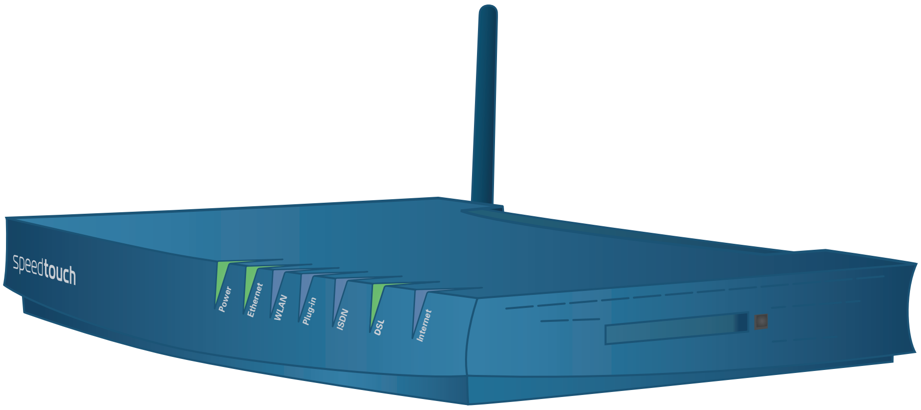
speedtouch™

SpeedTouch™608(WL)/620

(Wireless) Business DSL Router

IPSec Quick Start Guide



SpeedTouch™608WL and
SpeedTouch™620 only

A THOMSON BRAND

THOMSON

SpeedTouch™

608(WL)/620

IPSec Quick Start Guide

speedtouch™

Copyright

Thomson Telecom Belgium
Prins Boudewijnlaan, 47
B-2650 Edegem
Belgium

www.speedtouch.com

Trademarks

The following trademarks are used in this document:

- SpeedTouch™ is a trademark of THOMSON.
- Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.
- Ethernet™ is a trademark of Xerox Corporation.
- Wi-Fi® and the Wi-Fi logo are registered trademarks of the Wi-Fi Alliance. "Wi-Fi CERTIFIED", "Wi-Fi ZONE", "Wi-Fi Alliance", their respective logos and "Wi-Fi Protected Access" are trademarks of the Wi-Fi Alliance.
- UPnP™ is a certification mark of the UPnP™ Implementers Corporation.
- Microsoft®, MS-DOS®, Windows® and Windows NT® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Apple® and Mac OS® are registered trademarks of Apple Computer, Incorporated, registered in the United States and other countries.
- UNIX® is a registered trademark of UNIX System Laboratories, Incorporated.
- Adobe®, the Adobe logo, Acrobat and Acrobat Reader are trademarks or registered trademarks of Adobe Systems, Incorporated, registered in the United States and/or other countries.
- Netscape® and Netscape Navigator® are registered trademarks of Netscape Communications Corporation.

Other brands and product names may be trademarks or registered trademarks of their respective holders.

Document Information

Status: v1.0 (January 2006)
Reference: E-DOC-CTC-20051017-0173
Short Title: IPSec Quick Start Guide ST608(WL)/620 R5.4

Contents

About this IPSec Quick Start Guide

Abstract

The local Web pages of the SpeedTouch™ allow you to quickly configure the most common VPN scenarios:

- LAN-to-LAN connection
- VPN Client configuration
- VPN Server configuration

This document describes how to set up these basic VPN configurations.

For each scenario, the typical network environment is shown and the corresponding SpeedTouch™ configuration procedure is described.

In-depth information about the SpeedTouch™ IPSec configuration parameters and advanced VPN configurations can be found in the SpeedTouch™ IPSec Configuration Guide.

In some SpeedTouch™ products, the IPsec VPN features are bundled in an optional VPN software module. An optional VPN module is activated with a VPN software activation key. By default, this key is not installed. If you want to use the SpeedTouch™ VPN features, and the VPN software module is not activated on your SpeedTouch™, please contact your local dealer. Activating the VPN software module is described in the SpeedTouch™ Operator's Guide.

Applicability

This document applies to the following SpeedTouch™ products:

- The SpeedTouch™608 Business DSL Routers Release R5.3.0 and higher.
- The SpeedTouch™620 Business DSL Routers Release R5.3.0 and higher.

Used Symbols

The following symbols are used in this IPSec Quick Start Guide:

A ***note*** provides additional information about a topic.

A ***tip*** provides an alternative method or shortcut to perform an action.

A ***caution*** warns you about potential problems or specific precautions that need to be taken.

Terminology

Generally, the SpeedTouch™608 or SpeedTouch™620 will be referred to as SpeedTouch™ in this IPSec Quick Start Guide.

Documentation and software updates

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

For suggestions regarding this document, please contact documentation.speedtouch@thomson.net.

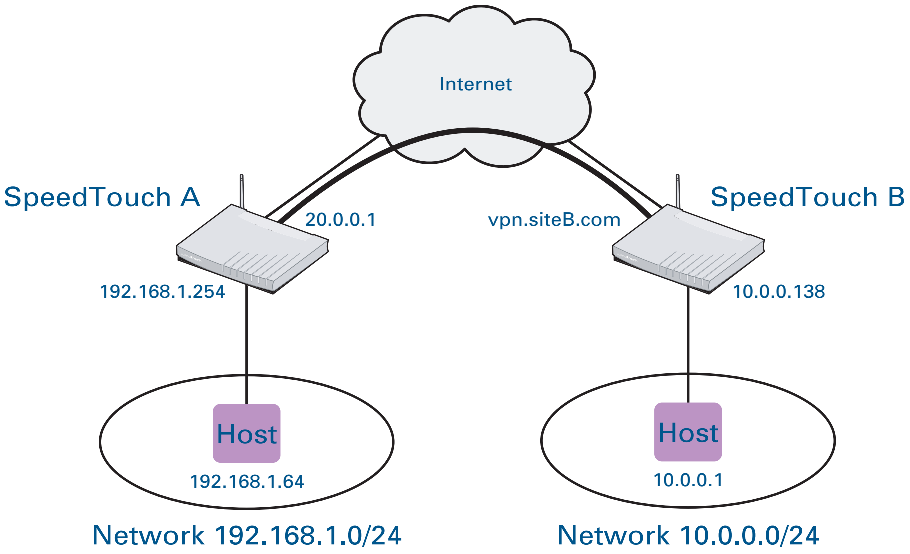
For more information on THOMSON's latest technological innovations, documents and software releases, visit us at:

www.speedtouch.com

1 LAN-to-LAN application

Reference network

A simple LAN-to-LAN network configuration is shown here.



The figure shows two LAN networks connected via a SpeedTouch™ to the public Internet. This chapter describes how to set up an IPSec VPN tunnel between Site A and Site B, using the respective SpeedTouch™ devices as the IPSec Security Gateway. A typical LAN-to-LAN connection is a symmetrical configuration. The IPSec tunnels can be initiated from both ends, and no remote configuration of network equipment is performed. In this example however, a slightly different approach is taken, in order to highlight a specific feature of the SpeedTouch™. When it is not required to set up VPN tunnels initiated from Site B, the SpeedTouch™ can be configured in such a way that remote sites can connect to Site B without the need to modify the SpeedTouch™ configuration at Site B.This situation may be encountered in a network where site B is a central node to which various satellite offices set up a VPN connection.

LAN IP addressing

In each LAN network, the IP addresses of the terminals are distributed by the built-in DHCP server of the SpeedTouch™. At Site A the default private network settings of the SpeedTouch™ are used (network 192.168.1.0/24). At Site B, the private network is the subnet 10.0.0.0/24.

Internet connection of Site A

Internet access at Site A is assumed to use a dynamic public IP address, attributed by the Internet Service Provider. As a consequence, the IP address shown in the figure above (20.0.0.1) changes each time when the Internet connection is activated. The IP address of Site A is to be considered as a variable.

Internet connection of Site B

For Site B, assume that the domain name (vpn.siteB.com) is resolvable by a DNS server on the public Internet. In this case, the public IP address attributed to site B is not relevant for the VPN configuration that we will construct.

IPSec parameters

The VPN connection between Site A and Site B relies on the IPSec protocol. In order to successfully complete the IPSec negotiations, a number of IPSec parameters need to be configured compliantly at both peers:

- pre-shared secret
- local and remote ID
- IKE exchange mode
- IKE Security Descriptor
- IPSec Security Descriptor
- local and remote network (in LAN-to-LAN application)

In this section

1.1 Configuring SpeedTouch A

VPN context

In this example, the VPN connection can only be initiated by Site A and is used for communication with hosts in the private network of Site B. This network context is encountered for example when a user at Site A is granted secure access to some file server at Site B. In addition, the DSL line of site A is used for Internet traffic. This traffic is not routed via the secure VPN tunnel, but is locally routed to the Internet Service Provider, which is called split-tunnelling.

In general, the default route of the SpeedTouch™ is the Internet connection. In our example, the VPN connection will add a route towards the secure tunnel for the communication with Site B only (to network 10.0.0.0/24). This traffic policy results in split tunnelling.

In our configuration example the VPN connection is secured in the following way:

- pre-shared key authentication method
- IKE negotiations in main mode
- AES as encryption algorithm
- SHA-1 as hashing function for message authentication
- use of Perfect Forward Secrecy for re-keying.

Configuration procedure outline

Perform the following steps to configure SpeedTouch A:

Step	Action	Page
1	"1.1.1 Defining the remote gateway parameters"	10
2	"1.1.2 Defining a new connection to the remote gateway"	13

1.1.1 Defining the remote gateway parameters

Introduction

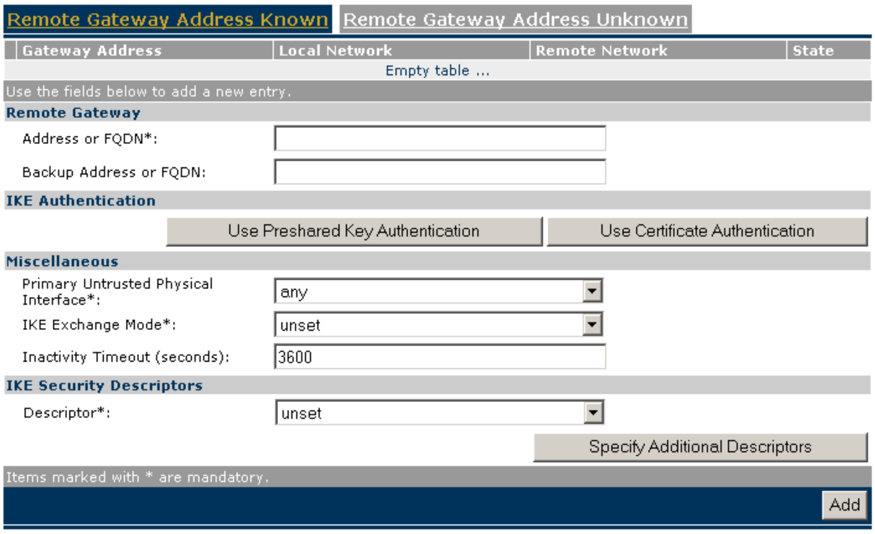
The following procedure describes how the remote gateway parameters are set for the LAN-to-LAN application. The remote gateway parameters define the remote peer of the VPN connection and the IKE (phase 1) negotiation characteristics.

Procedure

Proceed as follows:

1. In **Expert mode**, select **VPN > LAN to LAN > Remote Gateway Address Known**

   The following page is shown:

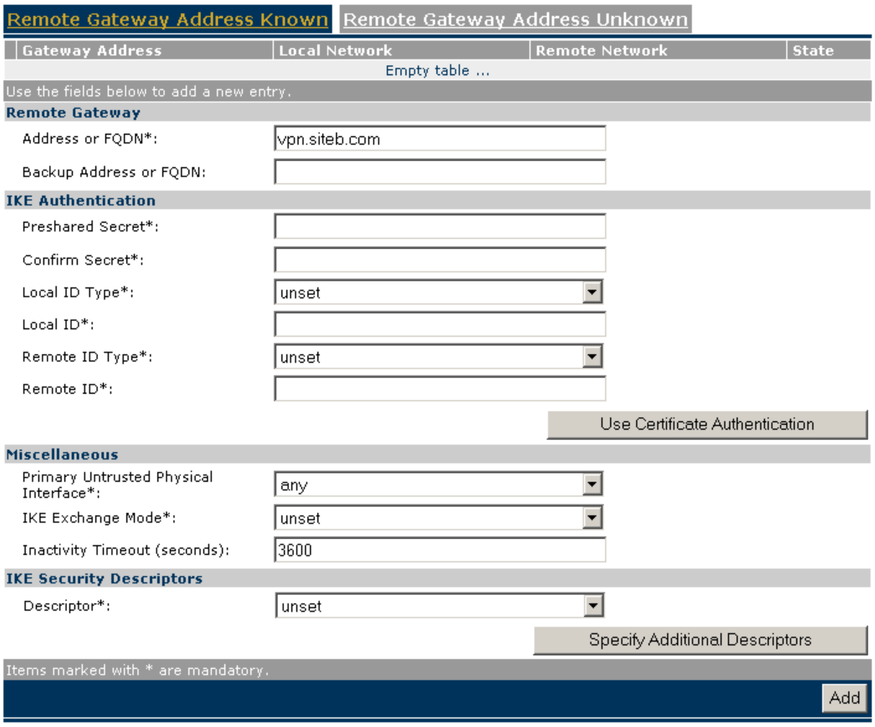

Remote Gateway Address Known
Remote Gateway Address Unknown
Gateway Address
Local Network
Remote Network
State
Empty table ...
Use the fields below to add a new entry.
Remote Gateway
IKE Authentication
Use Preshared Key Authentication
Use Certificate Authentication
Miscellaneous
IKE Security Descriptors
Specify Additional Descriptors
Add

Address or FQDN*:
Backup Address or FQDN:
Primary Untrusted Physical Interface*: any
IKE Exchange Mode*: unset
Inactivity Timeout (seconds): 3600
Descriptor*: unset
Items marked with * are mandatory.

2. Fill out the network location of the Remote Gateway in the **Address or FQDN** field. Use the domain name of site B. In our example: **vpn.siteB.com**.

   Leave the **Backup Address or FQDN** field open.

3 Select **Use Preshared Key Authentication**. The configuration page is updated and looks like this:


Remote Gateway Address Known
Remote Gateway Address Unknown
Use Certificate Authentication
Specify Additional Descriptors
Add

Gateway Address	Local Network	Remote Network	State
Empty table ...			

Use the fields below to add a new entry.

Remote Gateway

Address or FQDN*: vpn.siteb.com
Backup Address or FQDN:

IKE Authentication

Preshared Secret*:
Confirm Secret*:
Local ID Type*: unset
Local ID*:
Remote ID Type*: unset
Remote ID*:

Miscellaneous

Primary Untrusted Physical Interface*: any
IKE Exchange Mode*: unset
Inactivity Timeout (seconds): 3600

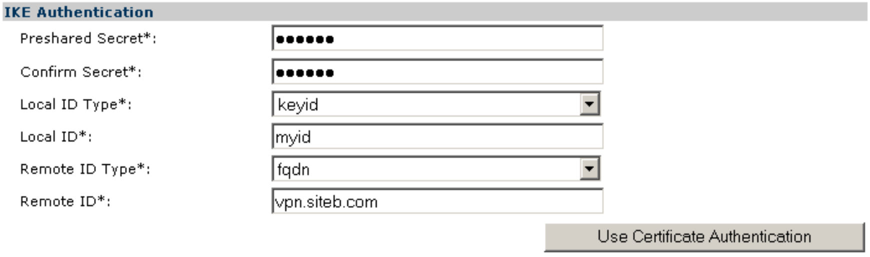
IKE Security Descriptors

Descriptor*: unset

Items marked with * are mandatory.

4 Fill out the IKE Authentication parameters as follows:

- **Pre-shared secret**: a string to be used as a secret password for the VPN connection. This secret needs to be identically configured at site A and site B.
- **Confirm Secret**: Re-type the secret to confirm your input (the secret is not shown in readable format on the screen).
- **Local ID Type**: Select **keyid**.
- **Local ID**: Type a text string, such as **myid**. This string identifies SpeedTouch A during the IKE negotiations.
- **Remote ID Type**: Select **fqdn**.
- **Remote ID**: Type the domain name of site B: **vpn.siteb.com**. This string identifies SpeedTouch B during the IKE negotiations.



IKE Authentication

Preshared Secret*: ●●●●●●
Confirm Secret*: ●●●●●●
Local ID Type*: keyid
Local ID*: myid
Remote ID Type*: fqdn
Remote ID*: vpn.siteb.com

5 Configure the **Miscellaneous** parameters in the following way:

- **Primary Untrusted Physical Interface**: Select your Internet interface from the list.
- **IKE Exchange Mode**: Select **main**.
- **Inactivity Timeout**: Use the default value of **3600 seconds**.

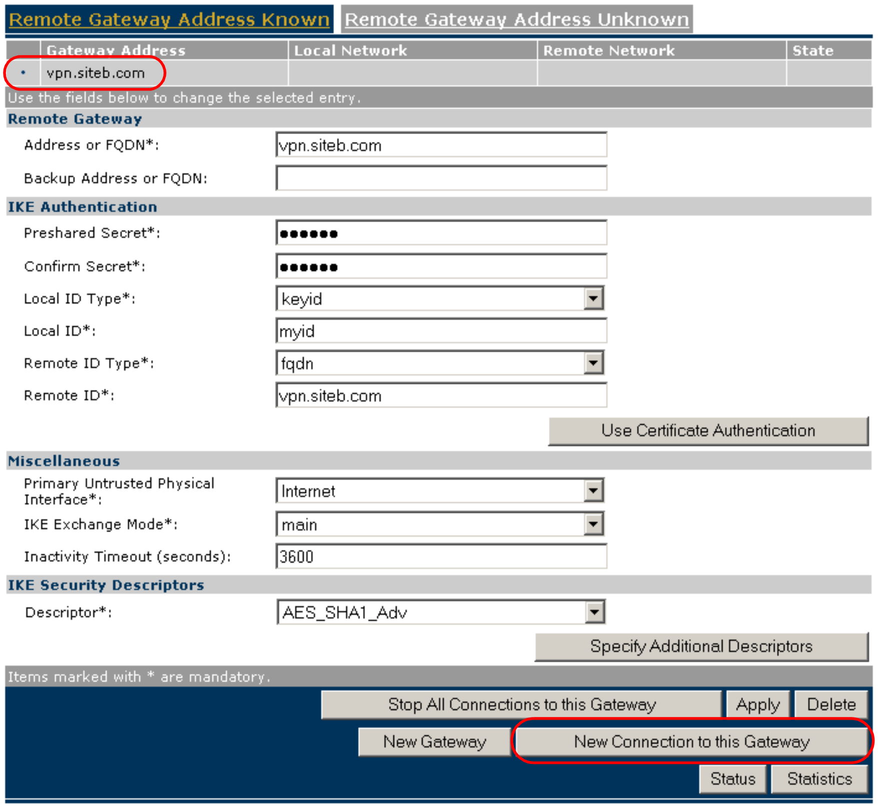
6 Select the **IKE Security Descriptor.**In our example the **AES_SHA1_Adv** descriptor is selected.

It is recommended to use **AES** as preferred encryption method. AES is more advanced, compared to DES or 3DES. It is faster for comparable key lengths, and provides better security.

AES is selected by the American government as the new encryption standard to replace DES/3DES.

7 Click **Add** to add the remote gateway settings to the configuration. The remote gateway is added to the table at the top of the configuration page, and now you can start defining a connection to this gateway.

The completed page now looks like this:


Remote Gateway Address Known
Remote Gateway Address Unknown

	Gateway Address	Local Network	Remote Network	State
•	vpn.siteb.com			

Use the fields below to change the selected entry.

Remote Gateway

Address or FQDN*:	vpn.siteb.com
Backup Address or FQDN:	

IKE Authentication

Preshared Secret*:	••••••
Confirm Secret*:	••••••
Local ID Type*:	keyid
Local ID*:	myid
Remote ID Type*:	fqdn
Remote ID*:	vpn.siteb.com

Use Certificate Authentication

Miscellaneous

Primary Untrusted Physical Interface*:	Internet
IKE Exchange Mode*:	main
Inactivity Timeout (seconds):	3600

IKE Security Descriptors

Descriptor*:	AES_SHA1_Adv

Items marked with * are mandatory.

Stop All Connections to this Gateway
Apply
Delete
New Gateway
New Connection to this Gateway
Status
Statistics

1.1.2 Defining a new connection to the remote gateway

Introduction

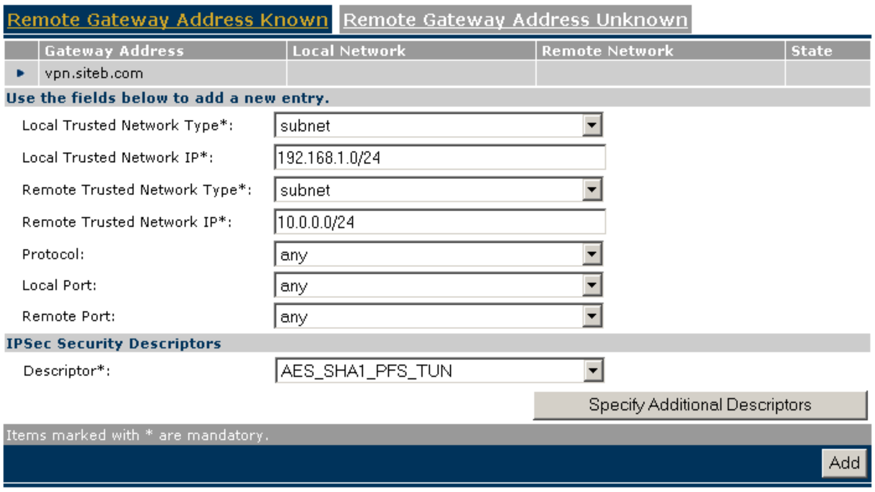
The following procedure describes how a connection to the remote gateway is defined. The connection parameters contain the traffic policy for the VPN connection and the IPSec security parameters.

Procedure

Proceed as follows:

1. Click **New Connection to this Gateway** to define a connection to site B.
2. Define the Connection parameters as explained below:
   - **Local Trusted Network Type**: select **subnet**
   - **Local Trusted Network IP**: type **192.168.1.0/24**
   - **Remote Trusted Network Type**: select **subnet**
   - **Remote Trusted Network IP**: type **10.0.0.0/24**
   - **Protocol**: use the default value **any**.
   - **Local Port**: use the default value **any**.
   - **Remote Port**: use the default value **any**.
   - **IPSec Security Descriptor**: select **AES_SHA1_PFS_TUN**.

   The completed page now looks like this:


Remote Gateway Address Known
Remote Gateway Address Unknown
Specify Additional Descriptors
Add

Gateway Address	Local Network	Remote Network	State
vpn.siteb.com			

Use the fields below to add a new entry.

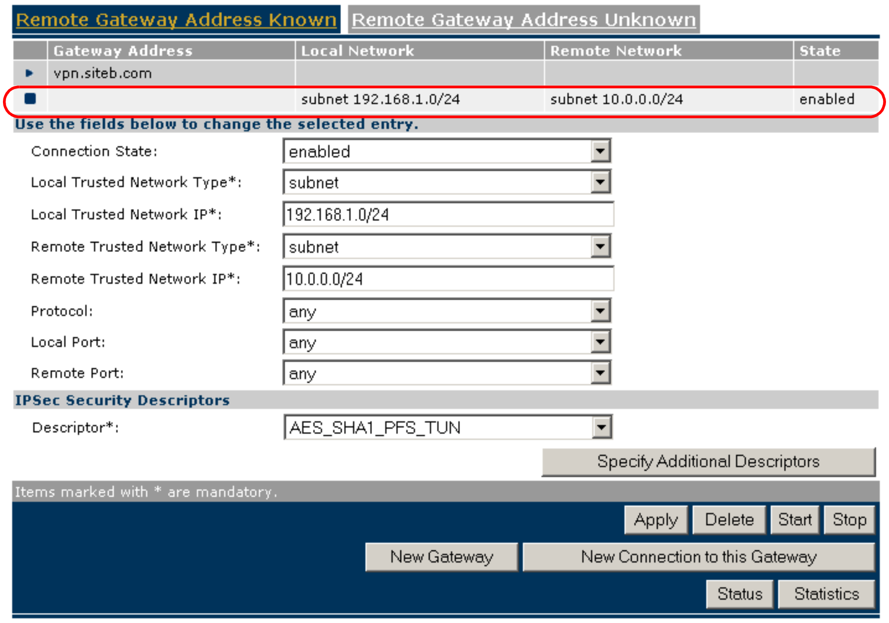
Local Trusted Network Type*: subnet
Local Trusted Network IP*: 192.168.1.0/24
Remote Trusted Network Type*: subnet
Remote Trusted Network IP*: 10.0.0.0/24
Protocol: any
Local Port: any
Remote Port: any

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Items marked with * are mandatory.

3 Click **Add** to add the connection to the configuration. The connection is shown in the table at the top of the configuration page, ready to be started.



	Gateway Address	Local Network	Remote Network	State
▸	vpn.siteb.com			
■		subnet 192.168.1.0/24	subnet 10.0.0.0/24	enabled

Use the fields below to change the selected entry.

Connection State: enabled
Local Trusted Network Type*: subnet
Local Trusted Network IP*: 192.168.1.0/24
Remote Trusted Network Type*: subnet
Remote Trusted Network IP*: 10.0.0.0/24
Protocol: any
Local Port: any
Remote Port: any

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Items marked with * are mandatory.

Specify Additional Descriptors
Apply
Delete
Start
Stop
New Gateway
New Connection to this Gateway
Status
Statistics

4 Click **Save All** to save the SpeedTouch™ configuration.

This concludes the configuration of SpeedTouch A.

1.2 Configuring SpeedTouch B

VPN context

Site B in our example is always the responder in the IKE negotiations. Site B does not know a priori which remote Security Gateway will attempt to set up a VPN connection. SpeedTouch B is configured in such a way that a secure connection will be established with any Remote Gateway that meets the VPN settings, regardless its location in the public network.

Configuration procedure outline

Perform the following steps to configure SpeedTouch B:

Step	Action	Page
1	"1.2.1 Defining the remote gateway parameters"	16
2	"1.2.2 Defining a new connection to the remote gateway"	19

1.2.1 Defining the remote gateway parameters

Introduction

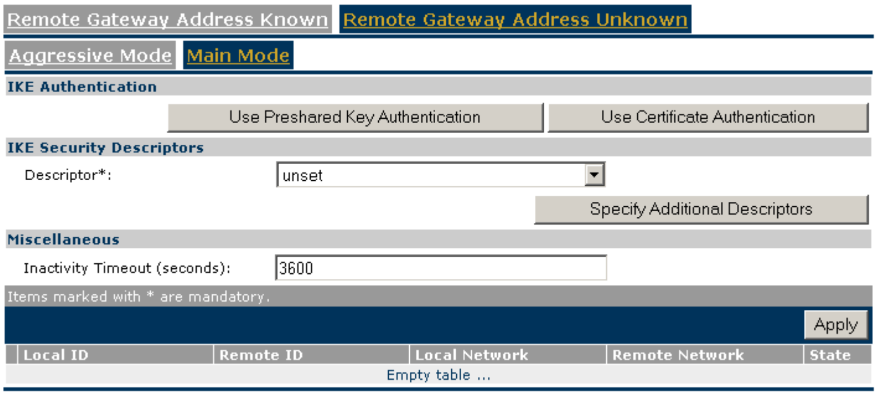
The following procedure describes how the remote gateway parameters are set in order to allow a VPN connection with SpeedTouch A.

Procedure

Proceed as follows:

1 In **Expert mode**, select **VPN > LAN to LAN > Remote Gateway Address Unknown > Main Mode**.

The following page is shown:


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
IKE Authentication
Use Preshared Key Authentication
Use Certificate Authentication
IKE Security Descriptors
Specify Additional Descriptors
Miscellaneous
Apply

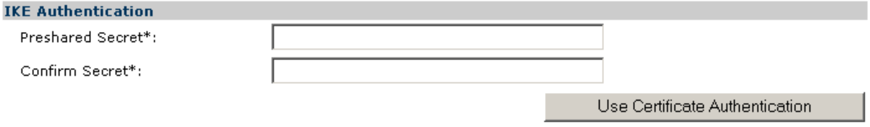
Descriptor*: unset

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

Local ID	Remote ID	Local Network	Remote Network	State
Empty table ...				

2 Select **Use Preshared key Authentication**. The configuration page is updated and looks like this:



Preshared Secret*:

Confirm Secret*:

3 Fill out the IKE Authentication parameters as follows:

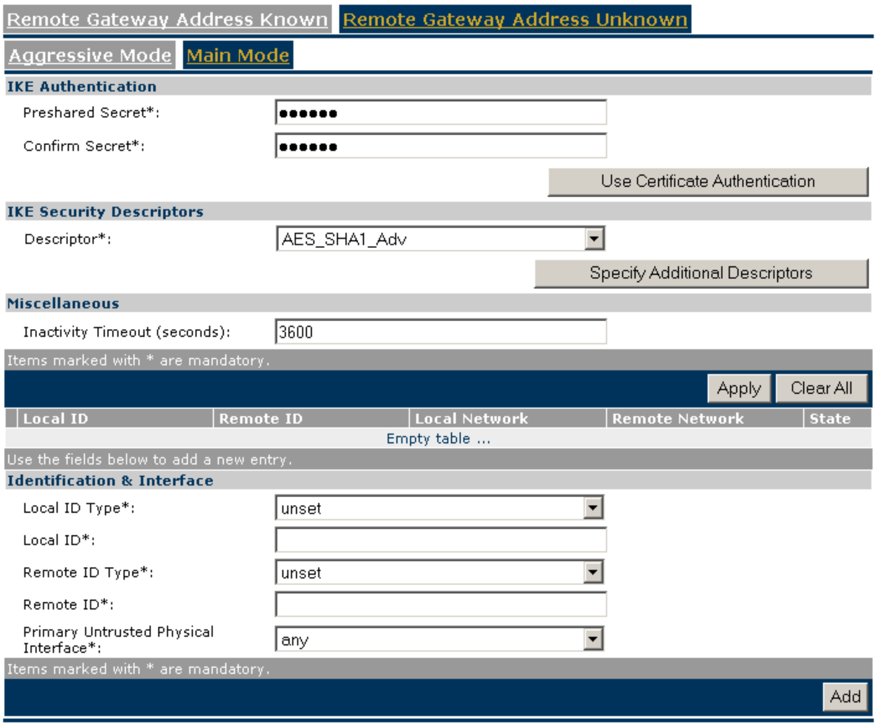
- **Pre-shared secret**: the same character string as configured in SpeedTouch A:
- **Confirm Secret**: Re-type the secret.

4 Fill out the **IKE Security Descriptor**. Select the same descriptor as configured in SpeedTouch A: **AES_SHA1_Adv**.

5 Configure the **Miscellaneous** parameter in the following way:

- **Inactivity Timeout**: Use the default value of **3600 seconds**.

6 Click **Apply**. The configuration page is modified as shown below.


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
IKE Authentication
Use Certificate Authentication
IKE Security Descriptors
Specify Additional Descriptors
Miscellaneous
Apply
Clear All
Identification & Interface
Add

Preshared Secret*: ●●●●●●
Confirm Secret*: ●●●●●●

Descriptor*: AES_SHA1_Adv

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

Local ID	Remote ID	Local Network	Remote Network	State
Empty table ...				

Use the fields below to add a new entry.

Local ID Type*: unset
Local ID*:
Remote ID Type*: unset
Remote ID*:
Primary Untrusted Physical Interface*: any

Items marked with * are mandatory.

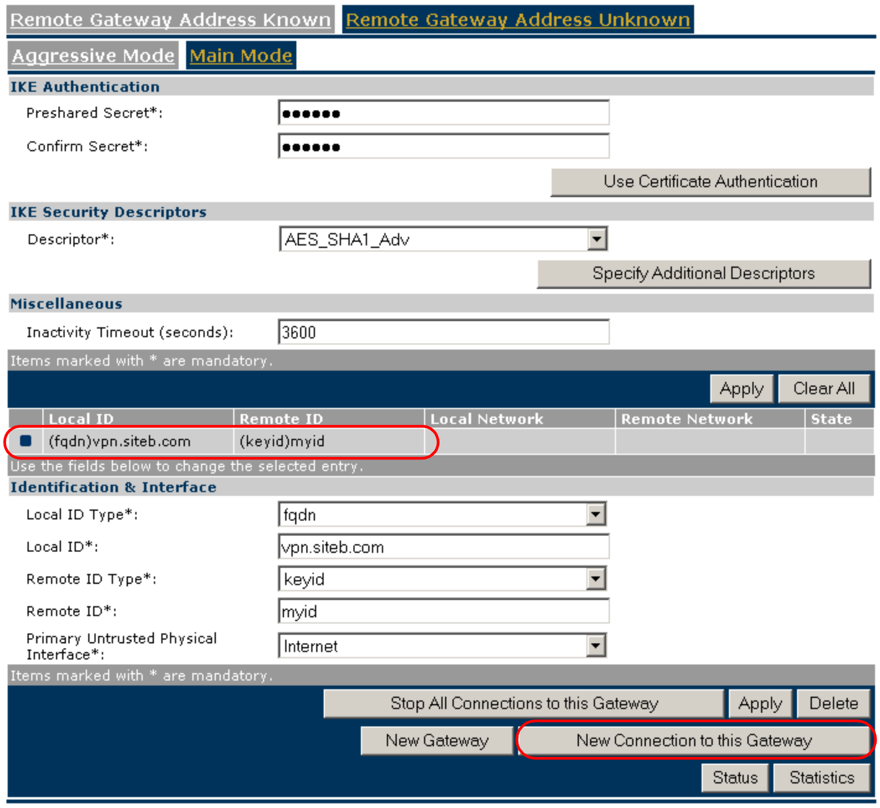
7 Configure the **Identification & Interface** parameters in the following way:

- **Local ID Type**: Select **fqdn**.
- **Local ID**: Type the domain name of site B: **vpn.siteb.com**.
- **Remote ID Type**: Select **keyid**.
- **Remote ID**: Type the keyid of site A: **myid.**
- **Primary Untrusted Physical Interface**: Select your Internet interface from the list.

The selection of a **Primary Untrusted Physical Interface** is relevant for incoming connections only. If you select **any**, VPN connections are accepted on all interfaces. This is relevant only in case your SpeedTouch™ is equipped with a backup interface.

8 Click **Add** to add the remote gateway settings to the configuration. The remote gateway is added to the table, and now you can start defining a connection to this gateway.

The completed page now looks like this:


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
Use Certificate Authentication
Specify Additional Descriptors
Apply
Clear All
Stop All Connections to this Gateway
Apply
Delete
New Gateway
New Connection to this Gateway
Status
Statistics

IKE Authentication

Preshared Secret*: ●●●●●●

Confirm Secret*: ●●●●●●

IKE Security Descriptors

Descriptor*: AES_SHA1_Adv

Miscellaneous

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

	Local ID	Remote ID	Local Network	Remote Network	State
■	(fqdn)vpn.siteb.com	(keyid)myid			

Use the fields below to change the selected entry.

Identification & Interface

Local ID Type*: fqdn

Local ID*: vpn.siteb.com

Remote ID Type*: keyid

Remote ID*: myid

Primary Untrusted Physical Interface*: Internet

Items marked with * are mandatory.

1.2.2 Defining a new connection to the remote gateway

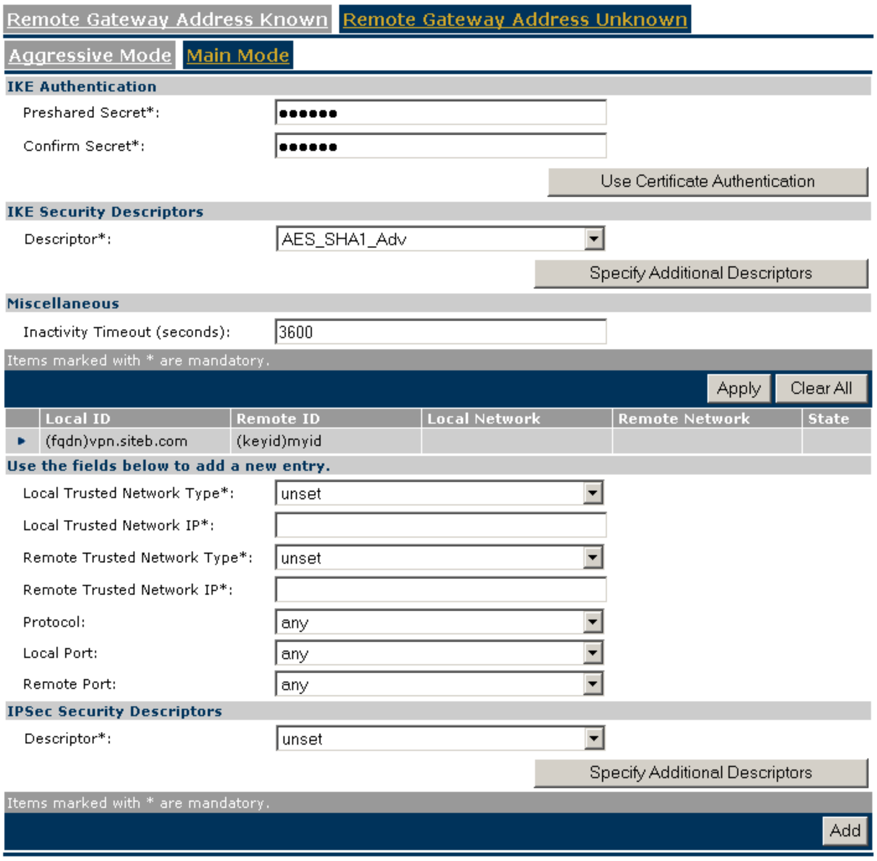
Introduction

The following procedure describes how a connection to the remote gateway is defined. The connection parameters contain the traffic policy for the VPN connection and the IPSec security parameters.

Procedure

Proceed as follows:

1 Click **New Connection to this Gateway** to define a connection to site A. The following page appears:


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
Use Certificate Authentication
Specify Additional Descriptors
Apply
Clear All
Specify Additional Descriptors
Add

IKE Authentication

Preshared Secret*: ●●●●●●

Confirm Secret*: ●●●●●●

IKE Security Descriptors

Descriptor*: AES_SHA1_Adv

Miscellaneous

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

	Local ID	Remote ID	Local Network	Remote Network	State
▸	(fqdn)vpn.siteb.com	(keyid)myid			

Use the fields below to add a new entry.

Local Trusted Network Type*: unset

Local Trusted Network IP*:

Remote Trusted Network Type*: unset

Remote Trusted Network IP*:

Protocol: any

Local Port: any

Remote Port: any

IPSec Security Descriptors

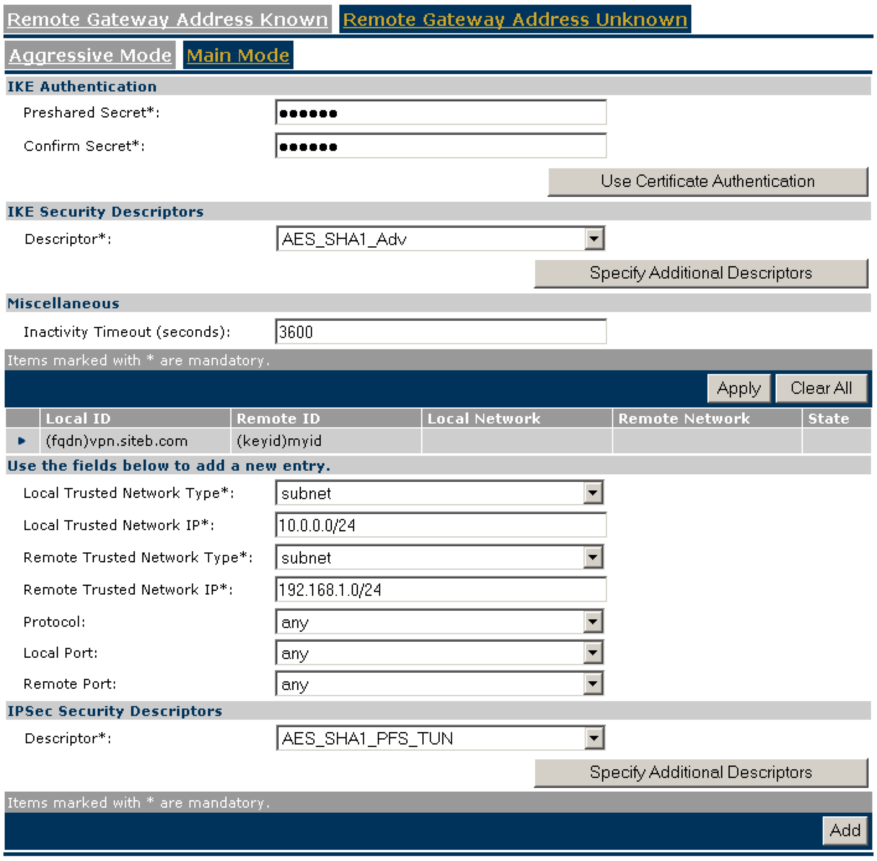
Descriptor*: unset

Items marked with * are mandatory.

2 Define the Connection parameters as explained below:

- **Local Trusted Network Type**: select **subnet**
- **Local Trusted Network IP**: type **10.0.0.0/24**
- **Remote Trusted Network Type**: select **subnet**
- **Remote Trusted Network IP**: type **192.168.1.0/24**
- **Protocol**: use the default value **any**.
- **Local Port**: use the default value **any**.
- **Remote Port**: use the default value **any**.
- **IPSec Security Descriptor**: select **AES_SHA1_PFS_TUN**.

The completely filled-out configuration page looks like this:


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
Use Certificate Authentication
Specify Additional Descriptors
Apply
Clear All
Specify Additional Descriptors
Add

IKE Authentication

Preshared Secret*: ••••••

Confirm Secret*: ••••••

IKE Security Descriptors

Descriptor*: AES_SHA1_Adv

Miscellaneous

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

	Local ID	Remote ID	Local Network	Remote Network	State
▸	(fqdn)vpn.siteb.com	(keyid)myid			

Use the fields below to add a new entry.

Local Trusted Network Type*: subnet

Local Trusted Network IP*: 10.0.0.0/24

Remote Trusted Network Type*: subnet

Remote Trusted Network IP*: 192.168.1.0/24

Protocol: any

Local Port: any

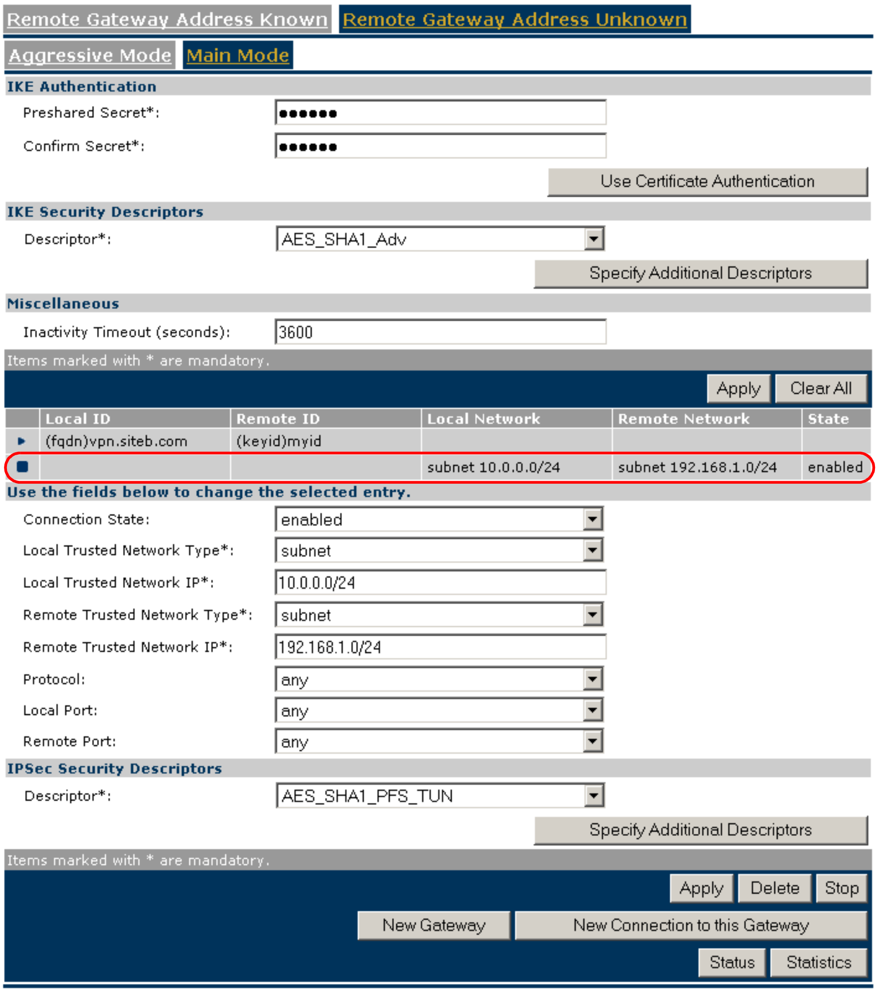
Remote Port: any

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Items marked with * are mandatory.

3 Click **Add** to add the connection to the configuration. The connection is shown in the table. The state of the connection is **enabled**, which means that a remote gateway can start negotiations to set up a VPN connection.


Remote Gateway Address Known
Remote Gateway Address Unknown
Aggressive Mode
Main Mode
Use Certificate Authentication
Specify Additional Descriptors
Apply
Clear All
Apply
Delete
Stop
New Gateway
New Connection to this Gateway
Status
Statistics

IKE Authentication

Preshared Secret*: ●●●●●●

Confirm Secret*: ●●●●●●

IKE Security Descriptors

Descriptor*: AES_SHA1_Adv

Miscellaneous

Inactivity Timeout (seconds): 3600

Items marked with * are mandatory.

	Local ID	Remote ID	Local Network	Remote Network	State
▸	(fqdn)vpn.siteb.com	(keyid)myid			
■			subnet 10.0.0.0/24	subnet 192.168.1.0/24	enabled

Use the fields below to change the selected entry.

Connection State: enabled

Local Trusted Network Type*: subnet

Local Trusted Network IP*: 10.0.0.0/24

Remote Trusted Network Type*: subnet

Remote Trusted Network IP*: 192.168.1.0/24

Protocol: any

Local Port: any

Remote Port: any

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Items marked with * are mandatory.

4 Click **Save All** to save the SpeedTouch™ configuration.

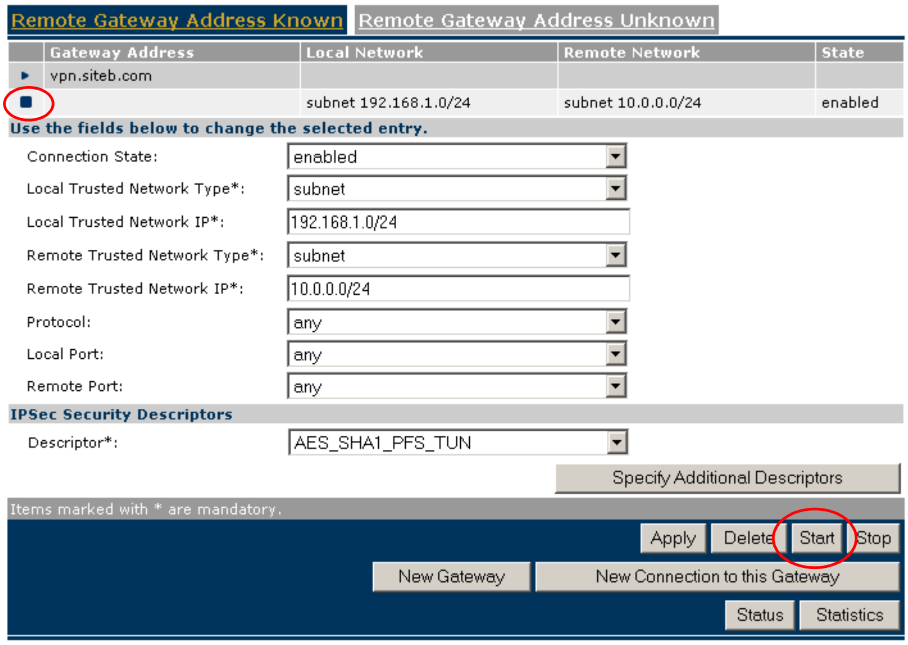
This concludes the configuration of SpeedTouch B.

1.3 Using the VPN connection

Start the VPN connection

The VPN connection is started from SpeedTouch A. In IPSec terms, SpeedTouch A is the initiator, SpeedTouch B the responder.

To start the VPN connection at SpeedTouch A, select the connection. Then click **Start**.



	Gateway Address	Local Network	Remote Network	State
▸	vpn.siteb.com			
■		subnet 192.168.1.0/24	subnet 10.0.0.0/24	enabled

Use the fields below to change the selected entry.

Connection State: enabled
Local Trusted Network Type*: subnet
Local Trusted Network IP*: 192.168.1.0/24
Remote Trusted Network Type*: subnet
Remote Trusted Network IP*: 10.0.0.0/24
Protocol: any
Local Port: any
Remote Port: any

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Items marked with * are mandatory.

Specify Additional Descriptors
Apply
Delete
Start
Stop
New Gateway
New Connection to this Gateway
Status
Statistics

Verify the VPN connection

Click **Status** to verify the status of the VPN connection.

Click **Statistics** to see how much traffic the VPN connection has transferred so far.

As soon as the VPN connection is active, you should be able to ping a computer located in the remote LAN segment. For example, the computer with IP address 192.168.1.64 is able to ping the computer with IP address 10.0.0.1, and vice versa.

Surfing through the VPN tunnel

One of the SpeedTouch™ features for easy Internet access is the so-called Web Browsing Interception, also referred to as Differentiated Services Detection (DSD). This feature monitors your HTTP traffic and alerts you when you want to browse to a location that is not reachable due to the fact that the connection to your Service Provider is not active. A SpeedTouch™ Web page appears that allows you to log in to your Service Provider.

When you configure an IPSec VPN connection, this feature has to be disabled in order to pass HTTP traffic through the VPN tunnel.

To verify that the Web Browsing Interception is disabled, proceed as follows:

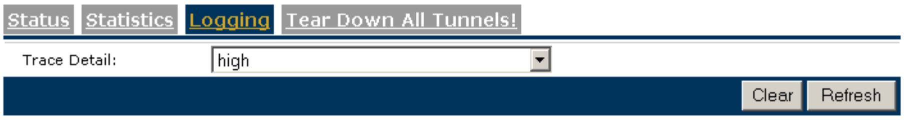
1. Browse to **Basic Mode > SpeedTouch > Configuration**.
2. Click **Configure**.
3. Make sure that under **System Configuration** the “**Web Browsing Interception**” check box is not selected.
4. If needed, clear the check box and click **Apply** to confirm the change.

If Web Browsing Interception is disabled, Web address based filtering is disabled as well. Keep this in mind if you use the Web based filtering tool for parental control.

Troubleshooting

If you encounter problems setting up the VPN connection, you can use the **Debug** pages to diagnose your problem. In addition to the **Status** and **Statistics** information, the **Debug** pages contain a **Logging** page where you can monitor the negotiation process. This page helps you to determine the phase where the negotiations fail and the reason why.

It is recommended to select the highest level of detail to diagnose problems.



Trace Detail: high

More information about the Debug pages is found in the IPSec Configuration Guide.

2 VPN client-server application

A typical teleworker scenario

As a reference configuration, a teleworker scenario is described here. Using an IPSec connection, a secure VPN connection is established between the teleworker and the corporate network of his employer. At both peers, a SpeedTouch™ is used for Internet access. This section describes how the SpeedTouch™ of the teleworker is configured as a VPN client Security Gateway, in order to get access to the remote corporate network. Furthermore, it is described how the SpeedTouch™ at the corporate peer is configured as a VPN server Security Gateway.

At the teleworker side

In general, the SpeedTouch™ is used for Internet access only. In the present application scenario it is shown how this configuration is enhanced to provide a secure access to a corporate network for teleworking.

In this teleworker scenario, it is assumed that a single residential user will connect to the corporate network via a secure VPN connection. His SpeedTouch™ needs to be configured as an IPSec VPN client. The SpeedTouch™ is the peer of the IPSec connection at the client side. No IPSec client software is required on the computer of the user.

When the teleworker dials in to the corporate VPN server, his SpeedTouch™ is integrated in the corporate network environment. A new private IP address is provided within the corporate network address range and for host name resolving the corporate DNS servers are used. These remote configuration parameters are transferred by the IKE Mode Config protocol from the VPN server to the VPN client.

As an additional level of security, optionally the IKE Extended Authentication protocol (XAuth) can be enabled. This means that the user has to provide a user name and password each time he dials in to the corporate network.

Other users in the network of the teleworker have no access to the VPN connection, but can still make use of the other services of the SpeedTouch™, such as Internet access.

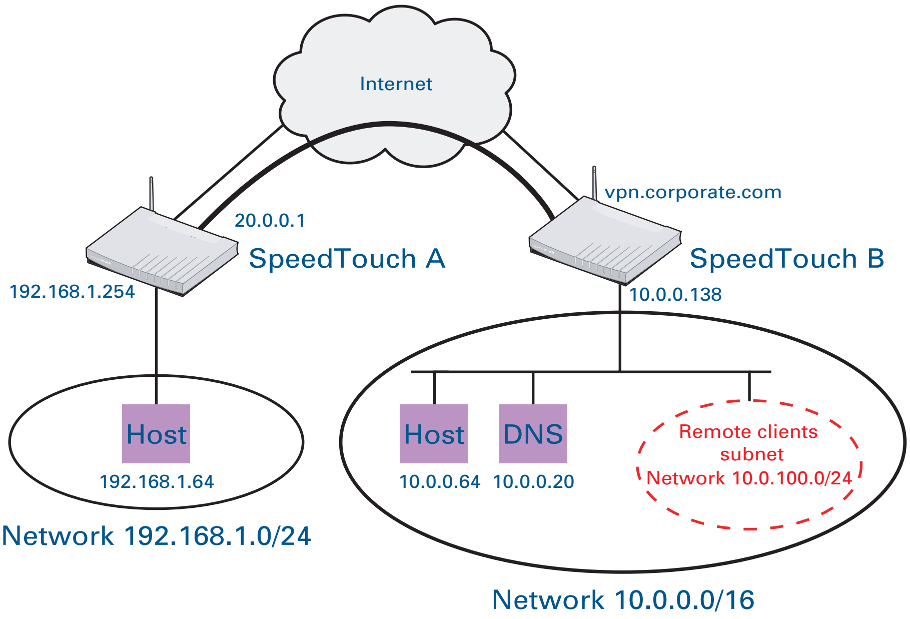
At the corporate side

The corporate network uses a SpeedTouch™ router for Internet access. In order to allow the secure connections with a number of teleworkers, this router has to be configured as a VPN server. In IPSec terms, it acts as the Security Gateway at the corporate peer. The SpeedTouch™ VPN server supports IKE Mode Config to provide an IP address and the location of the network servers to the remote VPN clients.

Optionally, the XAuth protocol can be enabled. In this case, a list of authorized users and their corresponding passwords is stored in the SpeedTouch™ VPN server. More information about the use of XAuth and the configuration of a list of authorized users is found in the SpeedTouch™ IPSec Configuration Guide.

Reference network

A simple VPN client-server network configuration is shown here.



The figure shows the teleworker's premises at the left hand side. The corporate network is shown at the right hand side. Both LAN networks are connected via a SpeedTouch™ to the public Internet.

LAN IP addressing

In each LAN network, the IP addresses of the terminals are distributed by the built-in DHCP server of the SpeedTouch™. The teleworker uses the default private network settings of the SpeedTouch™ (network 192.168.1.0/24). The corporate network uses the subnet 10.0.0.0/16. A dedicated address pool (subnet 10.0.100.0/24) is reserved for the remote VPN clients.

The corporate network furthermore contains a DNS server (IP address 10.0.0.20) that handles the host name resolving inside the private network.

The teleworker's Internet connection

It is assumed a dynamic public IP address is attributed by the Internet Service Provider. As a consequence, the IP address shown in the figure above (20.0.0.1) changes each time when the Internet connection is activated. The public IP address of the teleworker is to be considered as a variable.

The corporate network Internet connection

The domain name (**vpn.corporate.com**) is assumed to be resolvable by a DNS server on the public Internet. In this case, the public IP address attributed to SpeedTouch B is not relevant for the VPN configuration that we will construct.

IPSec parameters

The VPN connection between SpeedTouch A and SpeedTouch B relies on the IPSec protocol. In order to successfully complete the IPSec negotiations, a number of IPSec parameters need to be configured compliantly at both peers:

- pre-shared secret
- local ID
- remote ID
- IKE exchange mode
- IKE Security Descriptor
- IPSec Security Descriptor

VPN parameters

The VPN server remotely configures some Virtual Private Network parameters to integrate the VPN client in the corporate network. These parameters include:

- the IP address of the client in the VPN address range
- the location of the network servers, such as DNS server and WINS server.

VPN client-server scenario's on the SpeedTouch™

For a client-server scenario a dedicated set of user-friendly configuration pages is available. Separate pages exist for the client and server settings.

The **VPN Client** pages allow you to configure a VPN client that functions in Initiator mode. This means that the VPN client takes the initiative to set up a secure connection to a VPN server.

The **VPN Server** page allows you to configure a VPN server that functions in Responder mode. The VPN server provides simultaneous access for one or more VPN clients.

In this section

The following topics are discussed in this section:

2.1 Configuring the VPN client

VPN context

The VPN client always initiates the connection. Typically, the teleworker will manually dial in each time when the VPN connection is used.

Via the IKE Mode Config protocol, a new private IP address is attributed to the VPN client by the VPN server. This IP address is used as the private IP address in the encrypted messages. The SpeedTouch™ uses his Network Address Translation (NAT) capabilities to translate between this IP address and the IP address attributed to the computer in the private LAN section of the teleworker. In this way the computer communicates with the corporate network in a way that is transparent to the user.

For data transfers in the context of the VPN, the client will use the DNS and WINS servers of the corporate network.

For our configuration example, the pre-shared key authentication method is used.

VPN client configuration procedure outline

Perform the following steps to configure SpeedTouch A as a VPN client:

Step	Action	Page
1	"2.1.1 Filling out the VPN client parameters"	29
2	"2.1.2 Selecting the IKE authentication method"	31
3	"2.1.3 Selecting the start mechanism"	32

2.1.1 Filling out the VPN client parameters

Introduction

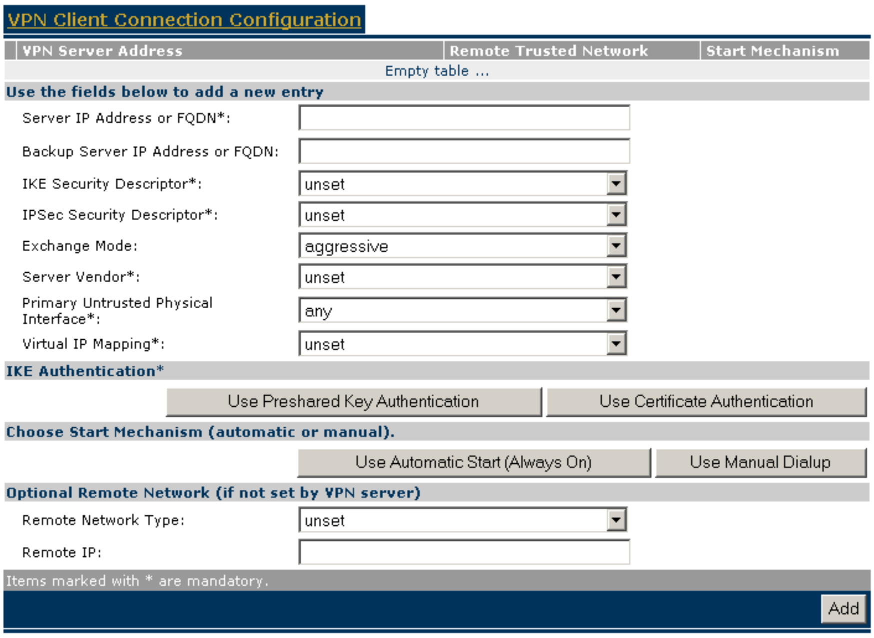
The following procedure describes how the remote gateway parameters are set for the VPN client-server application.

Procedure

Proceed as follows:

1 In **Expert mode**, select **VPN->VPN Client**.

The following page is shown:



VPN Client Connection Configuration

VPN Server Address	Remote Trusted Network	Start Mechanism
Empty table ...		

Use the fields below to add a new entry

Server IP Address or FQDN*:	
Backup Server IP Address or FQDN:	
IKE Security Descriptor*:	unset
IPSec Security Descriptor*:	unset
Exchange Mode:	aggressive
Server Vendor*:	unset
Primary Untrusted Physical Interface*:	any
Virtual IP Mapping*:	unset

IKE Authentication*

Choose Start Mechanism (automatic or manual).

Optional Remote Network (if not set by VPN server)

Remote Network Type:	unset
Remote IP:	

Items marked with * are mandatory.

Use Preshared Key Authentication
Use Certificate Authentication
Use Automatic Start (Always On)
Use Manual Dialup
Add

2 Fill out the network location of the server in the **Server IP Address or FQDN** field. Use the domain name: **vpn.corporate.com**. If you use the FQDN to identify the VPN server, the latter has to use the same FQDN as local identifier in the IKE negotiations.

Leave the **Backup Address or FQDN** field open.

3 Select the **IKE Security Descriptor**. In our example the **AES_SHA1_Adv** descriptor is selected.

> It is recommended to use **AES** as preferred encryption method. AES is more advanced, compared to DES or 3DES. It is faster for comparable key lengths, and provides better security.
>
> AES is selected by the American government as the new encryption standard to replace DES/3DES.

4 Select the **IPSec Security Descriptor**: In our example the **AES_SHA1_PFS_TUN** descriptor is selected.

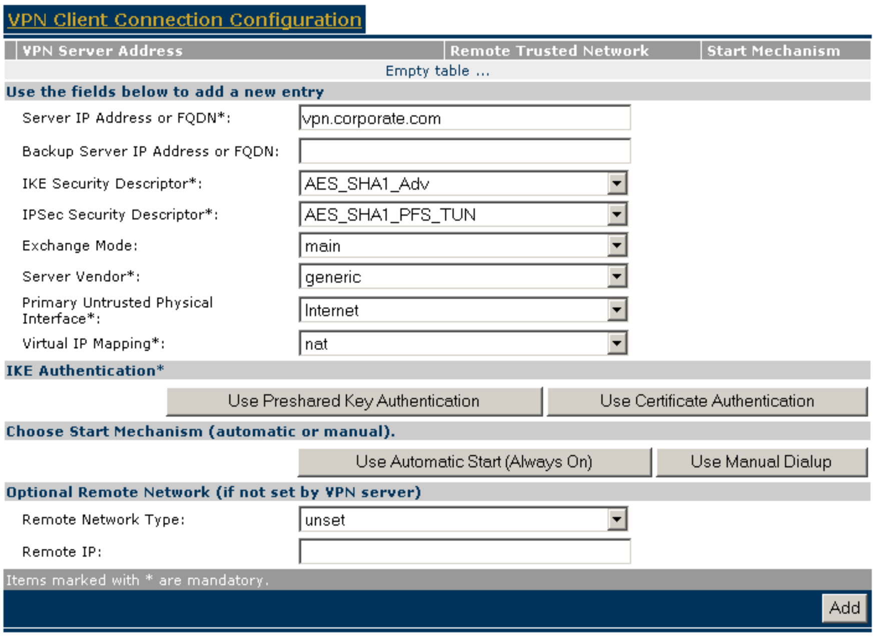
5 Select the **IKE Exchange Mode**: Select **main**.

6 Select the **Server Vendor**: Select **generic**.

7 Select the **Primary Untrusted Physical Interface**: Select your Internet interface from the list.

8 Select the **Virtual IP Mapping** method: select **nat**.

When all parameter fields are completed the configuration page looks like this:



VPN Client Connection Configuration

VPN Server Address	Remote Trusted Network	Start Mechanism
Empty table ...		

Use the fields below to add a new entry

Server IP Address or FQDN*: vpn.corporate.com
Backup Server IP Address or FQDN:
IKE Security Descriptor*: AES_SHA1_Adv
IPSec Security Descriptor*: AES_SHA1_PFS_TUN
Exchange Mode: main
Server Vendor*: generic
Primary Untrusted Physical Interface*: Internet
Virtual IP Mapping*: nat

IKE Authentication*

Use Preshared Key Authentication
Use Certificate Authentication

Choose Start Mechanism (automatic or manual).

Optional Remote Network (if not set by VPN server)

Remote Network Type: unset
Remote IP:

Items marked with * are mandatory.

Virtual IP mapping

Selecting **nat** as virtual IP address mapping has the effect that the VPN server attributes a virtual IP address to the SpeedTouch™ VPN client. This virtual IP address is stored in the SpeedTouch™. The SpeedTouch™ automatically creates a new NAT entry to map the virtual IP address to the IP addresses used on the local network. The NAT method supports simultaneous access to the VPN of multiple terminals. If you select the manual start mechanism however, the access to the VPN connection is restricted to the terminal that initiated the dial-in procedure.

2.1.2 Selecting the IKE authentication method

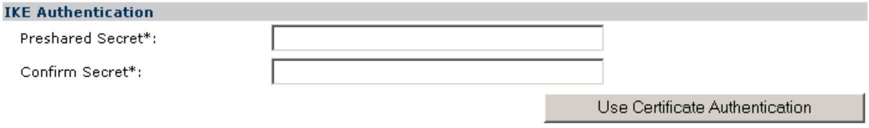
Introduction

The following procedure describes how to configure the pre-shared key authentication method.

Procedure

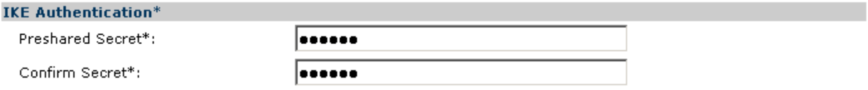
Proceed as follows:

1 Select **Use Preshared Key Authentication**. The configuration page is updated and looks like this:



2 Fill out the IKE Authentication parameters as follows:

- **Pre-shared secret**: a string to be used as a secret password for the VPN connection. This secret needs to be identically configured in the VPN client and VPN server.
- **Confirm Secret**: Re-type the secret to confirm your input (the secret is not shown in readable format on the screen).



IKE Authentication*

Preshared Secret*: ●●●●●●

Confirm Secret*: ●●●●●●

2.1.3 Selecting the start mechanism

Manual start

A teleworker will dial in to the corporate network when needed. Each time he has to enter his identity (his e-mail address). When using XAuth (optional), he has to provide his user name and password. If the XAuth information is not requested by the VPN server, the user name/password is not transmitted.

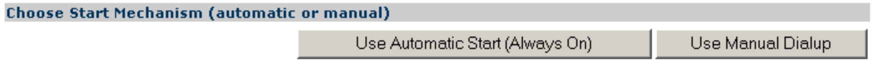
In addition, the selection of the manual start mechanism implies that only the terminal where the dial-in procedure is initiated gets access to the VPN connection. All other terminals can reach the Internet via the SpeedTouch™, but cannot reach the corporate network.

For a teleworker this is a convenient solution from a viewpoint of security.

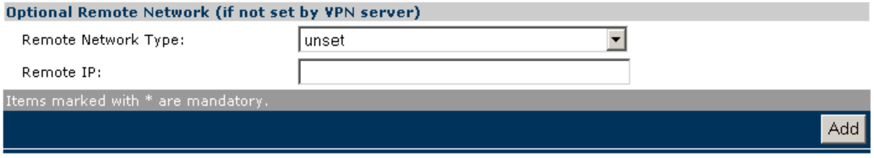
Procedure

Proceed as follows:

1 Select **Use Manual Dialup**.


Choose Start Mechanism (automatic or manual)
Use Automatic Start (Always On)
Use Manual Dialup

2 Leave the remaining fields open.

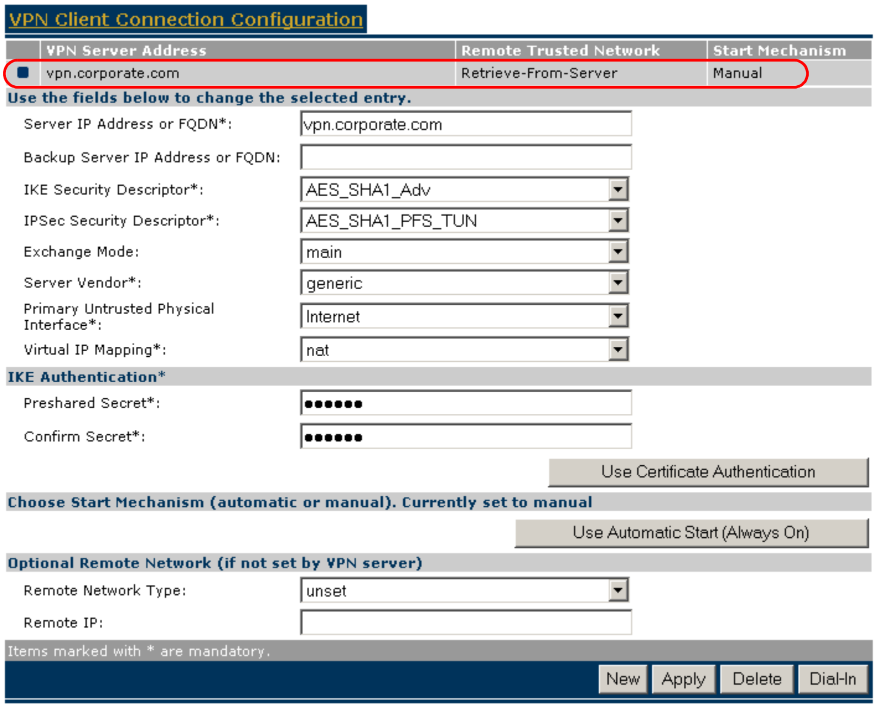


Remote Network Type: unset

Remote IP:

Items marked with * are mandatory.

3 Click **Add** to confirm the data. The VPN client is shown in the table at the top of the **VPN Client Connection Configuration** page.



	VPN Server Address	Remote Trusted Network	Start Mechanism
■	vpn.corporate.com	Retrieve-From-Server	Manual

Use the fields below to change the selected entry.

Server IP Address or FQDN*: vpn.corporate.com

Backup Server IP Address or FQDN:

IKE Security Descriptor*: AES_SHA1_Adv

IPSec Security Descriptor*: AES_SHA1_PFS_TUN

Exchange Mode: main

Server Vendor*: generic

Primary Untrusted Physical Interface*: Internet

Virtual IP Mapping*: nat

IKE Authentication*

Preshared Secret*: ●●●●●●

Confirm Secret*: ●●●●●●

Choose Start Mechanism (automatic or manual). Currently set to manual

Optional Remote Network (if not set by VPN server)

Remote Network Type: unset

Remote IP:

Items marked with * are mandatory.

4 Click **Save All** to save theSpeedTouch™ configuration.

This concludes the configuration of SpeedTouch A.

2.2 Configuring the VPN server

VPN context

In a VPN client-server scenario, the VPN server is always the responder in the IKE negotiations. Site B does not know a priori which remote Security Gateway will attempt to set up a VPN connection. SpeedTouch B is configured in such a way that a secure connection will be established with any Remote Gateway that meets the VPN settings, regardless its location in the public network.

VPN server configuration procedure outline

Perform the following steps to configure SpeedTouch B as a VPN server:

Step	Action	See
1	"2.2.1 Filling out the VPN server parameters"	34
2	"2.2.2 Selecting the IKE Authentication method"	38

2.2.1 Filling out the VPN server parameters

Introduction

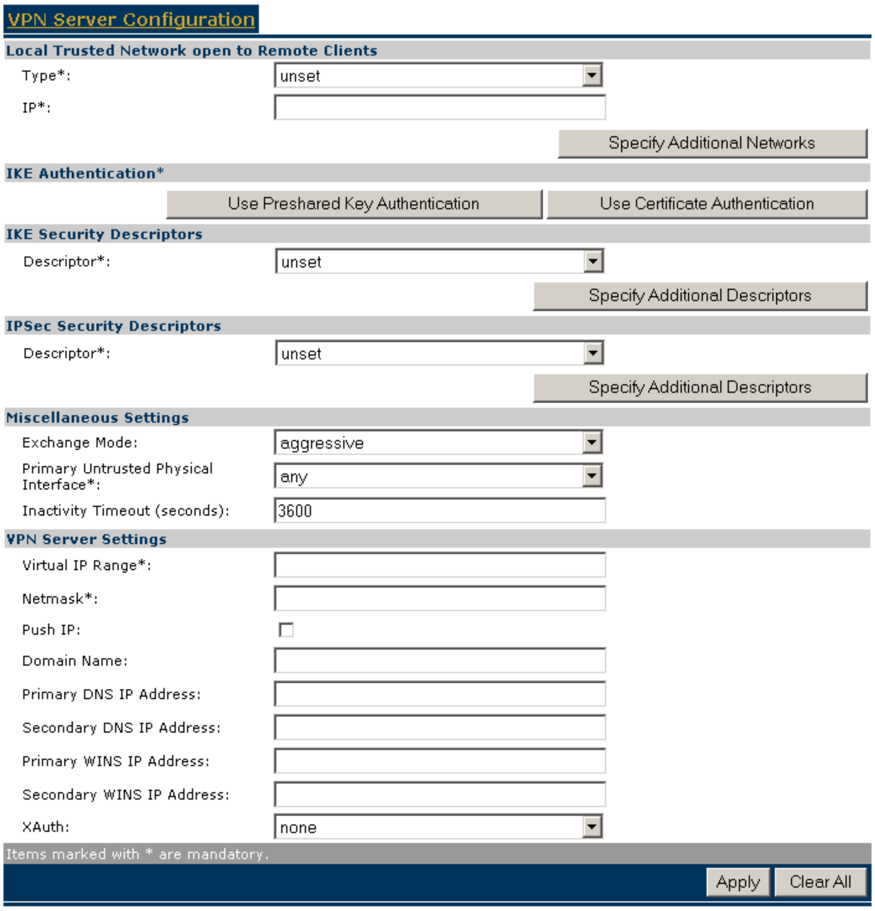
The following procedure describes how the VPN server parameters are set for the VPN client-server application.

Procedure

Proceed as follows:

1 In **Expert mode**, select **VPN->VPN Server.**

The following page is shown:



VPN Server Configuration

Local Trusted Network open to Remote Clients

Type*: unset

IP*:

IKE Authentication*

IKE Security Descriptors

Descriptor*: unset

IPSec Security Descriptors

Descriptor*: unset

Miscellaneous Settings

Exchange Mode: aggressive

Primary Untrusted Physical Interface*: any

Inactivity Timeout (seconds): 3600

VPN Server Settings

Virtual IP Range*:

Netmask*:

Push IP: ☐

Domain Name:

Primary DNS IP Address:

Secondary DNS IP Address:

Primary WINS IP Address:

Secondary WINS IP Address:

XAuth: none

Items marked with * are mandatory.

Specify Additional Networks
Use Preshared Key Authentication
Use Certificate Authentication
Specify Additional Descriptors
Specify Additional Descriptors
Apply
Clear All

2 Fill out the **Local Trusted Network** parameters as follows:

- Network **Type**: select **subnet** from the list
- **IP**: type the subnet identifier **10.0.0.0/16**

3 Select the **IKE Security Descriptor**. Select the same descriptor as configured in the VPN client. In our example **AES_SHA1_Adv** is selected.

4 Select the **IPSec Security Descriptor**. Select the same descriptor as configured in the VPN client. In our example **AES_SHA1_PFS_TUN** is selected.

5 Configure the **Miscellaneous** parameters in the following way:

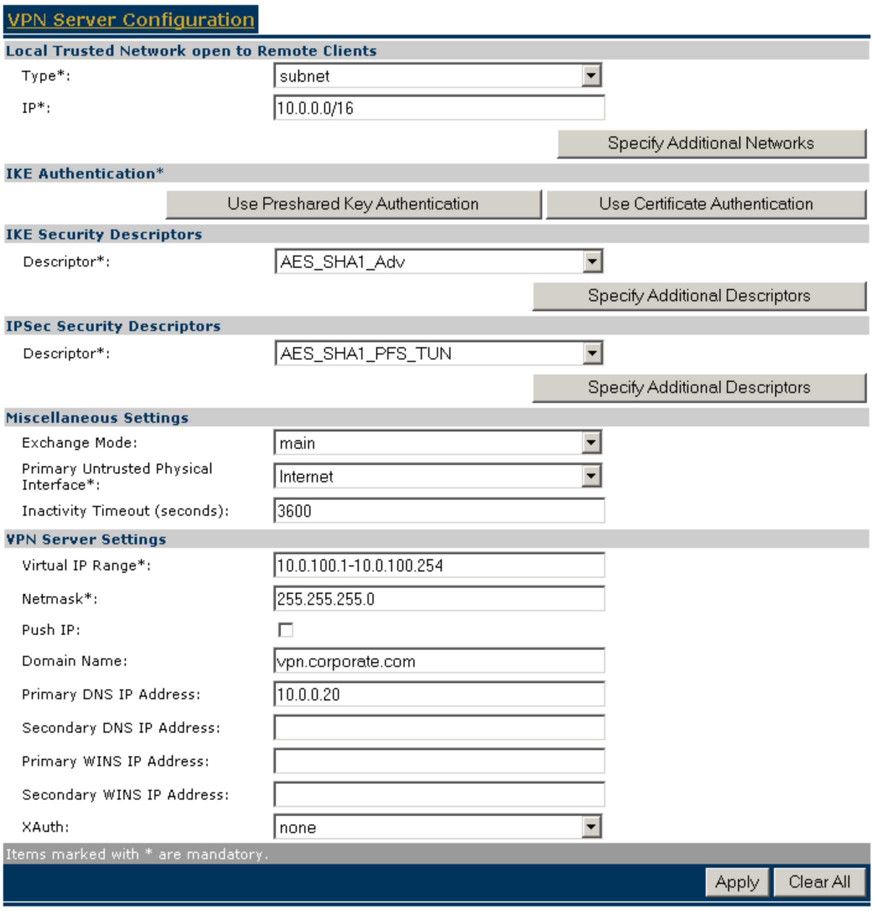
- Select the **IKE Exchange Mode**: Select **main**.
- Select the **Primary Untrusted Physical Interface**: Select your Internet interface from the list.

  The selection of a **Primary Untrusted Physical Interface** is relevant for incoming connections only. If you select **any**, VPN connections are accepted on all interfaces. This is relevant only in case your SpeedTouch™ is equipped with a backup interface.
- **Inactivity Timeout**: Use the default value of **3600 seconds**.

6 Fill out the VPN server Settings as follows:

- **Virtual IP Range**: Type **10.0.100.1-10.0.100.254**
  For more information, see “ Virtual IP Range” on page 36.
- **Netmask**: Type **255.255.255.0**
  For more information, see “ Netmask” on page 36.
- **Push IP**: Do not select the check box.
- For more information, see “ Push IP” on page 36.
- **Domain name**: Type **vpn.corporate.com**
  For more information, see “ Domain name” on page 36.
- **Primary DNS IP Address**: Type **10.0.0.20**
  For more information, see “ Primary DNS IP Address” on page 37.
- **Secondary DNS IP Address**: Leave open.
  For more information, see “ Secondary DNS IP Address” on page 37.
- **Primary WINS IP Address**: Leave open.
  For more information, see “ Primary WINS IP Address” on page 37.
- **Secondary WINS IP Address**: Leave open.
  For more information, see “ Secondary WINS IP Address” on page 37.
- **XAuth**: select **none**.

When all parameter fields are completed the configuration page looks like this:



VPN Server Configuration

Local Trusted Network open to Remote Clients

Type*: subnet

IP*: 10.0.0.0/16

IKE Authentication*

IKE Security Descriptors

Descriptor*: AES_SHA1_Adv

IPSec Security Descriptors

Descriptor*: AES_SHA1_PFS_TUN

Miscellaneous Settings

Exchange Mode: main

Primary Untrusted Physical Interface*: Internet

Inactivity Timeout (seconds): 3600

VPN Server Settings

Virtual IP Range*: 10.0.100.1-10.0.100.254

Netmask*: 255.255.255.0

Push IP: ☐

Domain Name: vpn.corporate.com

Primary DNS IP Address: 10.0.0.20

Secondary DNS IP Address:

Primary WINS IP Address:

Secondary WINS IP Address:

XAuth: none

Items marked with * are mandatory.

Specify Additional Networks
Use Preshared Key Authentication
Use Certificate Authentication
Specify Additional Descriptors
Specify Additional Descriptors
Apply
Clear All

Virtual IP Range

This parameter specifies the range of IP addresses from which the VPN client addresses are selected.

In our example, we reserved the subnet 10.0.100.0/24 for remote VPN client terminals. Therefore, in this field the range **10.0.100.1-10.0.100.254** is entered.

Netmask

This parameter specifies the netmask provided to the VPN client.

In our example we reserved the subnet 10.0.100.0/24 for remote VPN client terminals. the corresponding netmask is **255.255.255.0**.

Push IP

If you do not select this check box, the VPN server waits until the VPN client requests an IP address.

Domain name

The domain name provided to the VPN clients via IKE Mode Config. This setting depends entirely on the network architecture of private network located behind the VPN server.

In our example **vpn.corporate.com** is filled out.

Primary DNS IP Address	The IP address of the primary DNS server, provided to the VPN clients via IKE Mode Config. This is the primary DNS server in the local network that is open to VPN clients. In our example, this is the server with IP address **10.0.0.20**.
Secondary DNS IP Address	The IP address of the secondary DNS server, provided to the VPN clients via IKE Mode Config. This is the secondary DNS server in the local network that is open to VPN clients. In our example, no secondary DNS server is used. This field is left open.
Primary WINS IP Address	The IP address of the primary WINS server, provided to the VPN clients via IKE Mode Config. This is the primary WINS server in the local network that is open to VPN clients. In our example, no primary WINS server is used. This field is left open.
Secondary WINS IP Address	The IP address of the secondary WINS server, provided to the VPN clients via IKE Mode Config. This is the secondary WINS server in the local network that is open to VPN clients. In our example, no secondary WINS server is used. This field is left open.

2.2.2 Selecting the IKE Authentication method

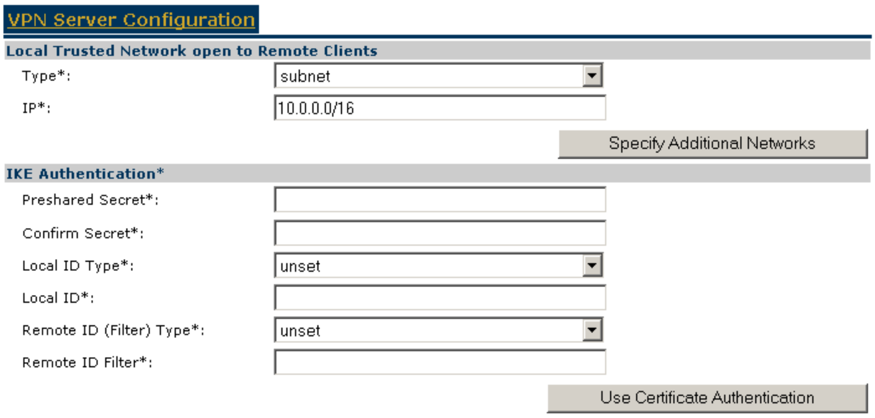
Introduction

The following procedure describes how to configure the pre-shared key authentication method.

Procedure

Proceed as follows:

1. Select **Use Preshared Key Authentication**. The configuration page is updated and looks like this:


VPN Server Configuration
Local Trusted Network open to Remote Clients
Specify Additional Networks
IKE Authentication*
Use Certificate Authentication

Type*: subnet
IP*: 10.0.0.0/16
Preshared Secret*:
Confirm Secret*:
Local ID Type*: unset
Local ID*:
Remote ID (Filter) Type*: unset
Remote ID Filter*:

2. Fill out the IKE Authentication parameters as follows:
   - **Pre-shared secret**: a string to be used as a secret password for the VPN connection. This secret needs to be identically configured in the VPN client and VPN server.
   - **Confirm Secret**: Re-type the secret to confirm your input (the secret is not shown in readable format on the screen)
   - Enter the **Local ID Type** and **Local ID**:
     - **Local ID Type**: select **fqdn**
     - **Local ID**: type **vpn.corporate.com**
       For more information, see “ Local ID” on page 38.
   - Enter the **Remote ID (Filter) Type** and **Remote ID Filter**:
     - **Remote ID (Filter) Type**: select **userfqdn**
     - **Remote ID Filter**: type ***@corporate.com**
       For more information, see “ Remote ID Filter” on page 39.
3. Click **Apply** to confirm the data.
4. Click **Save All** to save the SpeedTouch™configuration.

This concludes the configuration of SpeedTouch A.

Local ID

The **Local ID** parameter identifies the SpeedTouch™ VPN server during the Phase 1 negotiation with the remote VPN client. This identity must match the settings in the remote VPN client in order to successfully set up the IKE Security Association.

In our example, we used the domain name **vpn.corporate.com** in the VPN client settings to identify the server. In this case, we have to select **fqdn** as **Local ID Type** in the VPN server. The corresponding **Local ID** in our example is **vpn.corporate.com**.

Remote ID Filter

The **Remote ID** is used as a filter for VPN clients when they join the VPN. The values in the VPN server and in the remote VPN client must match in order to successfully set up the IKE Security Association.

In our example, the remote VPN client is a SpeedTouch™ device. This VPN client asks for the e-mail address of the user when he dials in. As a consequence we have to configure the allowed e-mail addresses in the VPN server. In order to allow simultaneous connections with multiple VPN clients, wildcards (an asterisk *) are used. It is required to select **userfqdn** for the **Remote ID (Filter) Type**. The corresponding e-mail address range is for example ***@corporate.com**, allowing all possible e-mail addresses in the domain corporate.com.

2.3 Using the VPN client-server connection

Dialling in

If the Manual Start mechanism is selected in the VPN client, no connection startup parameters are configured in SpeedTouch A. Each time the teleworker wants access to the VPN, he will need to manually dial in and enter the login parameters. A dial-in page is available in the SpeedTouch™ Web pages.

This is explained in "2.3.1 Dialling in to the VPN server" on page 41.

Closing a connection

When the VPN connection is not needed any more, the teleworker can manually close the connection. This is explained in "2.3.2 Closing a connection" on page 43.

2.3.1 Dialling in to the VPN server

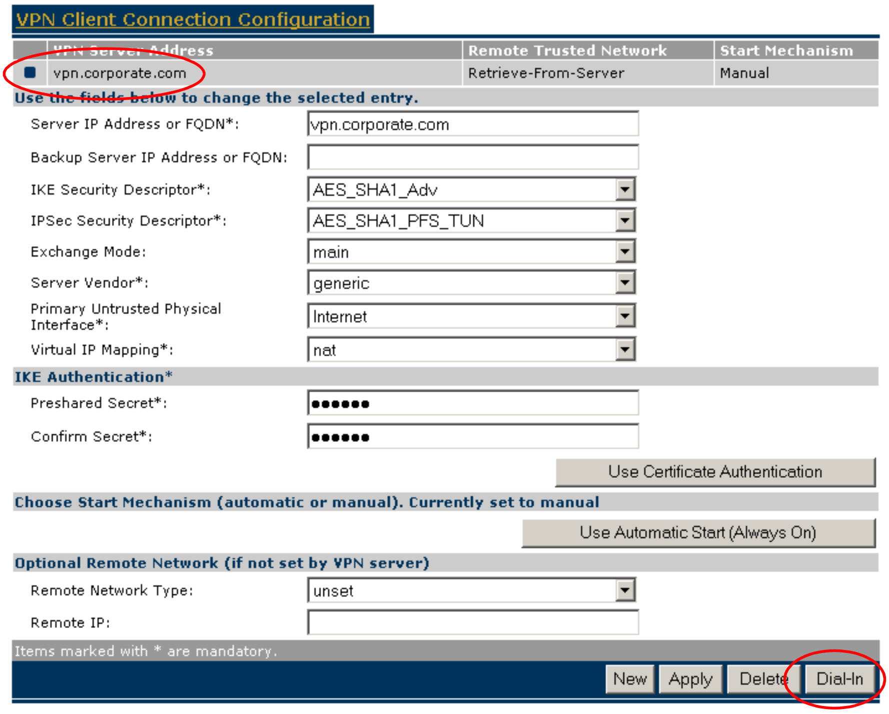
Introduction

The following procedure describes how to dial in to the VPN server.

Procedure

Proceed as follows:

1 In the **VPN client** page (SpeedTouch A in our example), select the VPN server from the table and click **Dial-In** at the bottom of the screen.



VPN Client Connection Configuration

	VPN Server Address	Remote Trusted Network	Start Mechanism
●	vpn.corporate.com	Retrieve-From-Server	Manual

Use the fields below to change the selected entry.

Server IP Address or FQDN*:	vpn.corporate.com
Backup Server IP Address or FQDN:	
IKE Security Descriptor*:	AES_SHA1_Adv
IPSec Security Descriptor*:	AES_SHA1_PFS_TUN
Exchange Mode:	main
Server Vendor*:	generic
Primary Untrusted Physical Interface*:	Internet
Virtual IP Mapping*:	nat

IKE Authentication*

Preshared Secret*:	••••••
Confirm Secret*:	••••••

Choose Start Mechanism (automatic or manual). Currently set to manual

Optional Remote Network (if not set by VPN server)

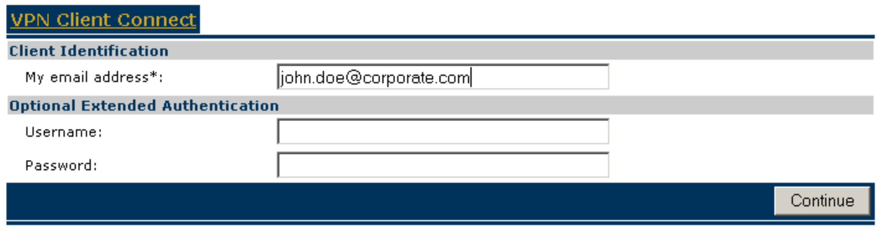
Remote Network Type:	unset
Remote IP:	

Items marked with * are mandatory.

Use Certificate Authentication
Use Automatic Start (Always On)
New
Apply
Delete
Dial-In

Alternatively you can use the link on the SpeedTouch™ home page.

2 In the **VPN Client Connect** page:



VPN Client Connect

Client Identification

My email address*:	john.doe@corporate.com

Optional Extended Authentication

Username:	
Password:	

Fill out the e-mail address of the teleworker, for example **john.doe@corporate.com**.

3 Click **Continue** to start the secure connection.

When the connection is established, this is shown on the **VPN Client Connection Configuration** page.

Verify the VPN connection

Click **Status** to verify the status of the VPN connection.

Click **Statistics** to see how much traffic the VPN connection has transferred so far.

As soon as the VPN connection is active, you should be able to ping a computer located in the remote LAN segment. For example, the computer with IP address 192.168.1.64 is able to ping the computer with IP address 10.0.0.1, and vice versa.

Surfing through the VPN tunnel

One of the SpeedTouch™ features for easy Internet access is the so-called Differentiated Services Detection (DSD). This feature monitors your HTTP traffic and alerts you when you want to browse to a location that is not reachable due to the fact that the connection to your Service Provider is not active. A SpeedTouch™ Web page appears that allows you to log in to your Service Provider.

When you configure an IPSec VPN connection, this feature has to be disabled in order to pass HTTP traffic through the VPN tunnel.

To verify that the Differentiated Services Detection is disabled, proceed as follows:

1 Browse to Basic Mode > Toolbox > Web Site Filtering.

2 Click Configure.

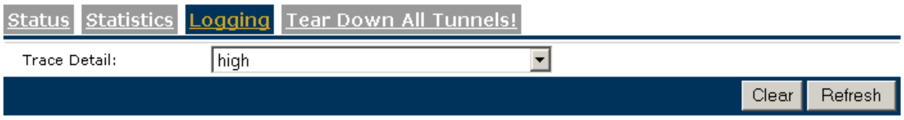
3 Verify that the check box “**Use Address Based Filter**” is not selected.

Be aware that in case Differentiated Services Detection is disabled, Web address based filtering is disabled as well. Take this in mind if you use the Web based filtering tool for parental control.

Troubleshooting

If you encounter problems setting up the VPN connection, you can use the **Debug** pages to diagnose your problem. In addition to the **Status** and **Statistics** information, the **Debug** pages contain a **Logging** page where you can monitor the negotiation process. This page helps you to determine the phase where the negotiations fail and the reason why.

It is recommended to select the highest level of detail to diagnose problems.

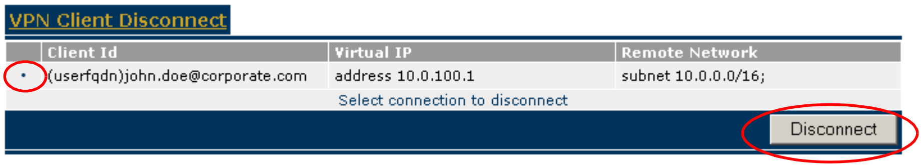


Trace Detail: high

2.3.2 Closing a connection

Disconnecting

All active VPN connections are shown on the **VPN Client Connection Configuration** page.



VPN Client Disconnect

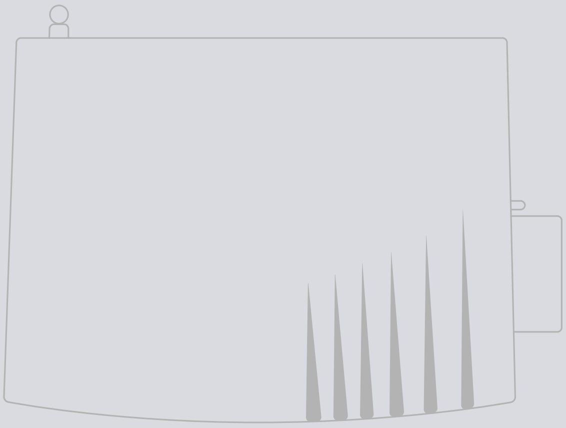
	Client Id	Virtual IP	Remote Network
●	(userfqdn)john.doe@corporate.com	address 10.0.100.1	subnet 10.0.0.0/16;

Select connection to disconnect

Select the connection you want to terminate and click **Disconnect**.

The secure connection is closed and is removed from the list of active connections.

A THOMSON BRAND



Need more help?

Additional help is available online at www.speedtouch.com

A THOMSON BRAND