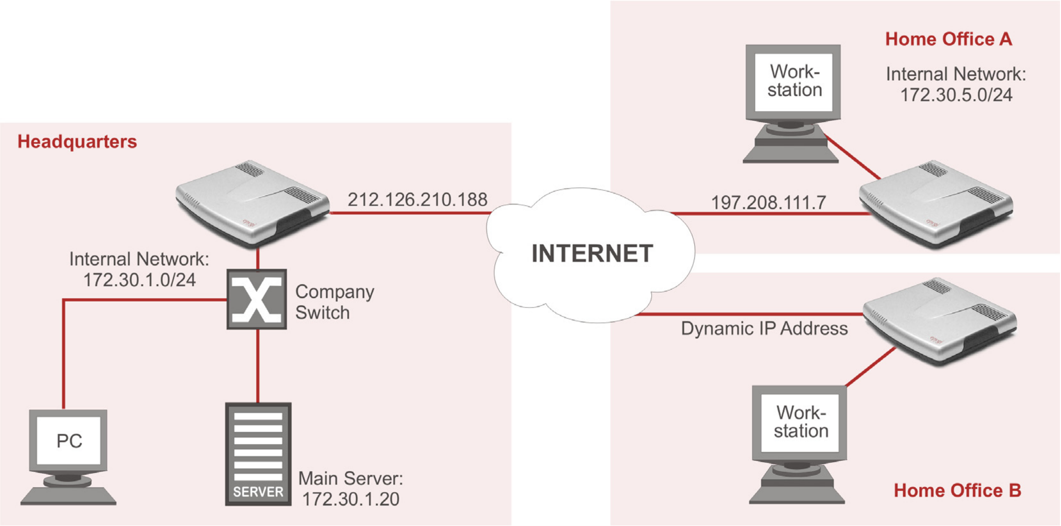
2 Clients Connecting to the Main Office via VPN

Abstract: This scenario shows how to configure a IPSec VPN infrastructure to connect 2 satellite or home offices to the headquarters using the **built in IPSec VPN functionality of the Quadro.**



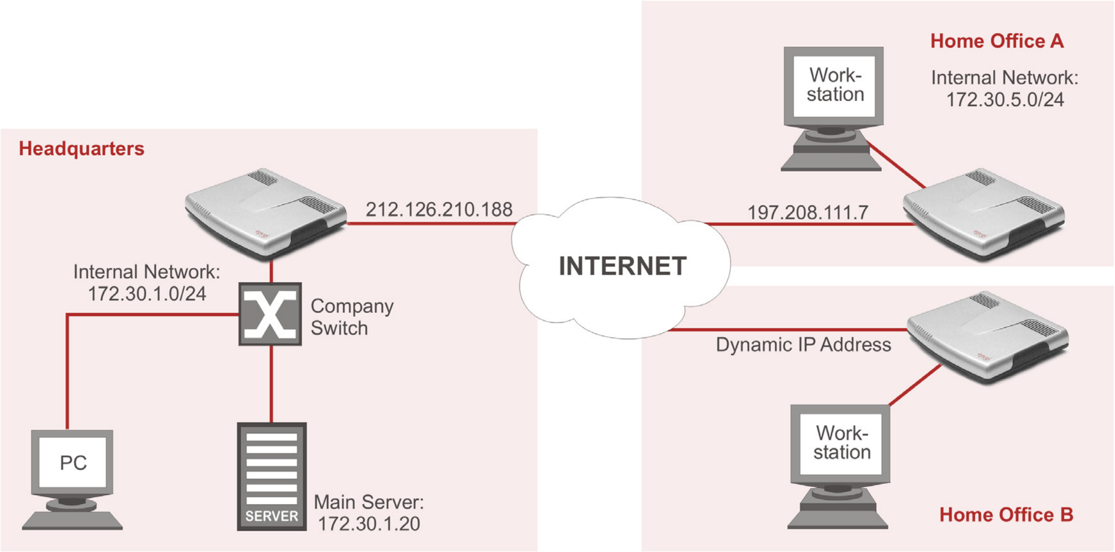
Quadro variants:	**Quadro2xPro, Quadro4x, Quadro16x**
valid for SW-version:	**All Quadro software**

Table of Contents:

1 Scenario

A customer has a headquarters with a couple of employees and 5 home/satellite offices. As the employees from the home offices need to access a server in the central office and transfer sensitive data, he wants to use VPNs. He wants to make sure that nobody else can connect to this server and that nobody in the Internet can decrypt the data.

The customer is using the Quadros also to make free phone calls to the home offices. But these calls do not need to be encrypted.



1.1 Objectives of the scenario

- The PCs located in the home office A and B can access the LAN and therefore the main server in the headquarters.
- The server in the headquarters is still safe, nobody else from outside can access it.

The data transport between the home office and the main server is strong encrypted, nobody can intercept that traffic.

1.2 Requirements and Preparations

- All internal networks must be disjunctive. This is a technical requirement for the IPSec VPN to work.
  In practice: If on both sides the LAN is 172.30.0.0, netmask 255.255.0.0 then the VPN can not connect the two sides.
  See also the sketch above as a valid example.
- All Quadros are installed and working, all of them have internet connectivity.

The PCs in the different location are using the Quadros as their Internet gateways.

2 Configuration

2.1 Configuring the Headquarters

Here we will create 2 IPSec VPN endpoints so that the home office A and B can connect to them.

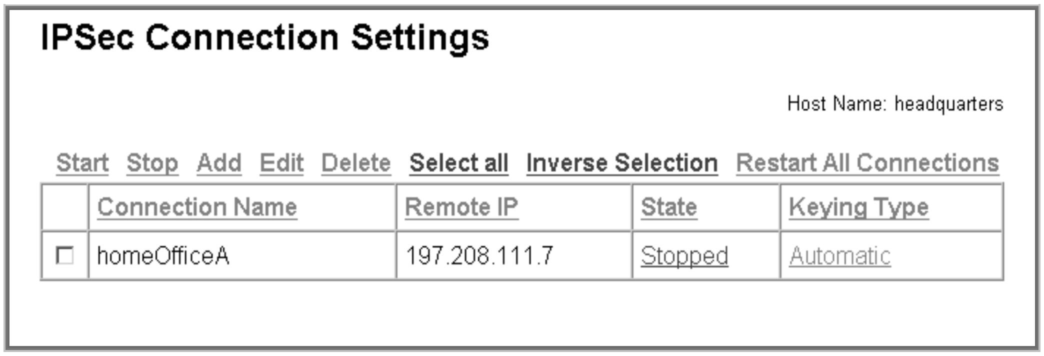
- Go to **VPN Configuration** -> **IPSec Configuration**
- Click on the **Add** Link to start the wizard.
- On the first page of the wizard type in a **Connection Name** and keep the **Peer Type** Quadro. In our example we use the Connection Name homeofficeA. No spaces are allowed here.
- On the second page of the wizard enter the following values:

Field	Value	Comment
Dynamic IP/Static IP	Static IP	The home office A has a static IP, so here we can select Static IP
Remote Gateway IP address	197.208.111.7	This is the IP of the home office A Quadro
Tunnel Checkboxes	Check only **Local Subnet <>Remote Subnet**	This will connect the local networks of the headquarters and the home office A
Remote Subnet IP	172.30.5.0/24	This is the subnet at home office A
Local Subnet IP	172.30.1.0/24	This is the subnet at the headquarters.
Keying Type	Auto(IKE)	Easiest way.

- On the next page then:

Field	Value	Comment
Shared Secret	secretone	This secret has to be identically on both sides of the connection. It is not the key that will encrypt the data. It is just used to establish a connection.
PFS	checked	

- On this page press **Finish** to complete the wizard.
- The wizard will take a while to create the VPN and the table of the VPN connections will look like:



IPSec Connection Settings

Host Name: headquarters

	Connection Name	Remote IP	State	Keying Type
□	homeOfficeA	197.208.111.7	Stopped	Automatic

- Now click on the **Add** Link to start the wizard and create the VPN to the second home office.
- On the first page of the wizard type in a connection name, this time homeofficeB.
- On the second page of the wizard:

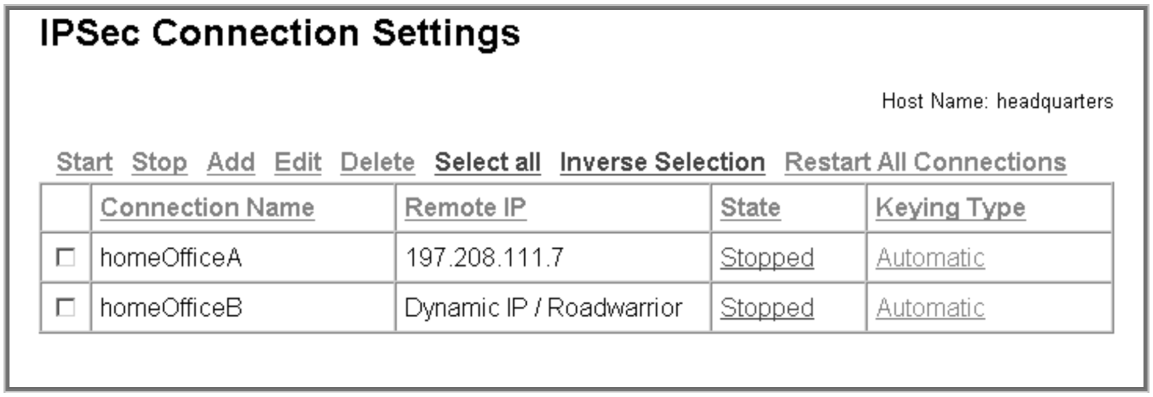
Field	Value	Comment
Dynamic IP / Static IP	Dynamic IP	The home office B has a dynamic IP address, so here we must select Dynamic IP
Tunnel Checkboxes	Only check **Local Subnet <> Remote Subnet**	This will connect the local networks of the headquarters and the home office B
Remote Subnet IP	172.30.6.0/24	This is the subnet at home office B
Local Subnet IP	172.30.1.0/24	This is the subnet at the headquarters.
Keying Type	Auto(IKE)	Easiest way.

- On the next page then:

Field	Value	Comment
Shared Secret	secrettwo	This secret has to be identically on both sides of the connection. It is not the key that will encrypt the data. It is just used to establish a connection.
PFS	checked	

Please Note:
If there is more than one VPN where you have to select Dynamic IP/Roadwarrior, all these VPNs have to share one secret.
In this example: If you create a VPN to home office C, which has as well a dynamic IP address, then home office B and C must have the same Shared Secret.

- On this page press finish to complete the wizard. The wizard will take a while to create the VPN and the table of the VPN connections will look like:



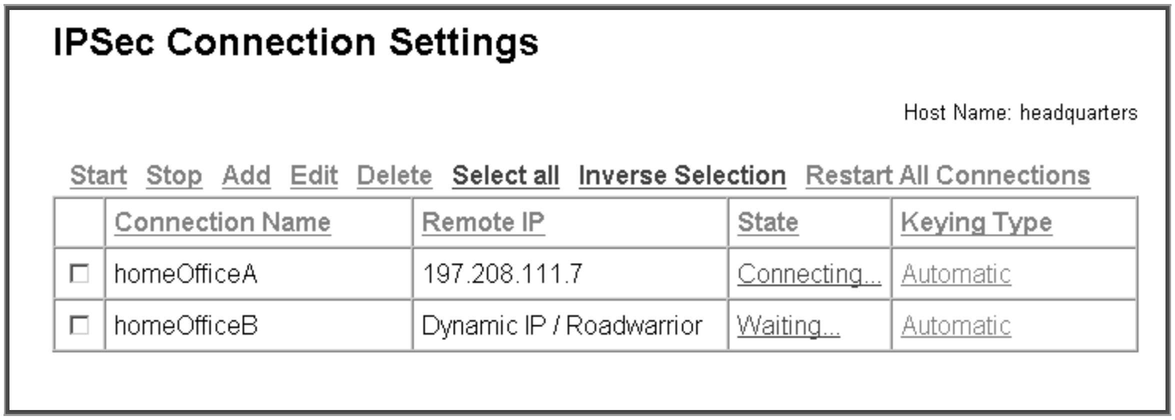
IPSec Connection Settings

Host Name: headquarters

Start Stop Add Edit Delete Select all Inverse Selection Restart All Connections

	Connection Name	Remote IP	State	Keying Type
□	homeOfficeA	197.208.111.7	Stopped	Automatic
□	homeOfficeB	Dynamic IP / Roadwarrior	Stopped	Automatic

- To activate both VPNs, check the box in the leftmost column and click the start link at the top of the table. Of course the VPNs will not work yet, as the remote side is not configured. Anyway it should show something like:



IPSec Connection Settings

Host Name: headquarters

Start Stop Add Edit Delete Select all Inverse Selection Restart All Connections

	Connection Name	Remote IP	State	Keying Type
□	homeOfficeA	197.208.111.7	Connecting...	Automatic
□	homeOfficeB	Dynamic IP / Roadwarrior	Waiting...	Automatic

Note the difference in the status occurs because of the difference in the Static/Dynamic Remote IP. If the remote IP is static, each side of the VPN may try to establish a connection. If the remote side is dynamic the local side does not know where to connect to and is waiting for the remote side to start the connection.

Now the headquarters is ready to get connected from the home offices.

2.2 Configuring the home office A

Here we will create the IPSec VPN endpoint for the home office A.

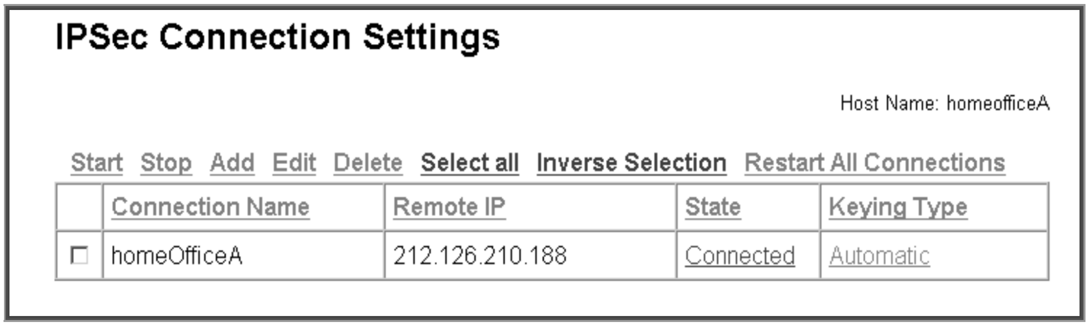
- Go to **VPN Configuration** -> **IPSec Configuration**
- Click on the **Add** Link to start the wizard.
- On the first page of the wizard type in a **Connection Name** and keep the **Peer Type** Quadro. in our example we use the connection name homeOfficeA.
  Please Note: The Connection Names at both ends of a VPN do not have to be the same. They are just names.
- On the second page of the wizard:

Field	Value	Comment
Dynamic IP/Static IP	Static IP	The headquarter has a static IP
Remote Gateway IP address	212.126.210.188	This is the IP of the headquarters Quadro
Tunnel Checkboxes	Check only **Local Subnet <>Remote Subnet**	This will connect the local networks of the headquarters and the home office A
Remote Subnet IP	172.30.1.0/24	This is the subnet of the headquarters
Local Subnet IP	172.30.5.0/24	This is the subnet of the home office A.
Keying Type	Auto(IKE)	Easiest way.

- On the next page then:

Field	Value	Comment
Shared Secret	secretone	This secret has to be identically on both sides of the connection. It is not the key that will encrypt the data. It is just used to establish a connection.
PFS	checked	

- On this page press **Finish** to complete the wizard. The wizard will take a while to create the VPN.
- Then check the box in the leftmost column and click the **Start** link. After some time the table should show:



IPSec Connection Settings

Host Name: homeofficeA

Start Stop Add Edit Delete Select all Inverse Selection Restart All Connections

	Connection Name	Remote IP	State	Keying Type
□	homeOfficeA	212.126.210.188	Connected	Automatic

If the State shows connected then it means the VPN between the two locations is ready and can be used.

2.3 Configuring the home office B

Here we will create the IPSec VPN endpoint for the home office B.

- Go to **VPN Configuration** -> **IPSec Configuration**
- Click on the **Add** Link to start the wizard.
- On the first page of the wizard type in a **Connection Name** and keep the **Peer Type** Quadro. in our example we use the connection name homeOfficeB.

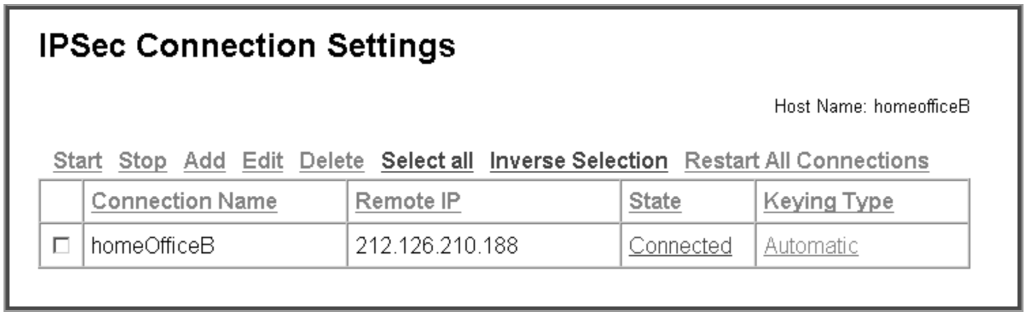
- On the second page of the wizard enter the following values:

Field	Value	Comment
Dynamic IP/Static IP	Static IP	The headquarter has a static IP
Remote Gateway IP address	212.126.210.188	This is the IP of the headquarters Quadro
Tunnel Checkboxes	Only check **Local Subnet <>Remote Subnet**	This will connect the local networks of the headquarters and the home office A
Remote Subnet IP	172.30.1.0/24	This is the subnet of the headquarters
Local Subnet IP	172.30.6.0/24	This is the subnet of the home office A.
Keying Type	Auto(IKE)	Easiest way.

- On the next page enter:

Field	Value	Comment
Shared Secret	secrettwo	This secret has to be identically on both sides of the connection. It is not the key that will encrypt the data. It is just used to establish a connection.
PFS	checked	

- On this page press **Finish** to complete the wizard. The wizard will take a while to create the VPN.
- Then check the box in the leftmost column and click the **Start** link. After some time the table should show:



IPSec Connection Settings

Host Name: homeofficeB

Start Stop Add Edit Delete Select all Inverse Selection Restart All Connections

	Connection Name	Remote IP	State	Keying Type
□	homeOfficeB	212.126.210.188	Connected	Automatic

If the **State** entry shows **Connected,** the VPN between the two locations is established and may be used.

3 Accomplished Functionality

In the sketched scenario the LANs of the headquarters and home office A / home office B are connected.
It means any PC located in the LAN of the home office A can reach any PC in the headquarters by means of the IP protocol. Same with the home office B.

As an example - when sitting at the workstation shown in the home office A and entering \\172.30.1.20 (the IP address of the main server) in the file explorer of Windows, then this request will reach the server, and the user will be asked to authenticate.

4 Additional Comments

- The described configuration does not connect the home office A and home office B.
- To encrypt VoIP calls between the locations as well, the tunnel checkbox: **Quadro <> Remote Gateway** must be checked on all endpoints.
- In the same manner you can create more VPNs to home offices.

- The throughput of the VPN is about 800Kbit/second with 3DES (highest encryption)
- In the current implementation it is not possible to have both endpoints of a VPN dynamic.
- If you want to address remote Windows machines by Windows names, then you need either to install or configure a WINS server, or add the host manually in the lmhosts file of Windows. This is out of the scope of this document.