screen

Click **Next** to continue the configuration procedure. This action automatically starts the SpeedTouch™ router detection process.

Click **Cancel** to abort the configuration procedure. This action closes the Install Wizard.

3.2.3 Detection Process

Phases of the SpeedTouch™ router detection process

Phase	Name	Description
1	Start	The SpeedTouch™ router detection process starts automatically when the user clicks **Next** in the welcome screen. The welcome screen disappears and is replaced by the Progress screen.
2	Progress	The wizard searches the local network for SpeedTouch™ routers. During this phase, the Progress screen indicates the progress of the detection process. Wait until the process automatically terminates.
3	End	The wizard has finished the search for SpeedTouch™ routers and displays all the devices encountered on the LAN.

SpeedTouch™ Check window

When the user clicks **Next** in the Welcome screen, the following window is displayed. A progress indicator bar indicates the progress of the detection process. This window automatically disappears when the detection process is completed. No user action is required while this window is displayed.

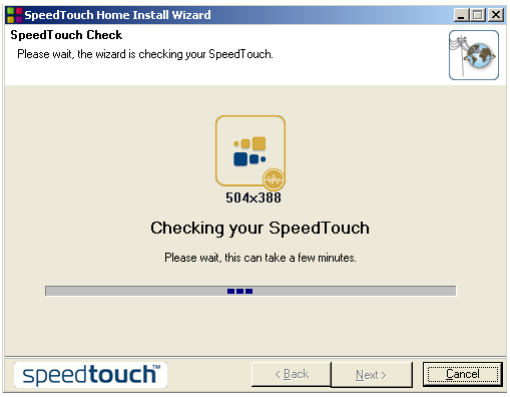


Figure 5: SpeedTouch™ Check window

3.2.4 Select your SpeedTouch™

Selection procedure

If more than one SpeedTouch™ device is connected to your network, the Selection window appears. In this case, proceed as follows:

1. Select a SpeedTouch™ router by clicking on the name.
2. If desired, the details of the selected device can be displayed
3. Click **Next** to proceed.

   If a password is required to gain access to the selected router, then automatically a password window will pop-up.
4. After gaining access, the **Configuration of SpeedTouch** window is shown.
5. Select to configure the SpeedTouch™ router by clicking the corresponding selection button.
6. Click **Next** to continue the configuration of the selected router.

Detected Device(s) window

This window is automatically displayed at the end of the detection process. It shows all the SpeedTouch™ devices found on the local network. The user selects the device to be configured by clicking on the name of a device.

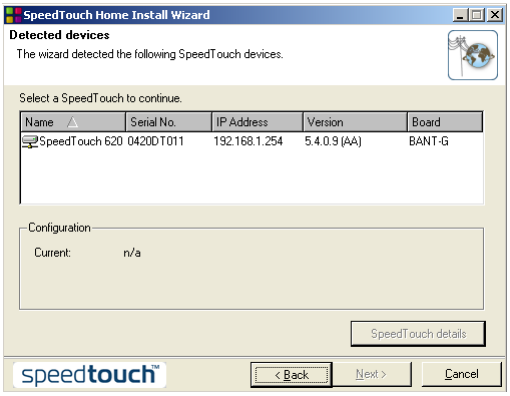


Figure 6: Detected Device(s)

Button	Function
SpeedTouch Details	Display the details of the selected device.
Back	Return to the previous window
Next	Continue the configuration procedure of the selected device.
Cancel	Abort the configuration process and end the wizard.

Since all windows contain the **Back**, **Next** and **Cancel** buttons, this information is not repeated in the remainder of this document.

Configuration of SpeedTouch window

Figure 7: Configuration of SpeedTouch window

Button	Function
Yes	Click this button if you intend to modify the configuration to the SpeedTouch™ router
No	Click this button if you intend to leave the SpeedTouch™ router configuration unmodified. Quits the Install Wizard.

3.2.5 Select your Service

Selecting Templates in the SpeedTouch™ Install Wizard: VPN to OXO

Three “VPN to OXO” templates are created to simplify the configuration procedure and to avoid interoperability issues.

The three templates are found under the heading **Service** in the **Internet Provider** window:

Select ….	When ….
Basic VPN-OXO mode	▸ PPP protocol is used on the DSL access line. ▸ You prefer to easiest way to configure the VPN connection. ▸ You let the configuration wizard control the advanced settings for you. For more information, see “3.2.6 Basic VPN-OXO Mode” on page 17.
Advanced VPN-OXO mode (PPP)	▸ PPP protocol is used on the DSL access line. ▸ You are familiar with the advanced settings. ▸ You want full control over all configuration parameters. For more information, see “3.2.7 Advanced VPN-OXO Modes” on page 22.
Advanced VPN-OXO mode (IPoA)	▸ IPoA is used on the DSL access line. ▸ You are familiar with the advanced settings. ▸ You want full control over all configuration parameters. For more information, see “3.2.7 Advanced VPN-OXO Modes” on page 22.
Click **Next** to confirm your selection and proceed with the configuration procedure	

Service Provider Window

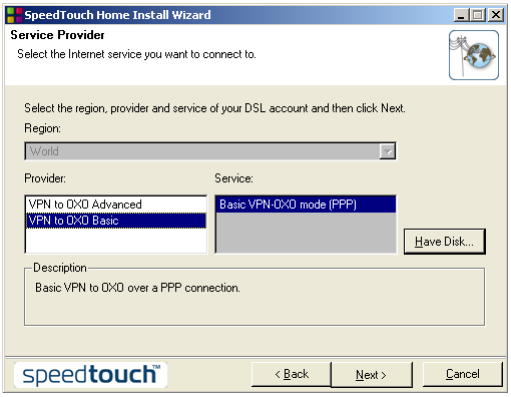


Figure 8: Template selection in Install Wizard

This window allows you to select:

- Basic VPN-OXO mode (PPPoA, PPPoE)
- Advanced VPN-OXO mode (PPPoA, PPPoE)
- Advanced VPN-OXO mode (IPoA)

3.2.6 Basic VPN-OXO Mode

Basic VPN-OXO mode configuration procedure

This is the easiest installation for the SpeedTouch™ with most variables pre-configured in the wizard template. The procedure consists of a number of windows that have to be completed subsequently. Firstly, the procedure is described. Secondly, the structure of the individual windows is described.

Step	Action
1	Complete the **Routed Internet Connection** window. ▸ Fill in **VPI/VCI** : mandatory ▸ Select **PPP mode** : mandatory Click **Next** to proceed.
2	Complete the **Internet Account Settings** window. ▸ Fill in **User name** field : mandatory ▸ Fill in **Password** field : mandatory ▸ Confirm the password : mandatory Click **Next** to proceed.
3	Complete the **SpeedTouch Security** window. ▸ Select the firewall level : mandatory Click **Next** to proceed.
4	Complete the **VPN Gateway** window. ▸ **Pre-shared key** field: default value is **speedtouch123**. Set the pre-shared key value in correspondence with the OXO pre-shared key. Take care to clear the **Pre shared key** field before you type in a different key. The OXO places restrictions on the format of the pre-shared key. A valid key contains at least 8 alphanumerical characters, of which at least one character is a digit. For more information, please consult the OXO documentation. ▸ **Address of the OXO** field: mandatory. Enter either an IP address or a DNS name. ▸ Select the security level used by the OXO. Click **Next** to proceed.
5	Complete the **Site-to-site VPN** window. ▸ **OXO Private Submit** field: mandatory ▸ **Your local ID** field: Enter the public IP address of your SpeedTouch™, preceded by the text **(addr)**. The OXO uses IP addresses for identification during the IPSec negotiations, so it is mandatory to use the format **(addr)x.x.x.x** ▸ **OXO ID** field: Enter the public IP address of the OXO, preceded by the text **(addr)**. The OXO uses IP addresses for identification during the IPSec negotiations, so it is mandatory to use the format **(addr)x.x.x.x** Click **Next** to proceed.

Step	Action
6	All configuration parameters have now been entered. Click **Next** to proceed. As a result, the **Configuration of SpeedTouch** window is shown. The remainder of the configuration procedure is found in section "3.2.8 Download Configuration" on page 34.

Routed Internet Connection window

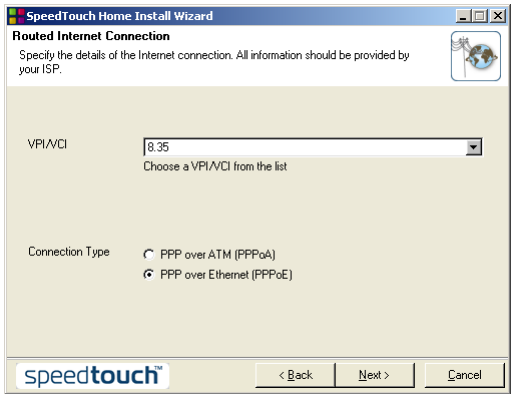


Figure 9: Routed Internet Connection window

This window has the following structure:

Area	Function
VPI/VCI	Select the virtual connection identifier (VPI/VCI) according to the ISP requirements for the DSL line. Select from list or enter an other value. The default value is 8/35.
Connection mode	Select the PPP mode according to the ISP requirements for the DSL line. The possible values are: ▸ **PPPoA** ▸ **PPPoE_llc/snap**: PPP with LLC/ SNAP encapsulation The default mode is **PPPoE**.

Internet Account Settings window

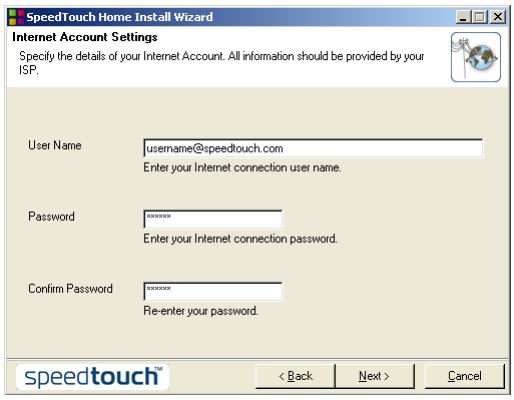


Figure 10: Internet Account Settings window

This window has the following structure:

Area	Function
User Name	Enter the user name for the PPP account. This information is provided by the Internet Service Provider (ISP).
Password **Confirm Password**	Enter the password for the PPP connection. This information is provided by the Internet Service Provider (ISP).

SpeedTouch Security window

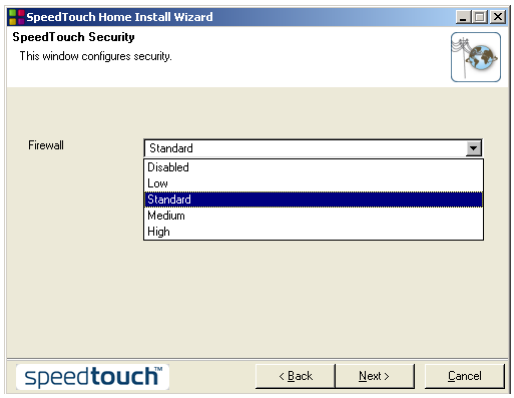


Figure 11: SpeedTouch Security window

This window has the following structure:

Area	Function
Firewall	Select one of the pre-defined Firewall settings.

VPN Gateway window

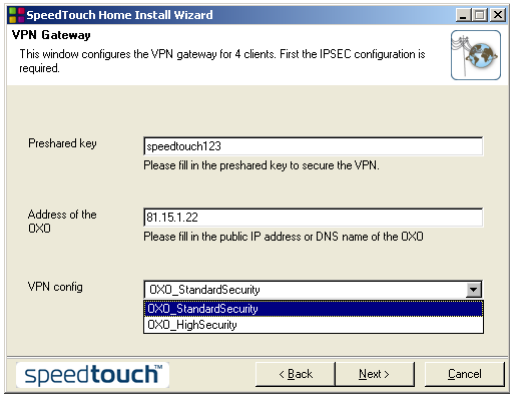


Figure 12: VPN Gateway window

This window has the following structure:

Area	Function
Pre-shared key	Set the pre-shared key value in accordance with the value configured in the OXO. By default, this field contains the value: speedtouch123. Take care to clear this field before typing a new value for the pre-shared key. Because the key value is not shown in cleartext in this field, the entered key value can not be verified. It is important that no characters of a previous key are mixed with a new key.
Address of the OXO	Set the public IP address of the WAN interface of the OXO.
VPN config	Select the desired level of security of the VPN tunnel in accordance with the OXO configuration. Possible values are: ▸ OXO StandardSecurity ▸ OXO HighSecurity For more information, see " Check or change the VPN settings on the OXO" on page 44.

The OXO places restrictions on the format of the pre-shared key. A valid key contains at least 8 alphanumerical characters, of which at least one character is a digit. For more information, please consult the OXO documentation.

Site-to-site VPN window

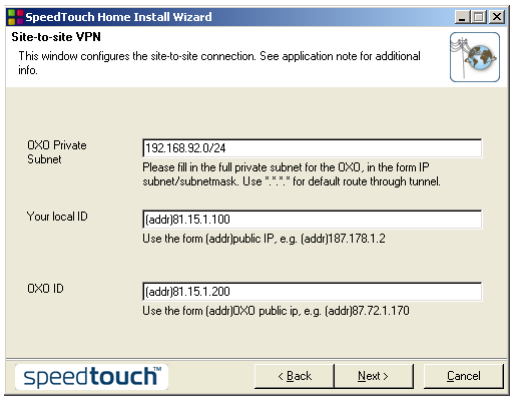


Figure 13: Site-to-site VPN window

This window has the following structure:

Area	Function
OXO Private Subnet	Set the private IP subnet served by the OXO. Default value: **192.168.92.0/24**.
Your local ID	Insert the public IP address of your SpeedTouch™. During the IPSec negotiations, the OXO recognizes IP addresses only.
OXO ID	Insert the public IP address of the OXO. During the IPSec negotiations, the OXO uses IP addresses only.

Configuration of SpeedTouch window

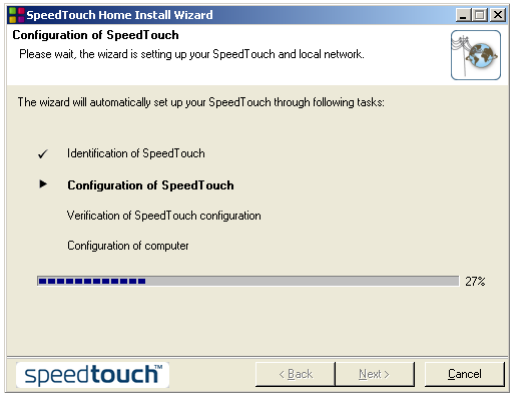


Figure 14: Configuration of SpeedTouch window

3.2.7 Advanced VPN-OXO Modes

Two advanced templates are defined to set up a connection between a SpeedTouch™ and an Alcatel OXO, one for PPP connections and one for IPoA connections. The advanced templates give the user the control over all important and advanced settings. These advanced templates only differ from each other in one window, the connection configuration window. The configuration procedure for the VPN tunnel is identical for both.

The selection between IPoA and PPP connectivity to the Internet depends on the DSL subscription with the ISP. IPoA is a fixed always-on connection to the Internet with less overhead than the PPP protocol.

PPP connectivity on the other hand is much more dynamic. Both connection types are commonly used by Internet Service Providers.

Advanced VPN-OXO mode configuration procedure

The advanced installation modes for the SpeedTouch™ allow the user full control over all relevant configuration parameters. The procedure consists of a number of windows that have to be completed subsequently. Firstly, the procedure is described. Secondly, the structure of the individual windows is described.

Step	Action
1	In case you selected the **Advanced VPN-OXO mode (IPoA)** service: proceed with step 2. In case you selected the **Advanced VPN-OXO mode (PPP)** service: proceed with step 3.
2	In case you selected the **Advanced VPN-OXO mode (IPoA)** template, then the **Connectivity** window is presented to the user. This window is shown in " IPoA Connection: Connectivity Window" on page 26. Complete the **Connectivity** window. ▸ Enter the **Public IP address**: mandatory ▸ Enter a **VPI/VCI** combination: mandatory Click **Next** to proceed. Proceed with Step 5 of this procedure.
3	In case you selected the **Advanced VPN-OXO mode (PPP)** template, then the **Routed Internet Connection** window is presented to the user. This window is shown in " PPP connection: Routed Internet Connection window" on page 26. Complete the **Routed Internet Connection** window. ▸ Fill in **VPI/VCI** : mandatory ▸ Select **PPP mode** : mandatory Click **Next** to proceed.
4	Complete the **Internet Account Settings** window. ▸ Fill in **User name** field: mandatory ▸ Fill in **Password** field: mandatory ▸ Confirm the password: mandatory. Click **Next** to proceed.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>5</td><td>Complete the SpeedTouch addressing window. This window is shown in “ SpeedTouch addressing window” on page 27.
▸ Enter the LAN side SpeedTouch IP address: mandatory. This is the IP address to be used by all LAN network devices as their Gateway address.
▸ Enter the Subnet mask : mandatory
Click Next to proceed.</td></tr>
<tr><td>6</td><td>Complete the DHCP window.
▸ Select whether you want to use DHCP in the remote office LAN network : mandatory.
Possible selections for DHCP on LAN:
▸ Yes: enables the Speedtouch™ DHCP server.
▸ No: disables the Speedtouch™ DHCP server.
<table>
<tr><th>In case DHCP is enabled:</th><th>In case DHCP is disabled:</th></tr>
<tr><td>▸ Enter the first IP address of the DHCP address pool. Default value: 192.168.1.64
▸ Enter the last IP address of the DHCP address pool. Default value: 192.168.1.253</td><td>Note In case DHCP is disabled, the default values of first and last IP addresses are irrelevant.</td></tr>
</table>
Click Next to proceed.</td></tr>
<tr><td>7</td><td>Complete the advanced SpeedTouch Security window.
▸ Select one of the pre-defined Firewall rule sets.
▸ Select the UPnP mode : optional.
▸ Specify a De-Militarized Zone (DMZ) IP address : optional
▸ Enable or disable Remote management via WAN interface: optional. (Default: Deactivated)
Click Next to proceed.</td></tr>
<tr><td>8</td><td>Complete the advanced VPN Gateway window.
▸ Specify Pre-shared key: mandatory (default in template: speedtouch123).
The pre-shared key value must match the OXO pre-shared key.
Note Take care to clear the Pre-shared key field before you type in a different key.
Note The OXO places restrictions on the format of the pre-shared key. A valid key contains at least 8 alphanumerical characters, of which at least one character is a digit. For more information, please consult the OXO documentation.
▸ Select the Phase 1 Encryption and Phase 2 Encryption methods in accordance with the settings on the OXO : mandatory.</td></tr>
</table>

Step	Action
9	Complete the advanced **Site-to-site VPN** window (part 1). ▸ **Address of the OXO** field: mandatory. Enter either an IP address or a DNS name. ▸ **OXO Private Subnet** field : mandatory. If you want to send all your traffic through the VPN tunnel (including access to the Internet), then make the VPN tunnel your default route. To do so, enter the following: ***.*.*.*** ▸ **Your local ID** field: Enter the public IP address of your SpeedTouch™, preceded by the text **(addr)**. The OXO uses IP addresses for identification during the IPSec negotiations, so it is mandatory to use the format **(addr)x.x.x.x** ▸ **OXO ID** field: Enter the public IP address of the OXO, preceded by the text **(addr)**. The OXO uses IP addresses for identification during the IPSec negotiations, so it is mandatory to use the format **(addr)x.x.x.x** Click **Next** to proceed. Complete the advanced **Site-to-site VPN** window (part 2). ▸ **Local Private Subnet** field : mandatory. Click **Next** to proceed.
10	Complete the advanced **VPN Enhanced Settings** window. ▸ Select whether you want to start up the VPN connection as soon as the connection is available. ▸ Select whether your SpeedTouch™ can be accessed through the VPN tunnel. Click **Next** to proceed.
11	Complete the advanced **Dynamic DNS** window. ▸ Select your dynamic DNS **Service Provider**: optional. ▸ Enter the dynamic DNS **Host Name**: optional. ▸ Enter the **User Name** and **Password** for the DNS service. Click **Next** to proceed.
12	Complete the advanced **Time Configuration** window. Optionally, you can select to enable automatic time configuration by clicking the corresponding check box. ▸ Specify the **Primary** and **Secondary Time Server**: optional. Click **Next** to proceed.
13	Complete the advanced **SNMP Settings** window. Optionally, you can select to enable the SNMP agent by clicking the corresponding check box. ▸ Complete the **Read-Only Community** field. By default, the value **public** is used. ▸ Complete the **R/W Community** field. By default, the value **private** is used. Click **Next** to proceed.

Step	Action
14	Complete the advanced **Access Control** window. ▸ For security reasons, access to the SpeedTouch™ router can be restricted by means of a password. If this is desired, then fill in the optional fields. ▸ Fill in **User Name** field: optional ▸ Fill in **Password** field: optional Otherwise, leave the optional fields blank. Click **Next** to proceed.
15	All configuration parameters have now been entered. Click **Next** to proceed. As a result, the **Configuration of SpeedTouch** window is shown (see " Configuration of SpeedTouch window" on page 35). The remainder of the configuration procedure is found in section "3.2.8 Download Configuration" on page 34.

Service Provider Window

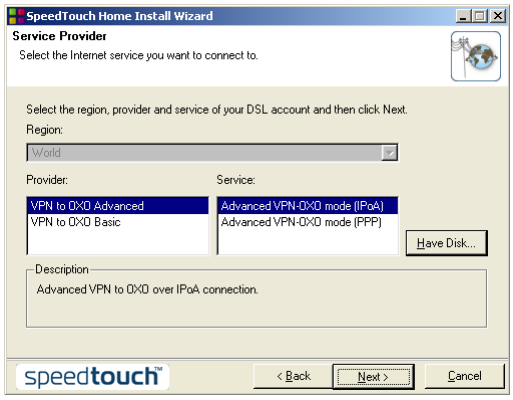


Figure 15: Template selection in Install Wizard

This window allows you to select:

- Basic VPN-OXO mode (PPPoA, PPPoE)
- Advanced VPN-OXO mode (PPPoA, PPPoE)
- Advanced VPN-OXO mode (IPoA)

IPoA Connection: Connectivity Window

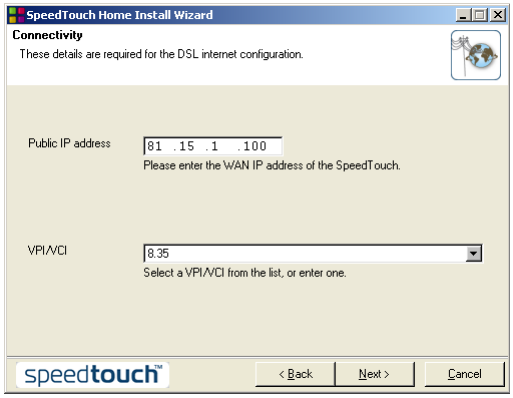


Figure 16: IPoA connection: Connectivity window

This window has the following structure:

Area	Function
Public IP address	Set the public IP address to be used on the DSL line of the SpeedTouch™ router. This information is provided by the ISP.
VPI/VCI	Set the virtual connection identifier (**VPI/VCI**) according to the ISP requirements for the DSL line. The syntax to use in this field is: VPI.VCI The default value is **8.35**.

PPP connection: Routed Internet Connection window

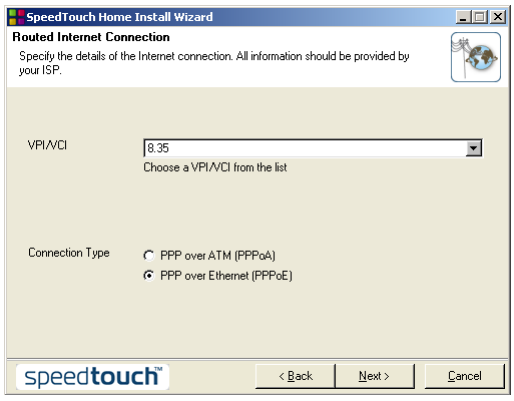


Figure 17: PPP connection: Routed Internet Connection window

This window is identical to the window shown in " Routed Internet Connection window" on page 18. See the accompanying text for window structure.

PPP connection: Internet Account Settings window

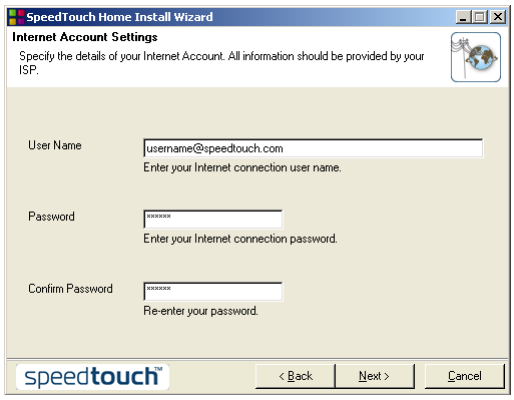


Figure 18: PPP connection: Routed Internet Connection window

This window is identical to the window shown in " Internet Account Settings window" on page 19. See the accompanying text for window structure.

SpeedTouch addressing window

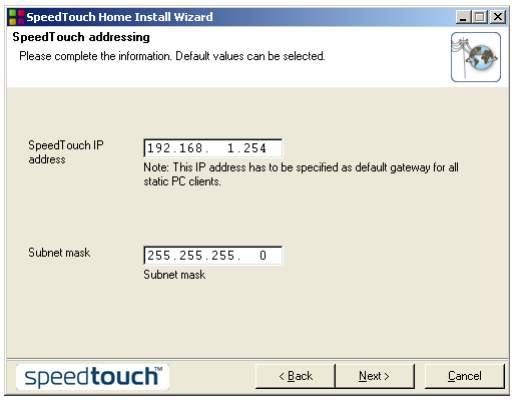


Figure 19: SpeedTouch addressing window

This window has the following structure:

Area	Function
SpeedTouch IP address	Router IP address is the LAN interface IP address of the router.
Subnet mask	The subnet mask in combination with the IP address defines the private IP address range of the SpeedTouch™. In case DHCP is used, the address pool is restricted to 256 IP addresses. Therefore the subnet mask is restricted to subnets of maximum 256 IP addresses. Valid subnet masks are in the range "/24" to "/31" (or in dotted format: 255.255.255.0 to 255.255.255.254).

DHCP window

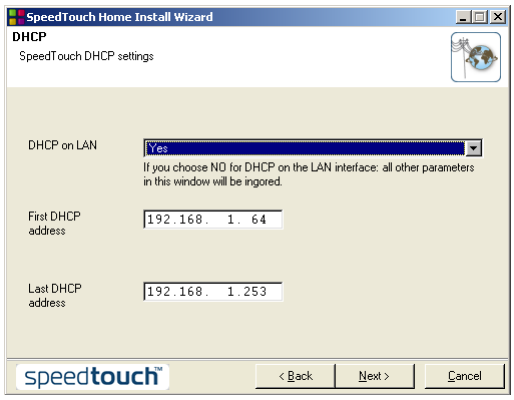


Figure 20: Advanced DHCP window

This window has the following structure:

Area	Function
DHCP on LAN	Select whether to activate the internal DHCP server of the SpeedTouch™.
First DHCP address	Configure the start address of the DHCP IP address pool. Default value is **192.168.1.64**.
Last DHCP address	Configure the end address of the DHCP IP address pool. Default value is **192.168.1.253**.

In case the SpeedTouch™ DHCP server is disabled, the default DHCP addresses have no effect.

Advanced SpeedTouch Security window

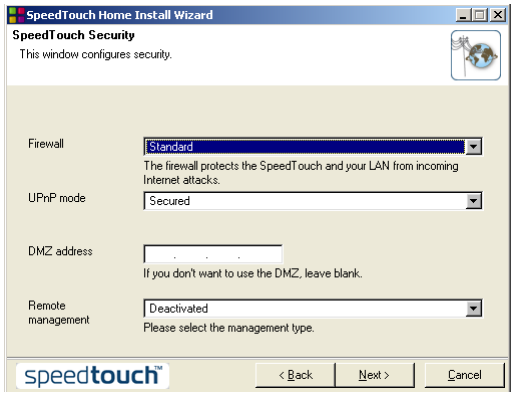


Figure 21: Advanced SpeedTouch Security window

This window has the following structure:

Area	Function
Firewall	Select one of the pre-defined Firewall settings. Possible values: **Disabled, Low, Standard, Medium, High.** Default value is **Standard.**
UPnP mode	Select the UPnP™ mode. Possible values: **Deactivated, Secured** and **Full.** Refer to the product's user documentation for more information. Default value: **Secured.**
DMZ address	Optionally, the IP address of a De-Militarized Zone can be specified.
Remote management	This setting adapts the SpeedTouch™ firewall rules allowing or denying access from the WAN interface for remote management of the SpeedTouch™ router. Possible values: **Deactivated, Web, Web_on_tcp8080.** Default value: **Deactivated.**

Advanced VPN Gateway window

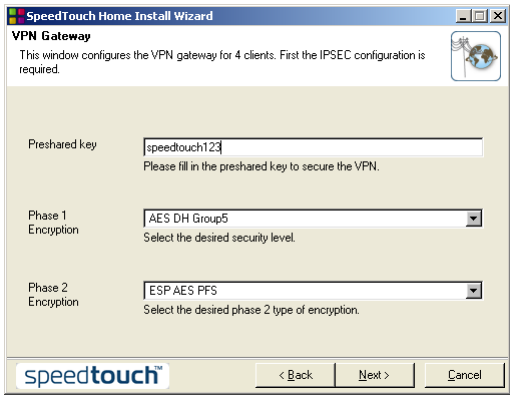


Figure 22: Advanced VPN Gateway window

This window has the following structure:

Area	Function
Pre-shared key	Set the pre-shared key value in accordance with the value configured in the OXO. By default, this field contains the value: **speedtouch123.** **Note** Take care to clear this field before typing a new value for the pre-shared key. Because the key value is not shown in cleartext in this field, the entered key value cannot be verified.
Phase 1 encryption	Select the security descriptor to be used for the IKE negotiation phase (phase 1). Select a descriptor in accordance with the security method used at the OXO side.
Phase 2 encryption	Select the security descriptor to be used for the IPSec communication phase (phase 2). This descriptor should correspond to the security method used at the OXO side.

Note The OXO places restrictions on the format of the pre-shared key. A valid key contains at least 8 alphanumerical characters, of which at least one character is a digit. For more information, please consult the OXO documentation.

Advanced Site-to-site VPN window (part 1)

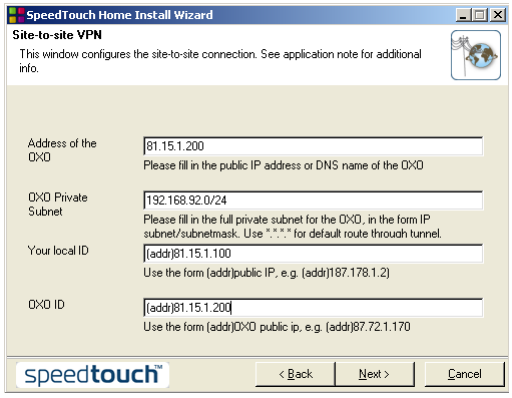


Figure 23: Advanced Site-to-site VPN window (part 1)

This window has the following structure:

Area	Function
Address of the OXO	Set the public IP address of the WAN interface of the OXO.
OXO Private Subnet	Set the private IP subnet served by the OXO. This is the network you can reach from the remote site. If you want to send all your traffic through the VPN tunnel (including access to the Internet), then make the VPN tunnel your default route. To do so, enter the following: ***.*.*.*** Default value: **192.168.92.0/24**.
Your local ID	Insert the public IP address of your SpeedTouch™. During the IPSec negotiations, the OXO recognizes IP addresses only.
OXO ID	Insert the public IP address of the OXO. During the IPSec negotiations, the OXO uses IP addresses only.

Advanced Site-to-site VPN window (part 2)

Figure 24: Advanced Site-to-site VPN window (part 2)

This window has the following structure:

Area	Function
Local Private Subnet	Set the private IP subnet served by the SpeedTouch™. Default value: **192.168.1.0/24**.

Advanced VPN Enhanced Settings window

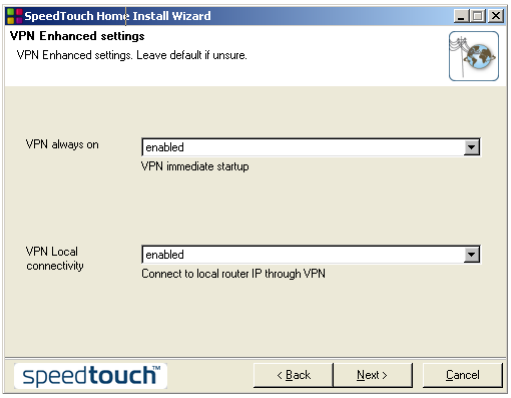


Figure 25: Advanced Site-to-site VPN window

This window has the following structure:

Area	Function
VPN always on	Select **enabled** when you want the VPN link to be established as soon as the SpeedTouch™ establishes the Internet connection. When you select **disabled**, the establishment of the VPN link is triggered by traffic that complies to the traffic policy.
VPN Local connectivity	If you select **enabled**, your SpeedTouch™ can be accessed via the VPN link.

Advanced Dynamic DNS window

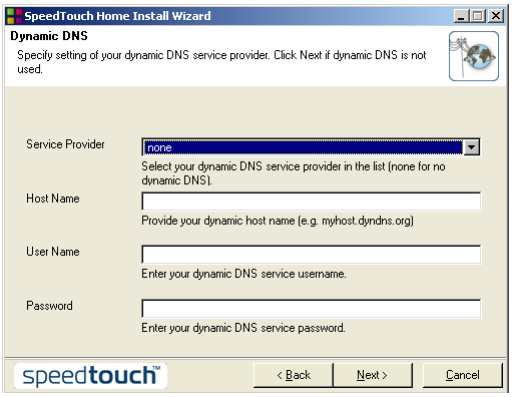


Figure 26: Advanced Dynamic DNS window

This window has the following structure:

Area	Function
Service Provider	Fill out your Dynamic DNS service provider. This is optional.
Host Name	Fill out the Dynamic DNS host name. This is optional.
User Name	Fill out your user name for the Dynamic DNS service. This is optional.
Password	Fill out your password for the Dynamic DNS service. This is optional.

Advanced Time Configuration window

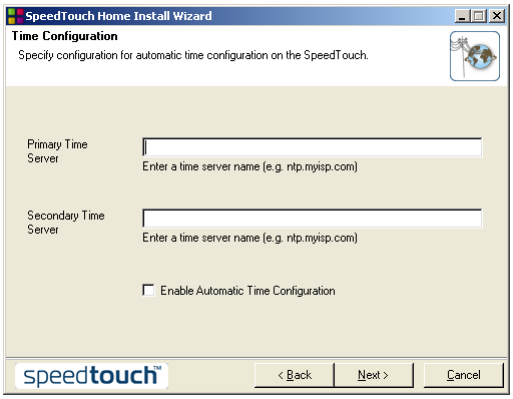


Figure 27: Advanced Time Configuration window

This window has the following structure:

Area	Function
Primary Time Server	Fill out the name of the primary Network Time Server. This is optional.

Area	Function
Secondary Time Server	Fill out the name of the secondary Network Time Server. This is optional.
Enable Automatic Time Configuration	To enable Automatic Time Configuration, click the check box.

Advanced SNMP Settings window

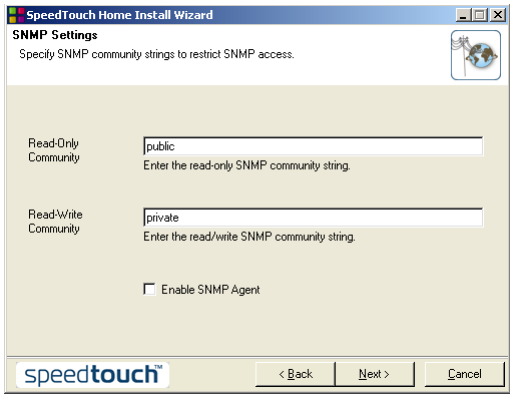


Figure 28: Advanced SNMP Settings window

This window has the following structure:

Area	Function
Read-Only Community	Specify the name of the group that has SNMP Read-Only access to the SpeedTouch™ router. For more information, refer to the Application note on Remote Management. Default Read-Only Community name: **public**
R/W community	Specify the name of the group that has SNMP Read and write access to the SpeedTouch™ router. For more information, refer to the Application note on Remote Management. Default value R/W community name: **private**.
Enable SNMP Agent	To enable the internal SNMP agent, click the check box.

Advanced Access Control window

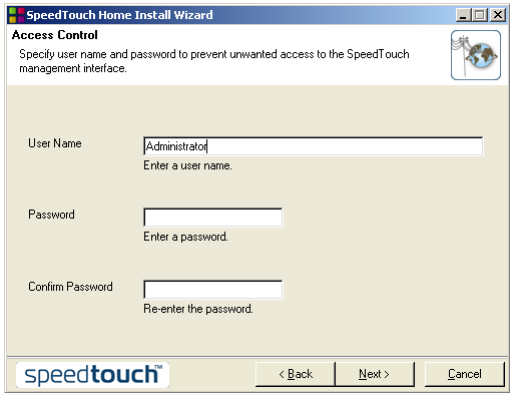


Figure 29: Advanced Access Control window

This window has the following structure:

Area	Function
User Name	Configure a user name for the SpeedTouch™ router. This is optional.
Password **Confirm Password**	Configure a password for the SpeedTouch™ router. This is optional.

3.2.8 Download Configuration

Download process

As soon as the Configuration of SpeedTouch window is displayed, the download process is automatically started. During the download process the progress is displayed.

Complete the configuration procedure

To complete the configuration procedure and terminate the Install Wizard, proceed as follows:

1. Wait until the download process terminates. The **Completion** window is displayed.
2. Exit the wizard by pressing the **Finish** button.

At this point, everything is configured. Internet connectivity and Connectivity through the secured tunnel to the Main Office should be established. To check the parameters and the connectivity please see: "Appendix D debug information Advanced" on page 50.

Configuration of SpeedTouch window

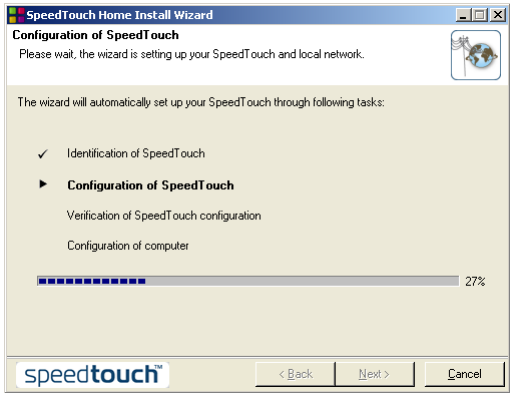


Figure 30: Configuration of SpeedTouch window

Completion window

Figure 31: Completing the SpeedTouch™ Install Wizard successfully

4 VPN TUNNEL ACCESS TO FORTINET FORTIGATE 200A

Application

A network built around the Alcatel OmniPCX Enterprise (OXE) can be extended to remote locations connected to the internet. Unlike the Alcatel OXO, the OXE does not have an integrated IPSec gateway. Therefore, a separate IPSec gateway, the Fortinet FortiGate 200A is inserted between the OXE and the internet. In this way, a secure VPN is constructed. At the remote location, a SpeedTouch™620 is used to establish a secure VPN tunnel through the internet to the Fortinet gateway. As a result, users at a remote office experience the same data and voice services as users that are locally connected to the OXE.

In the following section a reference network is described that can be used to demonstrate the interoperability of the SpeedTouch™620 and the Fortinet FortiGate, connected to the OXE.

Network Overview

The figure below shows the network topology for connection to an OXE. It consists of an Alcatel OXE and its local terminals (PCs and VoIP phones) located in a main office. The Alcatel OXE is connected to the Internet via a Fortinet IPSec gateway.

At the remote office, a SpeedTouch™620 is connected to a DSL line to provide internet access for its internal users, which can be both PCs and VoIP telephones.

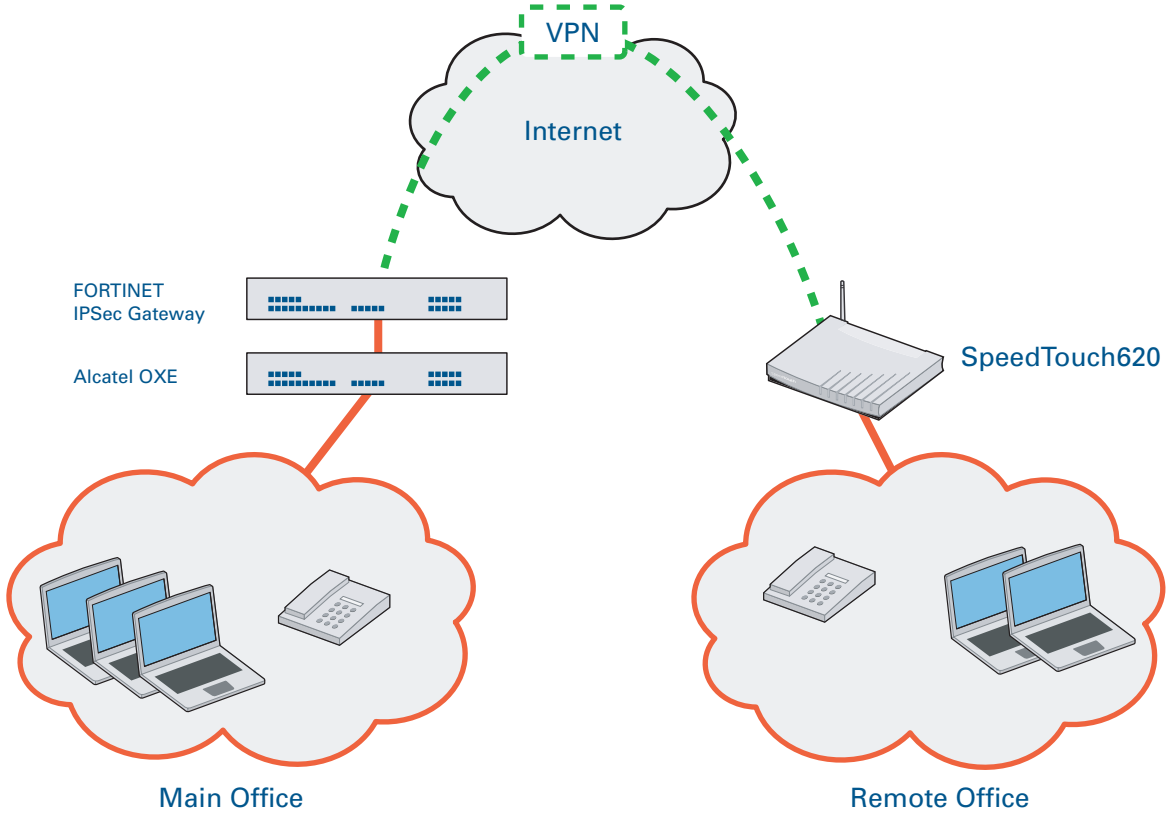


Figure 32: Network overview

5 CONFIGURATION FOR FORTINET

Introduction

In this chapter, the configuration procedures for both the Fortinet FortiGate and the SpeedTouch™620 are presented. For detailed information about the Fortinet FortiGate 200A, please refer to the manufacturer's documentation.

5.1 VPN configuration on FortiGate products

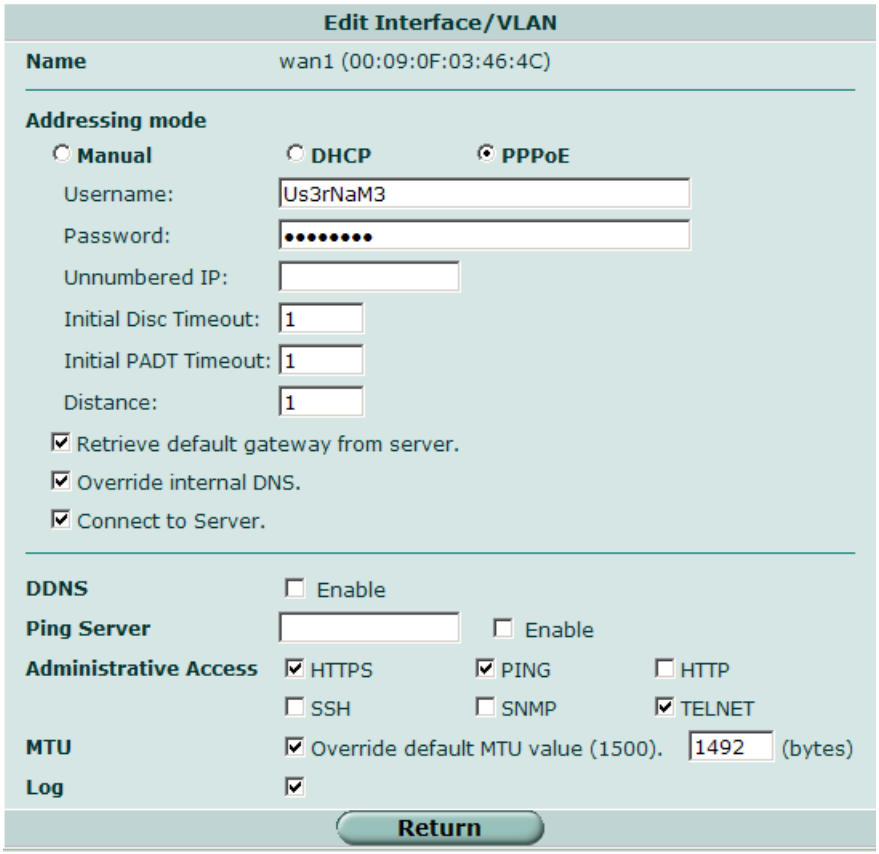
Configuration procedure

Proceed as follows to configure ta VPN on the FortiGate IPSec gateway:

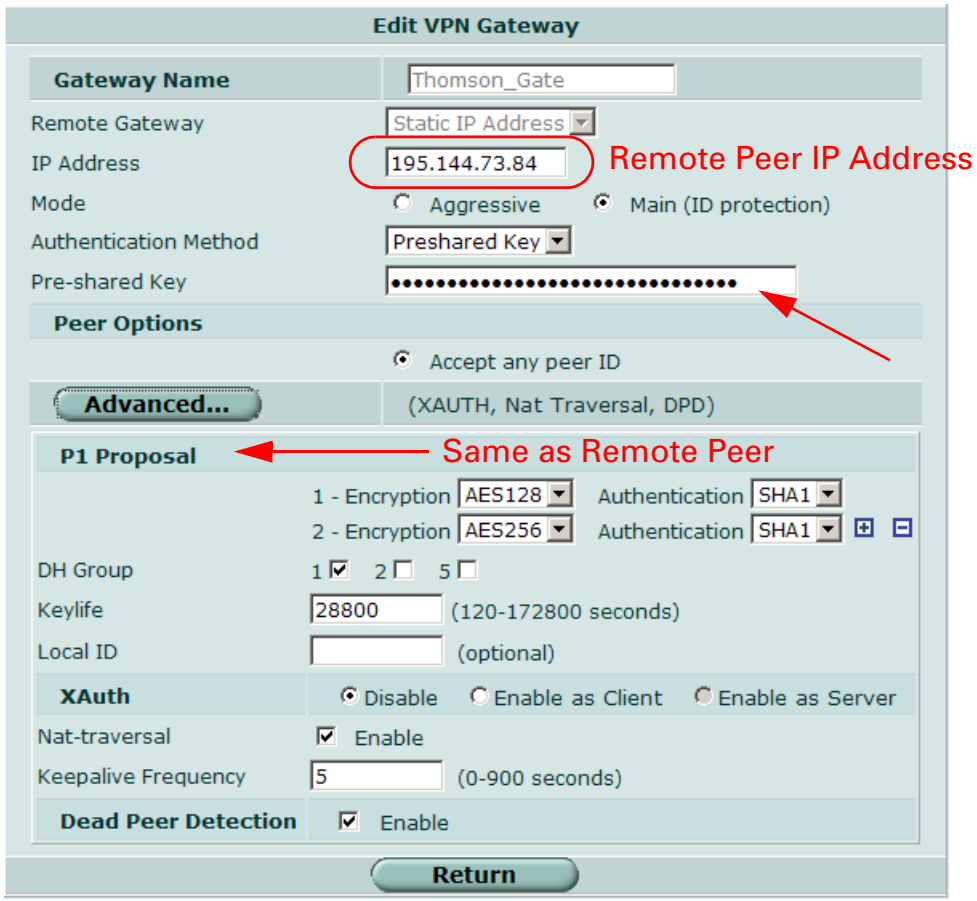
1 Define you internal and WAN interfaces (System -> Network)

Name	IP	Netmask	Access	Status	
internal	10.1.255.254	255.255.0.0	HTTPS,PING,TELNET		
dmz1			PING		
dmz2	10.10.10.254	255.255.255.0	PING		
wan1	83.206.62.65	255.255.255.248	HTTPS,PING,TELNET		
wan2	192.168.1.254	255.255.255.0	HTTPS,PING		

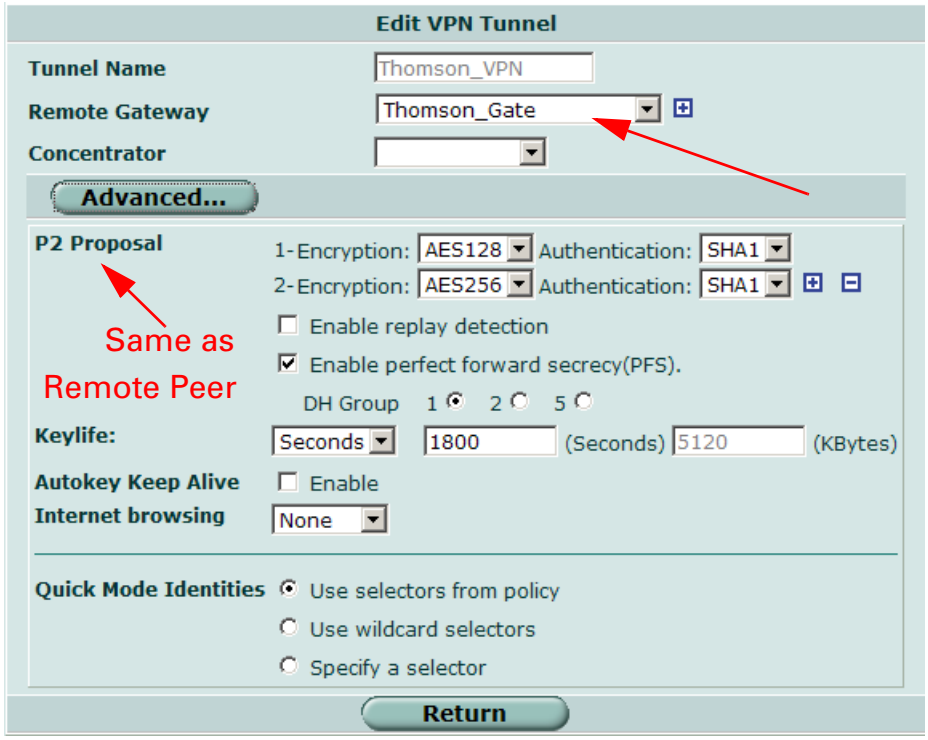
Via PPPoE, DHCP or manually:



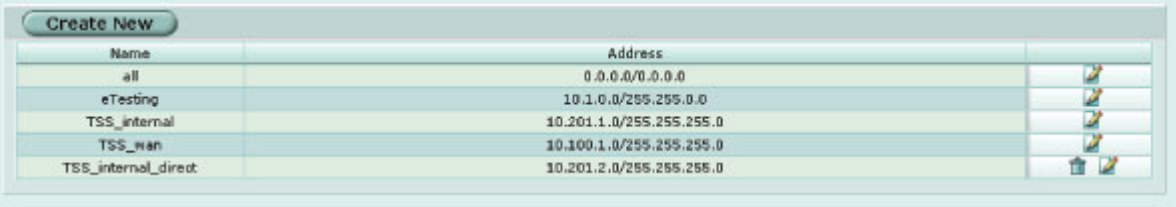
2 Create the VPN access - Phase1 (VPN -> IPSec -> Advanced):



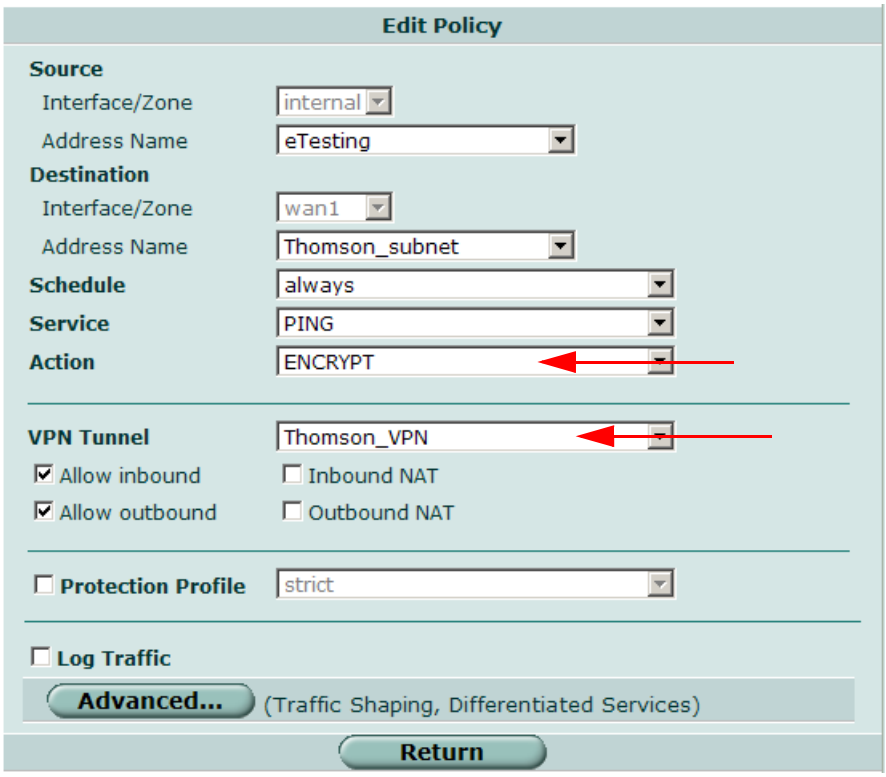
3 Create the VPN access - Phase2 (VPN -> IPSec -> Phase 2 -> Advanced):



4 Create the firewall rule: 1.Network/Address declaration (Firewall -> Address)

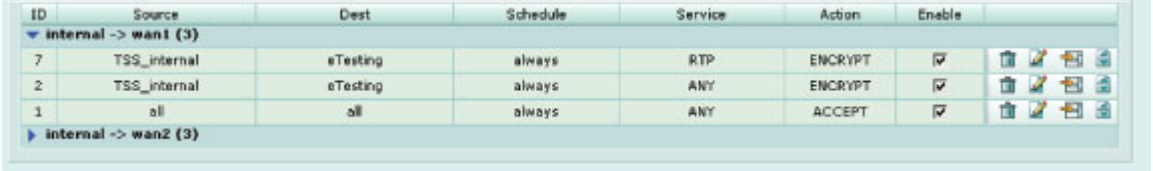


5 Create the firewall rule: 2.Rule declaration (Firewall -> Policy)



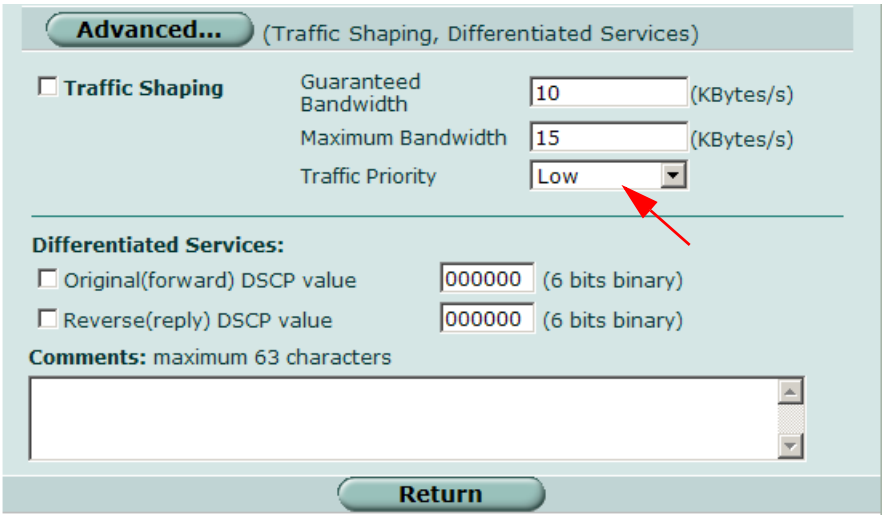
6 Create the firewall rule: 3.RTP Service declaration (Firewall -> Policy) = optional

7 Create the firewall rule: 4. AllAll_AnyAny Rule insertion (Firewall -> Policy)

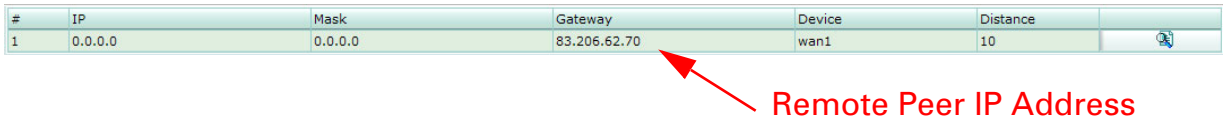


Optionally enable traffic shaping.

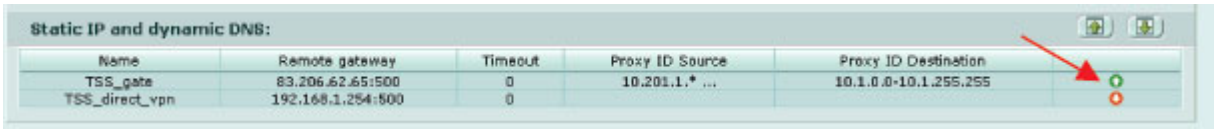
The screen shot shows Traffic Shaping for ANY rule (which is rule 2 in the screen shot above):



8 Static route (router -> Static):



9 VPN monitoring (VPN -> IPSec -> Monitor):



5.2 SpeedTouch™ Install Wizard Configuration Procedure

5.2.1 Main Configuration Steps

Dedicated templates

The introduction of the Fortinet IPSec gateway in the network requires the use of specific configuration templates. You can find these templates on the SpeedTouch™ Configuration CD or on the SpeedTouch™ web site.

The main configuration steps are almost identical as described in "3.2 SpeedTouch™ Install Wizard Configuration Procedure" on page 11.

Finding the correct templates

When you have the SpeedTouch™ installation CD, the templates are visible in the **Service Provider** window when you run the SpeedTouch™ Install Wizard.

In case you do not have the SpeedTouch™ installation CD, you can find the templates on the SpeedTouch™ web site at the following location:

- http://www.speedtouch.com/software/STeth/R610/Templates/AppNote_OmniPCX/ST620VPN2fortinet_ppp_adv.tpl
- http://www.speedtouch.com/software/STeth/R610/Templates/AppNote_OmniPCX/ST620VPN2fortnet_ipoa_adv.tpl

Using the templates

The templates will guide you through the configuration steps as described in "3.2 SpeedTouch™ Install Wizard Configuration Procedure" on page 11 and following.

5.3 Specific SpeedTouch™ settings for FortiGate

5.3.1 IPSec security descriptors

What are the specific settings for the Fortinet IPSec gateway?

The Fortinet IPSec gateway uses the key length when using AES in the Security Descriptors. These specific settings are included in the security descriptors of the SpeedTouch™ templates for the Fortinet connection.

Advanced VPN Gateway window

The screen shot shows the Phase 1 security descriptors you can use for connecting to the Fortinet IPSec gateway.

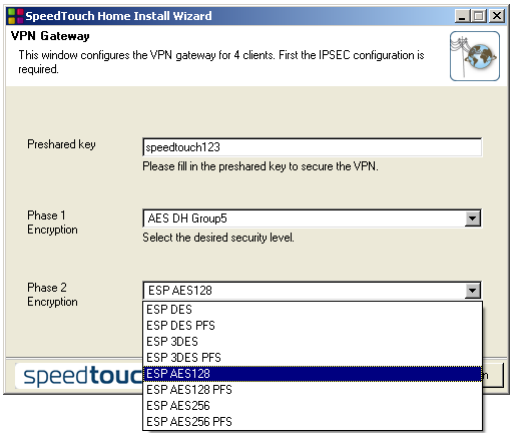


Figure 33: Advanced VPN Gateway window

Note that for AES the key length is explicitly included in the security descriptor. This is required by the Fortinet FortiGate.

5.3.2 Peer options for Dead Peer Detection

Don't worry

For the connection to the Fortinet IPSec Security gateway, some peer options have to be set in the SpeedTouch™. These settings are automatically set by the SpeedTouch™ Install Wizard when you use the provided templates. So, you don't have to worry about these settings.

To verify the peer options on the SpeedTouch™ web interface, browse to:

Expert mode -> VPN -> Advanced -> Peer -> Options.

APPENDIX A OXO WIZARDS

OXO configuration procedure

The OXO can be configured by means of a set of configuration wizards. The OXO configuration procedure is not explained in detail. Please use the product's documentation for this.

Use of the internal wizard of the OXO:

- Connection Wizard: to make the pre-configuration
- VPN Tunnel Wizard: to apply the VPN settings

OXO internal wizard selection window

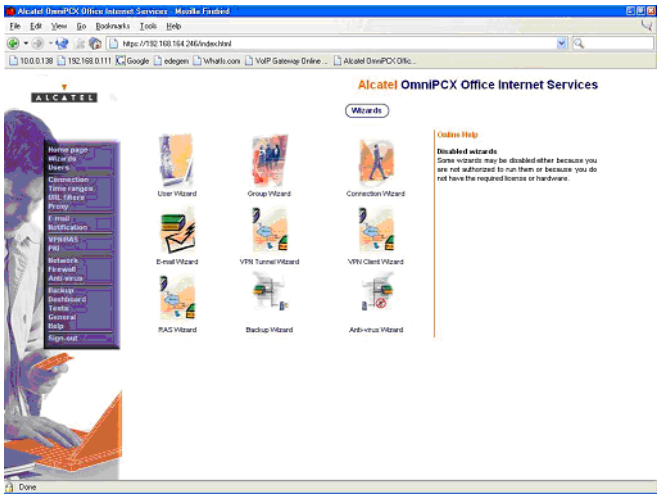


Figure 1: OXO Web Wizard

APPENDIX B OXO VPN CONFIGURATION

Check or change the VPN settings on the OXO

By default the OXO has some pre-configured profiles to configure VPN settings. These can be used as a basis for the configuration described in this document. Modifications to these profiles can easily be made via the web interface:

1. Use the VPN connection Wizard to create the peer connection
   - Use **High Security** or Standard Security as pre-defined security parameters profile for the connection.
   - VPN/RAS – define remote access
2. Click on **Tunnel Name > connection name**
3. Use Security Profile Management to check the VPN parameters: **High Security.**

OXO Security Profile Management window

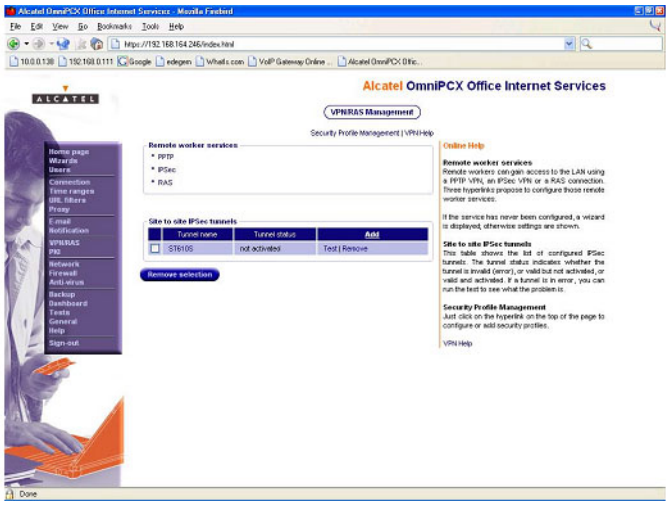


Figure 2: Security Profile Management

OXO Security Profile Selection window

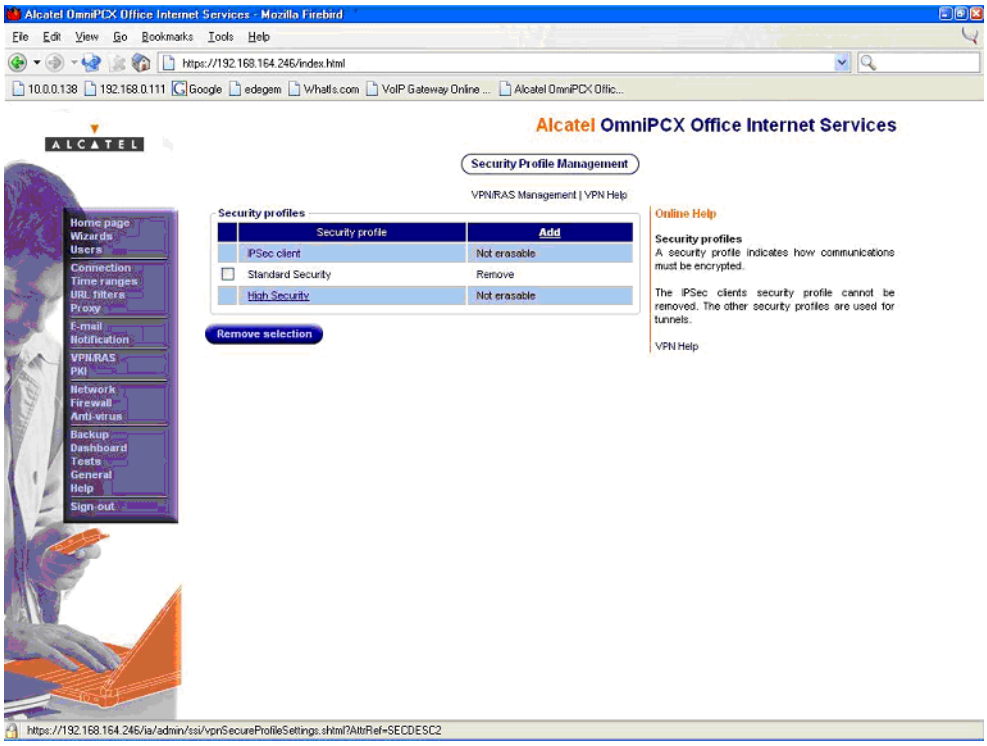


Figure 3: Security Profile Selection

OXO High or Standard Security Profile window

The three tab labels in this window specify all the parameters of the High Security or Standard Security profile. The three tab labels are:

- Identification: the profile name
- ISAKMP SA: Phase 1 settings
- IPSec SA: Phase 2 settings

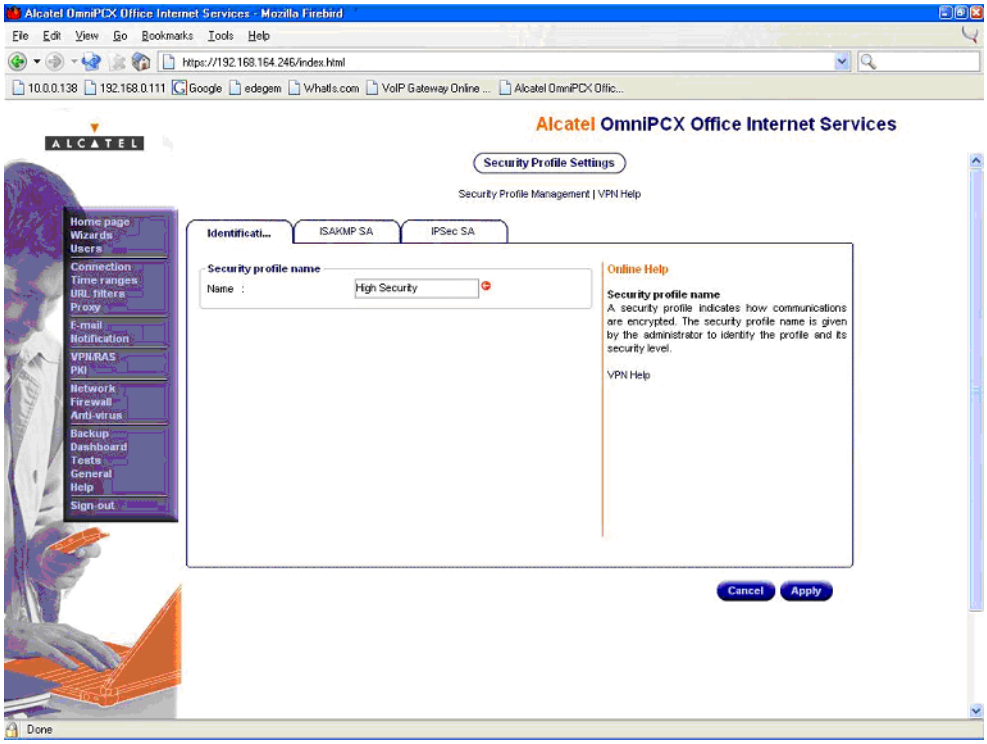


Figure 4: High Security Profile settings

High or Standard Security profile: ISAKMP Security Association window

This window shows the High Security profile settings for the ISAKMP Security Association (Phase 1). It contains various proposals for encryption and authentication methods, ordered in order of preference.

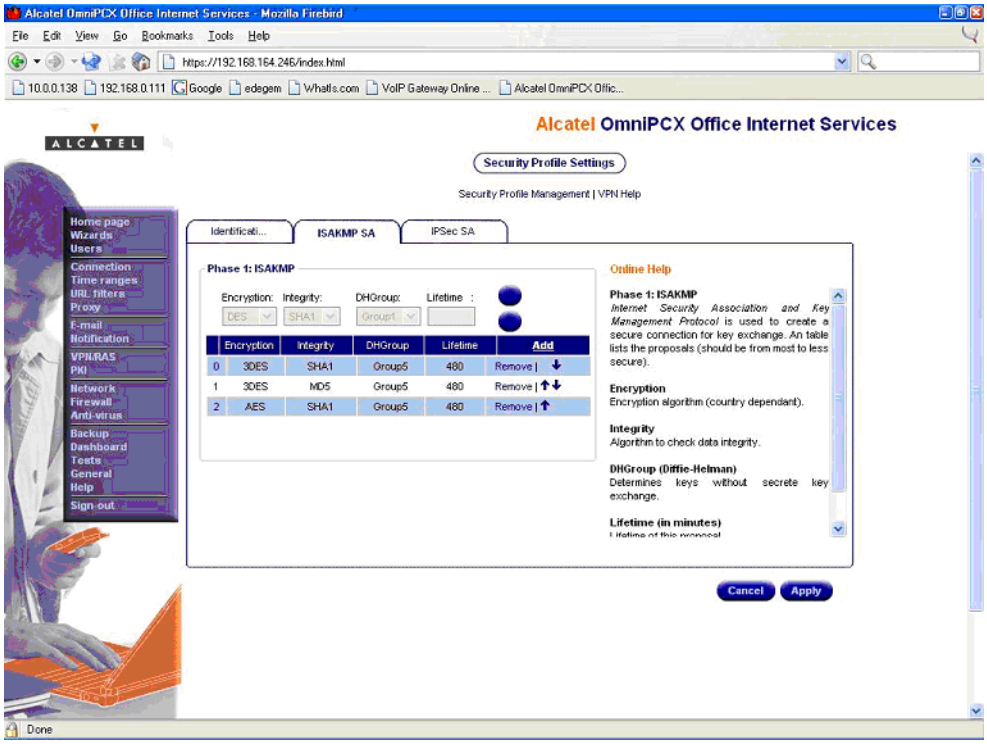


Figure 5: Phase 1 SA

High or Standard Security profile: IPSec Security Association window

This window shows the High Security or Standard Security profile settings for the IPSec Security Association (Phase 2). It contains various proposals for encryption and authentication methods, ordered in order of preference.

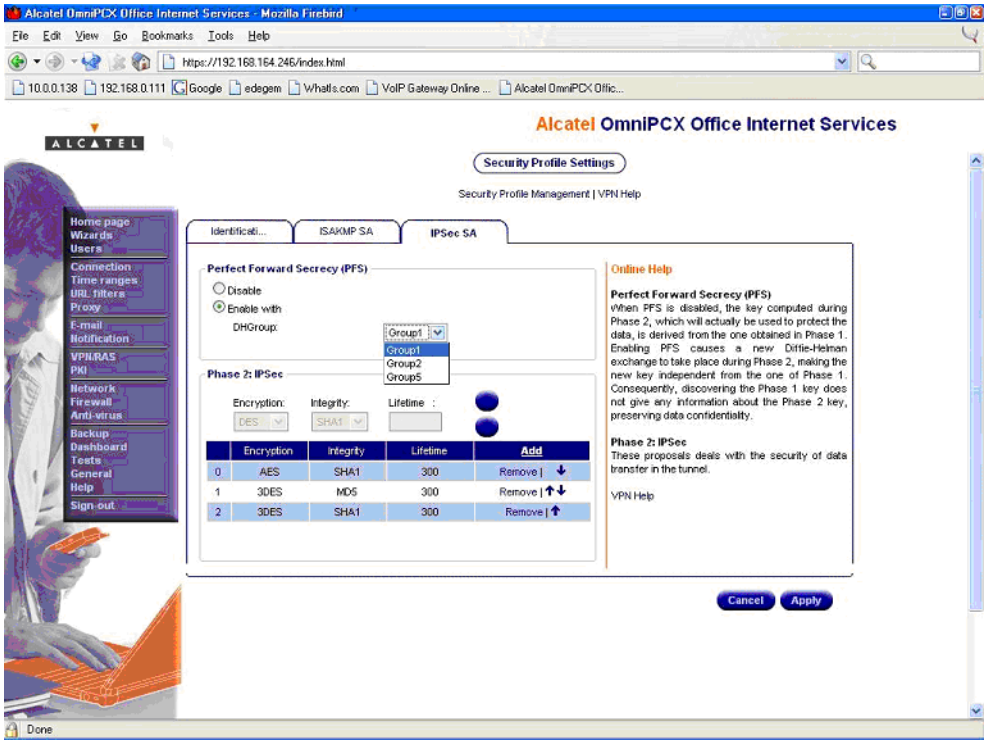


Figure 6: Phase 2 IPSec SA

APPENDIX C PRE-DEFINED SECURITY PROFILES FOR OXO

Pre-defined security profiles

Two pre-defined security profiles are defined for the SpeedTouch™ and the OXO. Both are highly secure.

In the SpeedTouch™ these profiles are characterized by Security Descriptors. Each profile contains two Security Descriptors: one for Phase 1 (ISAKMP SA) and one for Phase 2 (IPSec SA).

Perfect Forward Secrecy is used in both profiles.

Security descriptors corresponding to OXO_StandardSecurity:

- For IPSec Phase 1:

```
{Administrator}=>:ipsec peer descriptor list
[IKE_OXO_DES_MD5] : DES MD5 MODP1024 Lifetime 480s
[IKE_OXO_DES_SHA1] : DES SHA1 MODP1024 Lifetime 480s
{Administrator}=>
```

- For IPSec Phase 2:

```
{Administrator}=>:ipsec connection descriptor list
[ESP_OXO_DES_MD5] : DES HMAC-MD5 PFS Lifetime 300s Tunnel Mode
[ESP_OXO_DES_SHA1] : DES HMAC-SHA1 PFS Lifetime 300s Tunnel Mode
{Administrator}=>
```

Security descriptors corresponding to OXO_HighSecurity:

- For IPSec Phase 1:

```
{Administrator}=>:ipsec peer descriptor list
[IKE_OXO_AES_SHA1] : AES SHA1 MODP1536 Lifetime 480s
[IKE_OXO_3DES_MD5] : 3DES MD5 MODP1536 Lifetime 480s
[IKE_OXO_3DES_SHA1] : 3DES SHA1 MODP1536 Lifetime 480s
{Administrator}=>
```

- For IPSec Phase 2:

```
{Administrator}=>:ipsec connection descriptor list
[ESP_OXO_AES_SHA1] : AES HMAC-SHA1 PFS Lifetime 300s Tunnel Mode
[ESP_OXO_3DES_MD5] : 3DES HMAC-MD5 PFS Lifetime 300s Tunnel Mode
[ESP_OXO_3DES_SHA1] : 3DES HMAC-SHA1 PFS Lifetime 300s Tunnel Mode
{Administrator}=>
```

Figure 7: Advanced Phase 2

APPENDIX D DEBUG INFORMATION ADVANCED

Via web interface

See IPSec Application Note.

Via CLI

Telnet to the modem (default) cmd prompt: >telnet 192.168.1.254

Username/password

```
#ipsec sadb

#ipsec debug traceconfig detail high
<ctrl-q> to start Debug Information / trace
<ctrl-s> to stop the debug function
```

Visit us at:

www.speedtouch.com

Acknowledgements

All Colleagues for sharing their knowledge.

Coordinates

THOMSON Telecom

Prins Boudewijnlaan 47
B-2650 Edegem
Belgium

E-mail: documentation.speedtouch@thomson.net

speedtouch™

Copyright

A THOMSON BRAND