

InterJak Application Notes Virtual Private Networks

Filanet Corporation
931 Benecia Avenue
Sunnyvale, CA 94085 USA
(408) 331-2900

INTERJAK VPN APPLICATIONS	3
Introduction.....	3
VPN Data Security	4
INTERJAK VPN SOLUTIONS.....	5
IPSEC BASED VPN SOLUTION.....	5
IPsec based VPN Configuration of InterJak - Static.....	6
IPsec based Compatible Site-to-Site VPN Devices.....	7
InterJak Site-to-Site Connection with Cisco Secure PIX	8
InterJak Site-to-Site Connection with Cisco 3005.....	10
InterJak Site-to-Site Connection with FireWall-1	12
InterJak Site-to-Site Connection with FreeS/WAN.....	14
InterJak Site-to-Site Connection with NetScreen	16
InterJak Site-to-Site Connection with Nokia CryptoCluster	19
InterJak Site-to-Site Connection with Windows 2000.....	22
IPsec based VPN Configuration of InterJak - Dynamic	26
InterJak Site-to-Site Connection with Unknown Remote Client Endpoint	27
PPTP BASED VPN SOLUTION	29
PPTP based VPN Clients.....	31
PPTP based Windows 98 SE Client.....	31
PPTP based Windows NT 4.0 Client.....	32
PPTP based Windows 2000 Client: Dial-Up connection	33
PPTP based Windows 2000 Client: DSL or Cable Modem connection.....	34
SITE-TO-CLIENT VPN SOLUTION.....	35
IPsec based Clients.....	37
IRE's SafeNet/SoftPK Client	37

InterJak VPN Applications

Introduction

Virtual Private Networks (VPNs) are one of the most promising methods available for leveraging the power of public networks for private networking applications. VPNs provide secure and stable tunnels through shared IP-based networks for remote access, extranet, and Intranet connectivity at a significantly less cost than those associated with private leased lines. VPNs use a technique called tunneling to send encrypted data packets across the shared network in a private tunnel that simulates a point-to-point connection. The advanced security features of VPN prevent outsiders to penetrate the transmitted data until it reaches its destination.

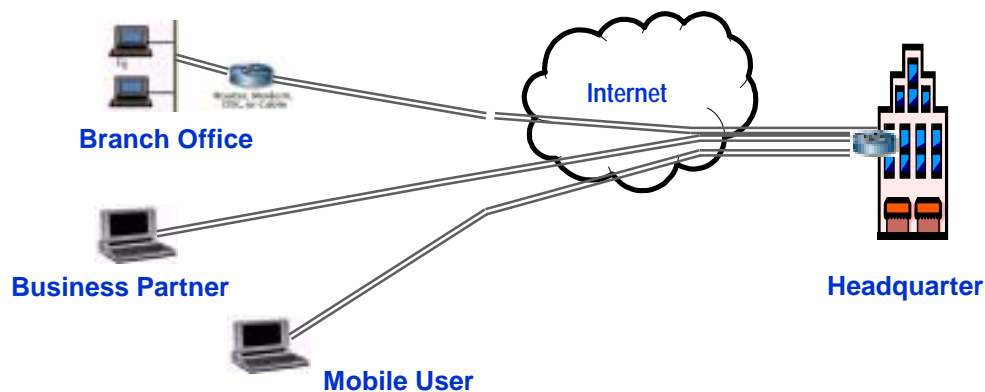


Figure 1: Site-to-Site Intranets, Extranets, and Mobile/Remote Users

Filanet's InterJak Service Appliance provides the VPN connectivity between small offices and their remote or mobile users. This allows small offices to extend their network quickly and securely to support emerging business opportunities and relationships without expensive and time-consuming additions to their networks. InterJak is easy to configure and remotely manageable through a web based browser interface. InterJak provides IPsec or PPTP (Point-to-Point Tunneling Protocol) based secure and stable connections over the Internet thus eliminating the need for expensive leased lines, dedicated modem banks or remote access servers for dial-up users.

The InterJak VPN is configured as an add-on keyed service that must be purchased before the service is activated. Service Providers can choose to offer VPN as part of their base service or a stand-alone value added service, depending on the individual needs of their customers.

VPN Data Security

Security of data traveling through VPN tunnels is achieved by the following three basic security “services”:

- Authentication
- Privacy
- Integrity

Authentication – This feature ensures that the correct remote devices are connected. Authentication is performed by a common shared secret pre-configured at both ends of the VPN tunnel or by a username and password.

IPsec based VPN authentication uses a shared secret and the Internet Key Exchange (IKE) protocol.

PPTP based VPN authentication uses username and password and one of the following protocols:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)
- MS-CHAP (CHAP using Microsoft encrypted passwords)
- MS-CHAPv2 (CHAP using Microsoft encrypted passwords)

Encryption – This feature ensures privacy by making the transmitted data useless for outsiders. Packets are encrypted using different algorithms.

- IPsec based VPN performs encryption using DES or 3DES algorithms.
- PPTP based VPN uses Microsoft Point-to-Point Encryption (MPPE). Note that encryption does not work with PAP and CHAP authentication.

Integrity – This feature ensures that any alteration to packets does not go undetected. This is achieved by checksums on the transmitted data, using the hash algorithms SHA-1 and MD5.

InterJak VPN Solutions

InterJak is designed to provide IPsec and VPN based solutions for three different types of configurations, listed below:

Types of connections	Number of Connections
Site-to-Site (IPsec based)	4
Site-to-Site/Client (IPsec based)	4
Client to Site (PPTP based)	8

Maximum Recommended Connections = 4 IPsec + 8 PPTP
 Tested IPsec Site-to-Site throughput = 1.1 Mbps with 3DES–MD5

IPsec based VPN Solution

IPsec is a security protocol defined by the Internet Engineering Task Force (IETF).

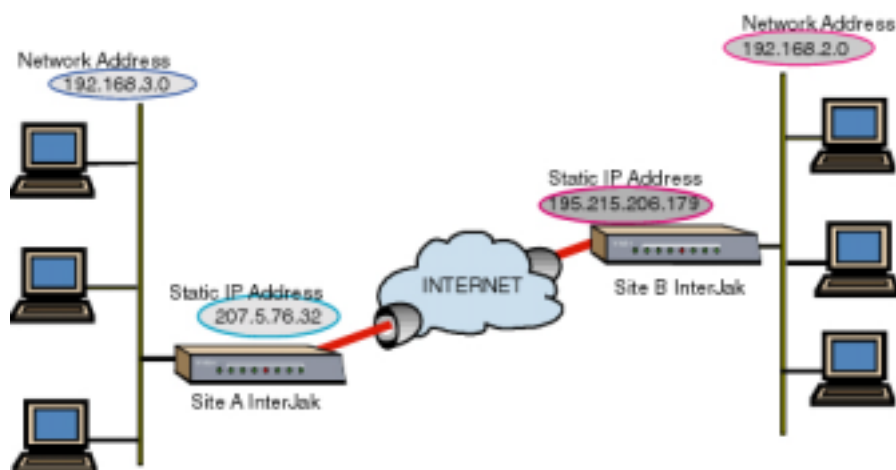


Figure 2: IPsec Based Site-to-Site VPN Connection

InterJak provides IPsec based VPN connections that can be enabled between two InterJaks, or InterJak and compatible VPN devices. A so-called Site-to-Site connection tunnels traffic between 2 IP subnets through an IPsec based VPN tunnel.

Two types of VPN tunnels can be configured, a Static tunnel where either side of the tunnel can negotiate the connection, or Dynamic tunnel where only the remote side of the tunnel can initiate the connection. For the Static VPN connection, knowledge of local and remote IP addresses, local and remote subnets, shared secret and type of security is required to configure such a connection. For the Dynamic VPN connection, knowledge of the remote IP address and remote subnet is not necessary, but you can configure a range for the remote subnet to restrict remote clients from connecting if they are not setup within that range.

IPsec based VPN Configuration of InterJak - Static

The following conditions must be fulfilled to create an IPsec based VPN tunnel between the InterJak and the remote device:

- IPsec based VPN capable devices at both ends of the tunnel.
- Static external public IP addresses at both ends
- Common shared secret must be available at both ends.

IPsec based VPN tunnel between site-to site devices is configured using the **Services, VPN** and then **Add Connection** command in the in InterJak Management Suite:

The screenshot displays the 'Add VPN Connection' configuration page in the InterJak Management Suite. The page is titled 'Services: VPN Site-to-Site/Client: Add Connection'. On the left, there is a navigation menu with 'SYSTEM', 'MONITOR', 'SERVICES', and 'USERS' tabs. The main content area is divided into several sections:

- Add VPN Connection:** Name: Tunnel1; Remote end-point (IP or host name): 195.215.205.179; Enabled:
- Note:** the VPN connection will always start on interface Ethernet 2.
- Local Subnet:** IP subnet: 192.168.3.0; IP subnet mask: 255.255.255.0
- Remote Subnet:** IP subnet: 192.168.2.0; IP subnet mask: 255.255.255.0
- Shared Secret:** Shared secret: ipsecsecret
- Advanced Settings:** Protocol: ESP: Triple DES and MD5 Signature; Perfect Forward Secrecy (PFS): ; ISAKMP security association lifetime: 1 hours 00 minutes; IPsec security association lifetime: 0 hours 00 minutes
- Settings for NAT:** NAT Remote end-point: [empty field]

At the bottom right, there are three buttons: 'Reset', 'Cancel', and 'Apply'.

Figure 3: Site-to-Site VPN Configuration Screen (Static)

Enter the following information to configure InterJak for IPsec based VPN connection.

- Check **Enable** VPN Connection
- Name of the Tunnel
- Remote and Local IP Addresses
- Remote and Local Subnets
- Shared secret
- Encryption Method
- Lifetimes of the IPsec and ISAKMP security
- Click **Apply** to save the above information.

IPsec based Compatible Site-to-Site VPN Devices

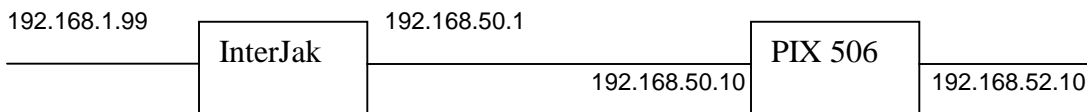
The InterJak is compatible with the following VPN devices; however, the latest list of compatible devices may be obtained from the Filanet web site <http://www.filanet.com>:

PIX – Cisco
3005 – Cisco
FreeS/Wan – Linux
Firewall-1 (VPN-1) – Checkpoint
Windows 2000 – Microsoft
NetScreen – NetScreen
Nokia CC – Nokia

InterJak Site-to-Site Connection with Cisco Secure PIX

The following is a simple example of a VPN tunnel between a Cisco PIX (506) and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.52.0/255.255.255.0.

Schematic drawing of setup:



InterJak configuration

Name:	InterJak-Cisco
Remote end-point (IP or host name):	192.168.50.10
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.52.0
IP subnet mask:	255.255.255.0
Shared secret:	Cisco1234
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	Empty

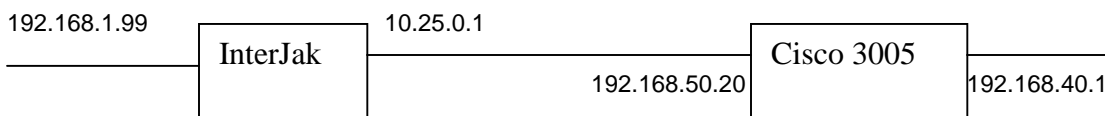
Cisco Configuration

Configuration commands	Comments
access-list 90 permit ip 192.168.52.0 255.255.255.0 192.168.1.0 255.255.255.0	<i>Local and Remote subnet</i>
ip address outside 192.168.50.10 255.255.255.0 ip address inside 192.168.52.10 255.255.255.0	<i>IP addresses of PIX</i>
nat (inside) 0 0.0.0.0 0.0.0.0 0 0	
static (inside,outside) 192.168.52.0 192.168.52.0 netmask 255.255.255.0 0 0	
sysopt connection permit-ipsec	
crypto ipsec transform-set myset esp-3des esp-md5-hmac	<i>Matches Protocol</i>
crypto map toInterJak 20 ipsec-isakmp	
crypto map toInterJak 20 match address 90	
crypto map toInterJak 20 set pfs	<i>Matches PFS</i>
crypto map toInterJak 20 set peer 192.168.50.1	<i>InterJak IP address</i>
crypto map toInterJak 20 set transform-set myset	
crypto map toInterJak interface outside	
crypto ipsec security-association lifetime second 28800	<i>Matches IPsec SA lifetime</i>
isakmp enable outside	
isakmp key cisco1234 address 192.168.50.1 netmask 255.255.255.255	<i>Matches preshared secret</i>
isakmp identity address	
isakmp policy 9 authentication pre-share	
isakmp policy 9 encryption 3des	
isakmp policy 9 hash md5	
isakmp policy 9 group 2	
isakmp policy 9 lifetime 86400	<i>Matches ISAKMP SA lifetime</i>

InterJak Site-to-Site Connection with Cisco 3005

The following is a simple example of a VPN tunnel between a Cisco 3005 and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.40.0/255.255.255.0.

Schematic drawing of setup:



InterJak configuration

Name:	InterJak-Cisco
Remote end-point (IP or host name):	192.168.50.20
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.40.0
IP subnet mask:	255.255.255.0
Shared secret:	Cisco1234
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	No
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	empty

Cisco Configuration

(Make sure you are configuring the Concentrator from the private side, because the HTTP packets won't make it through the filter on the public side)

From the HTML interface (using a web browser) navigate to:

Configuration | System | Tunneling Protocols | IPSec | Lan-to-Lan

And set the following parameters:

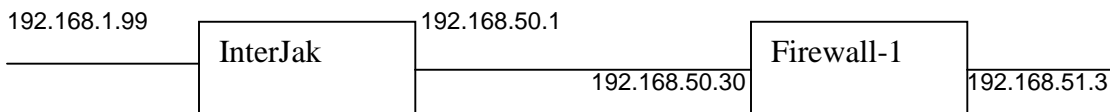
Name	InterJak
IKE Peer	10.25.0.1
Dig. Cert.	<i>None</i>
Preshared Key	Cisco1234
Authentication	ESP/MD5/HMAC-128
Encryption	3DES-168
IKE Proposal	IKE-3DES-MD5
Local Network	
Network List	<i>(leave at default setting)</i>
IP Address	192.168.40.0
Wildcard Mask	0.0.0.255 (this will be the inverse of the Remote subnet mask on the InterJak)
Remote Network	
Network List	<i>(leave at default setting)</i>
IP Address	192.168.1.0
Wildcard Mask	0.0.0.255 (this will be the inverse of the Local subnet mask on the InterJak)

Hit Apply at the bottom of the Lan-to-Lan page and then OK.

Remember to save the configuration by pressing the save icon in the top right hand corner.

InterJak Site-to-Site Connection with FireWall-1

The following is a simple example of a VPN tunnel between a FW-1 and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.52.0/255.255.255.0. (This setup was tested against a FW-1 version 4.1 running on an NT server.)



InterJak Configuration

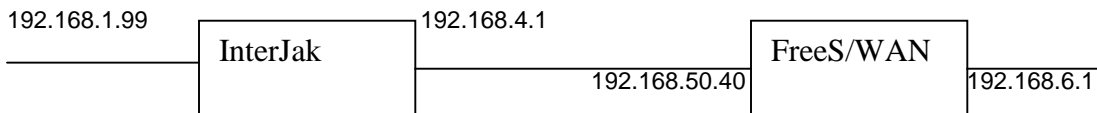
Name:	InterJak-FW1
Remote end-point (IP or host name):	192.168.50.30
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.51.0
IP subnet mask:	255.255.255.0
Shared secret:	secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	empty

Firewall-1 Configuration

- Create 2 network objects representing the subnets between which the VPN traffic runs. In this example create Net_1 and Net_51 like this:
 - Net_1
IP address: 192.168.1.0
Netmask: 255.255.255.0
 - Net_51
IP address: 192.168.51.0
Netmask: 255.255.255.0
- Configure a network object to represent the InterJak with the following settings:
 - It must be of type gateway.
 - In the VPN properties, select the Domain to be Net_1.
 - The encryption scheme should be IKE.
 - Under IKE Properties select 3DES and MD5.
 - Authentication method should be Pre-shared Secret, and the pre-shared secret should be entered. (The pre-shared secret should match the one entered on the InterJak, in this example it is `secret`)
 - Deselect Aggressive Mode
 - Select Support Subnets
- The network object that represents the Firewall-1 itself should also be modified. Its VPN properties should be similar to the properties of the object representing the InterJak.
- The lifetimes of the Encryption Keys are set in the Policy->Properties. Select the Encryption tab.
 - Renegotiate IKE Security Associations every: 60 mins
 - Renegotiate IPSEC Security Associations every: 28800 secs
- Now create 2 firewall rules for the actual traffic. One rule is for traffic from Net_1 to Net_51, while the other is for traffic from Net_51 to Net_1. The action for both rules should be encrypt, with the following properties:
 - Encryption Scheme: IKE
 - IKE properties:
 - Transform: ESP
 - Encryption Algorithm: 3DES
 - Data Integrity: MD5
 - Allowed Peer Gateway: InterJak
 - Perfect Forward Secrecy: Checked.

InterJak Site-to-Site Connection with FreeS/WAN

The following is a simple example of a VPN tunnel between a FreeS/WAN and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.99.0/255.255.255.0. (This setup was tested against a FreeS/WAN 1.3.)



InterJak configuration:

Name:	InterJak-FreeS/WAN
Remote end-point (IP or host name):	192.168.50.40
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.6.0
IP subnet mask:	255.255.255.0
Shared secret:	secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	empty

FreeS/WAN Configuration

In the /etc/ipsec.conf file you must setup the configuration as follows:

```
conn vpnij
    # Remote security gateway, subnet behind it, next hop toward it.
    right=192.168.4.1
    rightsubnet=192.168.1.0/24
    rightright=192.168.4.4
    # Local security gateway, subnet behind it, next hop toward it.
    left=192.168.50.5
    leftsubnet=192.168.6.0/24
    leftnextthop=192.168.50.1
    # Authorize this connection, but don't actually start it, at startup.
    auto=add
```

Each connection must have a unique name.
 The nextthop parameter is the IP of the router opposite the VPN device.
 Any line preceded by # is a comment line.

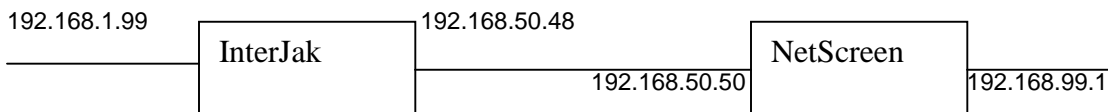
In the /etc/ipsec.secrets file you must setup the configuration as follows:

```
192.168.50.5 192.168.4.1 "secret"
```

The format is: <local-endpoint> <remote-endpoint> "<secret>"
 The secret must always be in quotes.

InterJak Site-to-Site Connection with NetScreen

The following is a simple example of a VPN tunnel between a NetScreen and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.99.0/255.255.255.0. (This setup was tested against a NetScreen 5 running ver. 2.10r4.)



InterJak configuration:

Name:	InterJak-Netscreen
Remote end-point (IP or host name):	192.168.50.50
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.99.0
IP subnet mask:	255.255.255.0
Shared secret:	secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	8 hours 00 minutes
IPSec security association lifetime:	1 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	<i>empty</i>

Note: The lifetimes for ISAKMP and IPSec are set to match the default settings of the NetScreen.

NetScreen Configuration

Select Network->VPN->Gateway->New Remote Gateway

Name: InterJak

Preshare key: secret

Phase 1 proposal: pre-g2-3des-md5

Local identity: *empty*

Remote Gateway - Fixed IP address: selected

IP address: 192.168.50.48

Remote Gateway ID: *empty*

Mode: Select Main mode Remote Gateway/Used - Dynamic IP address: Not selected

Press OK

Select Network->VPN->Autokey IKE->New Autokey IKE Entry

Name: InterJak

Enable Replay Protection: Selected

Remote Gateway Tunnel Name: InterJak (The one configured above)

Phase 2 proposal: g2-esp-3des-md5

Press OK

Select Lists->Addresses->Trusted->New Address

Address Name: Localnet

IP Address/Domain Name: 192.168.99.0

NetMask: 255.255.255.0

Comment: Local network

Location: Select Trust

Press OK

Select Lists->Addresses->Untrusted->New Address

Address Name: Remotenet

IP Address/Domain Name: 192.168.1.0

NetMask: 255.255.255.0

Comment: Remote network

Location: Select Untrust

Press OK

Select Network->Policy->Outgoing->New Policy

Name: VPN tunnel

Source Address: Localnet

Destination Address: Remotenet

Service: ANY

Action: Encrypt

VPN tunnel: InterJak

Logging: Not selected

Counting: Not selected

Alarm Threshold: 0 Bytes/Sec 0 Bytes/Min

Schedule: None

Traffic Shaping: Off

Press OK

If you have virtual addresses defined, you will also need to create an incoming policy.

Select Network->Policy->Incoming->New Policy

Name: VPN tunnel

Source Address: Remotenet

Destination Address: Localnet

Service: ANY

Action: Encrypt

VPN tunnel: InterJak

Logging: Not selected

Counting: Not selected

Alarm Threshold: 0 Bytes/Sec 0 Bytes/Min

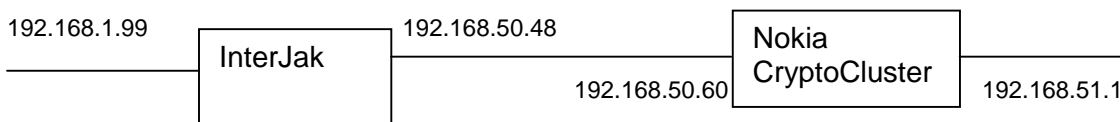
Schedule: None

Traffic Shaping: Off

Press OK

InterJak Site-to-Site Connection with Nokia CryptoCluster

The following is a simple example of a VPN tunnel between a Nokia CC500 and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.99.0/255.255.255.0. (This setup was tested against a Nokia running ver. xx.)



InterJak configuration:

Name:	InterJak-Nokia
Remote end-point (IP or host name):	192.168.50.60
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.51.0
IP subnet mask:	255.255.255.0
Shared secret:	secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	8 hours 00 minutes
IPSec security association lifetime:	1 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	empty

Note: The lifetimes for ISAKMP and IPSec are set to match the default settings of the Nokia CryptoCluster.

Nokia CryptoCluster Configuration

Select Gateway Properties->TRAFFIC FILTERS->Gateway Filters->New...

"New Filter" window opens

Filter Name: InterJak-Nokia

Select radio button: Protect Traffic Using IPSec

Select Establish tunnels to Remote Gateway:New...

Answer Yes to "Do you want to define a new Non-Managed Gateway?"

"New Non-managed Gateway" window opens

Description: InterJak

IP Address: 192.168.50.48

Press OK

"Edit Gateway Peering" window opens

Select Establish security tunnels using IKE policy:New...

"New IKE Policy" window opens

Description: IJ Preshared Key

Preshared key: secret

Confirm key: secret

Select Advanced...

"Advanced IKE Policy Settings" window opens

Use integrity algorithm: MD5

Use encryption algorithm: TRIPLE DES

Use Diffie-Hellman group description: Group #2 (MODP 1024-bit)

Generate new security associations when elapsed time reaches: 8 hours

Press OK

Press OK

Press OK

Back at the **"New Filter"** window

Select Protect traffic by applying IPSec policy: New...

"Add IPSec Policy" window opens

Select Advanced...

Policy Name: InterJak Policy

Select Enable Privacy checkbox

Enable Privacy: TRIPLE DES

Select Enable Integrity & replay prevention checkbox

Enable Integrity & replay prevention: HMAC MD5

Implement integrity using the IPSec protocol: ESP

Select Enable PFS to protect session keys checkbox

Use Diffie-Hellman group description: Group #2 (MODP 1024-bit)

Select Generate new keys when time elapsed reaches checkbox

Generate new keys when time elapsed reaches: 1 hour

Press OK

Back at the **"New Filter"** window

Select Standard radio button under Filter View

Local Hosts:

Select Select...

"Select local hosts protected by" window opens

Select New...

"New Host Group" window opens

Description: local subnet

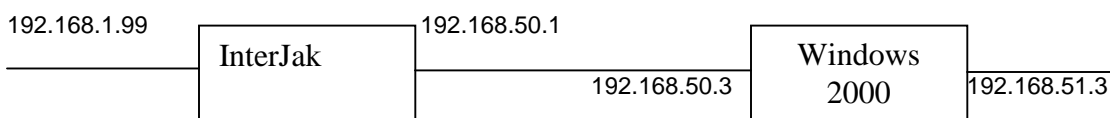
Select Add...
“**New Host**” window opens
IP Address: 192.168.99.0
Subnet Mask: 255.255.255.0
Press OK
Press OK
Highlight “local subnet” and Press Add
Press OK
Remote Hosts:
Select Select...
“**Select remote hosts protected by**” window opens
Select New...
“**New Host Group**” window opens
Description: remote subnet
Select Add...
“**New Host**” window opens
IP Address: 192.168.1.0
Subnet Mask: 255.255.255.0
Press OK
Press OK
Highlight “remote subnet” and Press Add
Press OK
Back at the “**New Filter**” window
Select All Services radio button
Press OK
File->Close
Save Changes? Press Yes
Gateway->Apply changes now

InterJak Site-to-Site Connection with Windows 2000

For an introduction in using VPNs in Windows 2000 please refer to [Step-by-Step Guide to Internet Protocol Security \(IPSec\)](#) from Microsoft.

The following is a simple example of a VPN tunnel between a Windows 2000 server and an InterJak. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.51.0/255.255.255.0.

Note that in order to use 3DES encryption with Windows 2000, a security update from Microsoft might be required.



InterJak Configuration

Name:	InterJak-W2K
Remote end-point (IP or host name):	192.168.50.3
Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.51.0
IP subnet mask:	255.255.255.0
Shared secret:	secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	empty

Windows 2000 Configuration for InterJak

Open My Computer -> Control Panel -> Administrative Tools -> Local Security Policy.

Select "IP Security Policies on Local Machine" from the tree.

From the "Action" menu select "Create IP Security Policy"

This starts the IP Security Policy Wizard. Click Next.

Give the connection a meaningful name, e.g. W2K-InterJak

Click Next

Deselect "Activate the default response rule"

Click Next

Select "Edit Properties"

Click Finish

This opens a properties box for the connection.

Under the General tab set the following:

Check for policy changes every: 180 minutes.

Click Advanced

Select "Master Key Perfect Forward Secrecy"

Authenticate and generate a new key after every: 60 minutes.

Click "Methods"

Make sure that "IKE 3DES MD5 medium (2)" is first on the list.

Click Ok

Click Ok

You should now be back to the connection properties.

Select the Rules tab.

Make sure "Use Add Wizard" is selected.

Click Add. This starts the Security Rule Wizard

Click Next

Select "The tunnel endpoint is specified by this IP address"

and enter the IP address of the W2000 server (in this example 192.168.50.3)

Click Next

Network type: All network connections

Click Next

In Authentication method select "Use this string to protect the key exchange (pre-shared key)", and enter the key (in this example: `secret`)

Click Next

In the IP filter list click Add, this starts an IP filter list window

Make sure "Use Add wizard is selected".

Click Add. This starts the IP filter wizard.

Click Next

IP traffic source: "A specific IP subnet"

Set the subnet to the first protected subnet (in this example 192.168.1.0/255.255.255.0)

Click Next

IP traffic destination: "A specific IP subnet"

Set the subnet to the second protected subnet (in this example 192.168.51.0/255.255.255.0)

Click Next

For IP protocol type select Any

Click next

Select "Edit properties"

Click Finished. This opens filter properties.
 Deselect "Mirrored"
 Click Apply
 Click Ok
 Give the IP filter list a name, e.g. Net1_to_Net51
 Click close
 Select the new IP filter from the IP filter list
 Click next
 In the filter Action menu select Add (make sure "Use Add Wizard" is selected)
 This launches the Filter Action Wizard
 Click Next
 Give the Filter a name, e.g. 3DES-MD5
 Click next
 Select Negotiate Security
 Click Next
 Select "Do not communicate with computers that do not support IPSec"
 Click Next
 Select custom and click on settings
 Select ESP, MD5 integrity algorithm and 3DES encryption algorithm
 Also select "Generate a new key every 28800 seconds"
 Click OK
 Click Next
 Select Edit Properties
 Click Finish
 In the filter action properties select "Session key Perfect Forward Secrecy"
 Click OK
 This takes you back to the Security Rule Wizard.
 Select here the newly created Filter Action (3DES-MD5)
 Click Next
 Select Edit Properties
 Click Finish
 Click OK in the properties
 You should now be back in the Security Policy Wizard.
 Another IP security rule should be added. This rule should be the "opposite" of the previous rule, i.e. define traffic the other way in the tunnel.
 Click Add
 Click Next
 Select "This tunnels endpoint is specified by its IP address" and enter the IP address of the InterJak server (in this example 192.168.50.1)
 Click Next
 Network type: All network connections
 Click Next
 In Authentication method select "Use this string to protect the key exchange (pre-shared key)", and enter the key (in this example: secret)
 Click Next
 In the IP filter list click Add, this starts an IP filter list window
 Make sure "Use Add wizard is selected".
 Click Add. This starts the IP filter wizard.
 Click Next
 IP traffic source: "A specific IP subnet"

Set the subnet to the second protected subnet (in this example
192.168.51.0/255.255.255.0)

Click next

IP traffic destination: "A specific IP subnet"

Set the subnet to the first protected subnet (in this example

192.168.1.0/255.255.255.0)

Click next

For IP protocol type select Any

Click next

Select "Edit properties"

Click Finished

Deselect "Mirrored"

Click Apply

Click Ok

Give the IP filter list a name, e.g. Net51_to_Net1

Click close

Select the new IP filter from the IP filter list

Click next

Select the Action that was defined previously from the filter action list (3DES-MD5)

Click Next

Select Edit Properties

Click Finish

Click OK in the properties

Click Close

You have now defined a new IPsec policy.

To enable it right-click on it and choose assign.

To edit it right click it and choose properties.

IPsec based VPN Configuration of InterJak - Dynamic

The following conditions must be fulfilled to create an IPsec based VPN tunnel between the InterJak and the remote device:

- IPsec based VPN capable devices at both ends of the tunnel.
- Static external public IP addresses at one end.
- Common shared secret (for all remote users) must be available at both ends.

The IPsec based VPN tunnel between two networks where only one network has a static endpoint address is configured using the **Services, VPN** and then **Dynamic VPN** command in the in InterJak Management Suite:

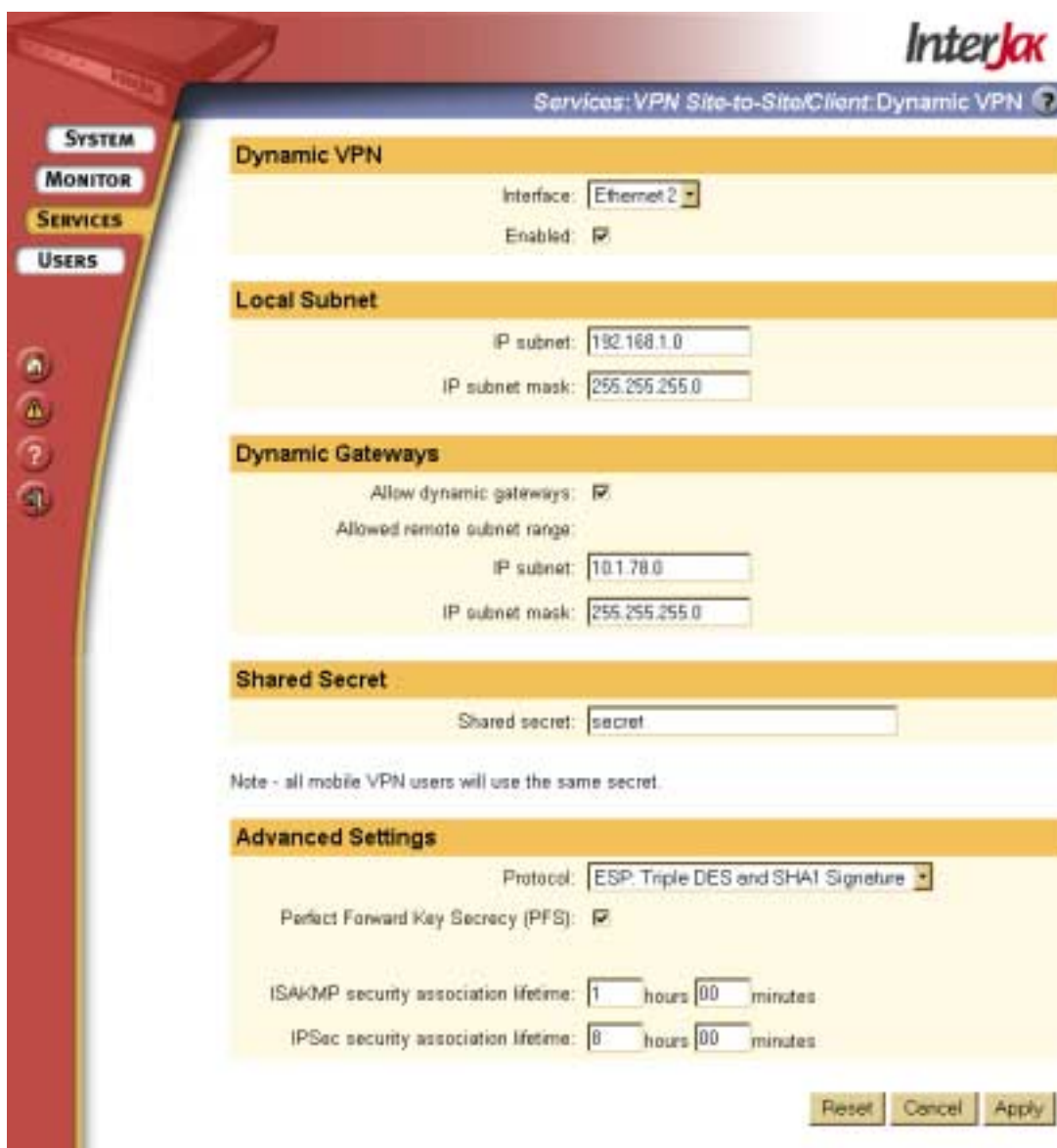
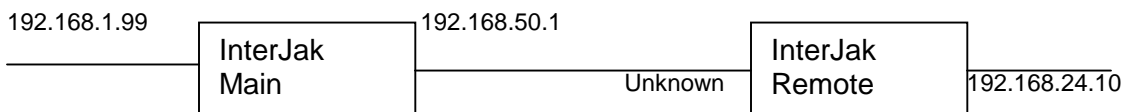


Figure 4: Site-to-Site VPN Configuration Screen (Dynamic)

InterJak Site-to-Site Connection with Unknown Remote Client Endpoint

The following is a simple example of a VPN tunnel between two InterJaks. The VPN tunnel was between subnets 192.168.1.0/255.255.255.0 and 192.168.24.0/255.255.255.0.

Schematic drawing of setup:



InterJak Main configuration

Enabled:	Selected
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Dynamic gateways	
Allow dynamic gateways	Selected
Allowed remote subnet range	
IP subnet	Empty
IP subnet mask	Empty
Shared Secret	
Shared secret:	dynamic_secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes

InterJak Remote configuration

Name:	InterJak Main
Remote end-point (IP or host name):	192.168.50.1
Enabled:	Selected
Local Subnet	
IP subnet:	192.168.24.0
IP subnet mask:	255.255.255.0
Remote Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Shared secret:	dynamic_secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes
Settings for NAT	
NAT Remote end-point:	<i>empty</i>

PPTP Based VPN Solution

PPTP is a network protocol that encapsulates PPP packets in IP datagrams for transmission over public TCP/IP networks, such as the Internet. PPTP is included with Microsoft Windows 95 (upgrade), 98, NT and 2000. PPTP clients are also available for other operating systems such as UNIX, Linux and Apple Macintosh. PPTP allows a client to connect to a private network as a remote access client. This enables the remote client to establish a confidential line of communication with the private network to access resources on the private network such as files servers, printers, mail servers etc. InterJak supports up to 8 simultaneous PPTP based VPN connections.

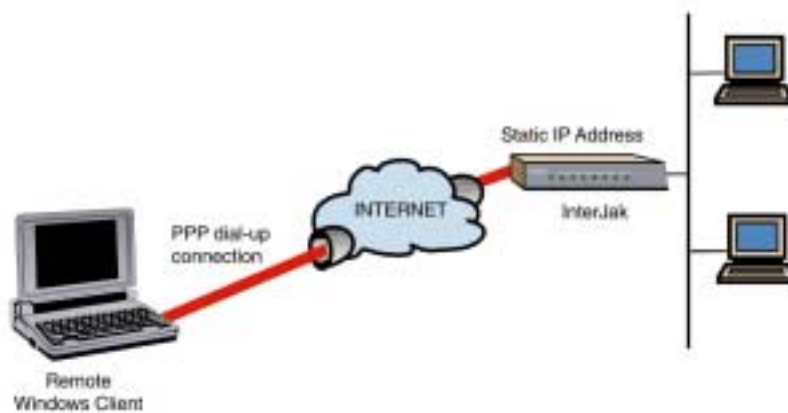


Figure 5: PPTP based Client-to-Site VPN Connection

An example of the use of PPTP could be that a client first establishes a standard PPP connection (typically a dial-up connection) to an Internet Service Provider (ISP) to gain access to the Internet. Through this dial-up connection, a PPTP connection is established which allows the client to connect to the InterJak, which acts as a PPTP server. Through the PPTP tunnel the client has now access to resources on the private LAN behind the InterJak as well as disks and printers connected directly to the InterJak. The data is encrypted and encapsulated before transmission.

PPTP based VPN Configuration of InterJak

Three things must be configured in order for the PPTP server on the InterJak to function correctly. The PPTP server itself must be configured, the firewall must be opened to allow PPTP traffic through and the users connecting via PPTP must be created.

The PPTP server configuration on the InterJak is performed through the **Services:VPN: Remote Access (PPTP)** page in the InterJak Management Suite as follows:



Figure 6: PPTP VPN Configuration Screen

Enter the following information to configure InterJak for PPTP based VPN connections:

- **Server IP base address:** This is one of the eight IP server addresses, which consists of a base address and the next 7 addresses.
- **Client IP base address:** This is one of the eight IP client addresses, which consists of a base address and the next 7 addresses.
- **Authentication:** Select authentication method. Note that encryption does not work with PAP and CHAP authentication.
- **Encryption:** Select the encryption method or No Encryption.
- Click **Apply** to save the above information.

When a client connects using PPTP, a part of the PPTP connection is a PPP tunnel. The endpoints of this tunnel get IP addresses from the “Server IP base address” and “Client IP base address”. However these addresses are not “exposed” to the public network carrying the PPTP tunnel, and can therefore fall in the so-called private address range. The addresses selected should however not conflict with other addresses on the LAN behind the InterJak.

Second the firewall must be opened to allow PPTP traffic through. This is a default setting on the InterJak, but can be configured from the **Services:Firewall:Firewall Setup** page.

Users must also be configured and allowed to be connected using PPTP to the InterJak. When connecting via PPTP the client is prompted for a user name and password. This username and password must be configured on the InterJak, using the **Users:Add User** page. Also the option “Allow remote access to local network using PPTP” must be enabled for the user.

PPTP based VPN Clients

PPTP users may access their office LAN from a home office or while traveling using a PPTP connection. PPTP based VPN client software is available with the following operating systems.

Windows 95 with PPTP upgrade
 Windows 98 with PPTP upgrade
 Windows 98 Second Edition
 Windows NT/4.0 with Service Pack 5 or higher
 Windows 2000 Professional
 Windows ME
 UNIX, Linux and Apple Macintosh

PPTP based Windows 98 SE Client

- In Windows, open the **Start** menu and choose **Settings** and then open **Control Panel**.
- Double-click on the **Add/Remove Programs** icon and then click on **Windows Setup** tab.
- Select the **Communication** icon in the **components** list and then click on the **Details** button to open the **Communications** window.
- Select the **Virtual Private Networking** item and mark the checkbox and then click **OK**.
- Windows now installs the required files and asks to reboot.

Now that the VPN adapter is available, dial-up networking account must be created that uses the VPN.

- Double-click on the **My Computer** icon on the Windows desktop to open **My Computer** window.
- Double-click on the **Dial-up Networking** window and then double click on the **Make New Connection** icon to create new VPN account.
- Type in the name for the connection and choose the **VPN Adapter** from the **Select a device** drop down list and then click **Next**.
- Enter the host name or IP address of the InterJak to which the connection is to be made. This must be the public IP address or name that InterJak uses on the port facing WAN.
- Click **Next** to see the final window summarizing the setting. Click **Finish** to create this account with a new icon in the Dial-up Networking.

Once the new account is established on the client computer, it may be necessary to configure the account to access the specific network that is being connected. Network

administrator should provide this information to be entered on the client computer. In order to customize any information to this VPN account, follow these steps:

- Right click on the VPN account icon in the **Dial-up Networking** window and choose **Properties** from the contextual menu that appears.
- Click on the **Server Types** tab and make settings that are required for the network or as specified by the network administrator.

Once the settings are entered, VPN account can be established from the client computer to the InterJak by first making the regular PPP connection to the ISP and then double-clicking on the VPN account icon in the **Dial-up Networking**.

PPTP based Windows NT 4.0 Client

- Log in to Windows NT as an administrator of the client PC.
- Open **Start** menu and choose **Settings** and open **Control Panel** window.
- Double-click on the **Network** icon to open the **Network** window and then click on the **Protocols** tab.
- Click on the **Add** button and **Select Network Protocol** window appears.
- Select **Point to Point Tunneling Protocol** item and click **OK**.
- A new window appears asking the number of virtual private networks. Leave this set to 1 and click on **OK**.
- A message appears to setup PPTP protocol. Click **OK** to proceed to the **Remote Access Setup** window and click **Add**. Choose **VPN2-RASPPTPM** from the drop-down list and click **OK** to return to the **Network** window. Click on the **Close** button. Several messages will appear. Dismiss each of them until reboot message appears.
- Reboot the system.
- Re-apply the latest Windows NT 4.0 Service Pack to make sure all the system components are fully up to date.

Now that the PPTP protocol has been added, create a dial-up networking account that uses PPTP for VPN as follows:

- Double-click on the **My Computer** icon on the Windows desktop to open **My Computer** window.
- Double-click on the **Dial-up Networking** window and then double click on the **Make New Connection** icon to create new VPN account.
- Click **New** button to open the **New Phonebook Entry Wizard** window.
- Type in a name for the phonebook entry in the field and click **Next**. The **Server** window appears.
- Mark **I am calling the Internet** checkbox and click on **Next**. The **Modem or Adapter** window appears.
- Choose the **RASPPRPM** entry and click on **Next**. This adds the VPN device and then **Phone Number** window appears.
- Instead of the phone number, enter the host name or IP address on the InterJak to which VPN connection is made. This must be public IP address or host name that the InterJak uses on the WAN port.

- Click **Next** and VPN connection is set.

PPTP based Windows 2000 Client: Dial-Up connection

- Log in to Windows 2000 as an administrator of the client PC.
- Open **Start** menu and choose **Settings** and open **Control Panel** window.
- Double-click on the **Network and dial-up connections** icon to open the **Network** window.
- Double-click on the **Make New Connection** icon, which opens the welcome screen.
- Click on **Next** to proceed to the **Network Connection Type** page.
- Select **Dial-up to private network** radio button and click on **Next** to open **Phone Number to Dial** window. Enter the phone number and click **Next** to open **Connection Availability** window.
- Enter the host name or IP address of the InterJak to which the client wants to connect. This must be the public address or host name that the InterJak uses on the port facing the WAN. Then click **Next** to open **Connection Availability** page.
- The setting on this page controls how many other users of the client machine will be able to use the VPN account. Choose **Only for myself** or **For all users** depending upon how the machine is to be used.
- Click **Next** to open **Internet Connection Sharing** page. Select **Enable Internet Connection Sharing for this connection**, if other computers on the network are to be accessed through this dial-up connection.
- Click **Next** to access the final wizard page. Type in the name of this dial-up VPN account and check **Add a shortcut to my desktop**. Click **Finish** to create the dial-up VPN account.
- Right click on the dial-up VPN account icon in the **Network and Dial-up Connections** window and click on **Properties**.
- Click on **Networking** tab and select **Internet Protocol (TCP/IP)**. Click **Properties** to open **General** window.
- Click **Advanced** in **General** window to open **Advanced TCP/IP setting** window. Click open **Options** tab and select **IP security** in the **Optional settings** window.
- Click **Properties** in the **Options** tab to open **IP security** window. Click radio button **Use the IP security policy**. And select one of the three security policy options and click **OK** to get back to the **Network and Dial-up Connection**.

Once the VPN account is established, double-click on the shortcut on the desktop or double-click on the VPN account in the **Network and Dial-up Connections** window and then follow steps to connect to the InterJak.

PPTP based Windows 2000 Client: DSL or Cable Modem connection

- Log in to Windows 2000 as an administrator of the client PC.
- Open **Start** menu and choose **Settings** and open **Control Panel** window.
- Double-click on the **Network and dial-up connections** icon to open the **Network** window.
- Double-click on the **Make New Connection** icon to open the welcome screen.
- Click on **Next** to proceed to the **Network Connection Type** page.
- Select **Connect to a private network through the Internet** radio button and click on **Next**. The **Destination Address** page appears.
- Enter the host name or IP address of the InterJak to which the client wants to connect. This must be the public address or host name that the InterJak uses on the port facing the WAN. Then click **Next** to open **Connection Availability** page.
- The setting on this page controls how many other users of the client machine will be able to use the VPN account. Choose **Only for myself** or **For all users** depending upon how the machine is to be used.
- Click **Next** to open **Internet Connection Sharing** page. Select **Enable Internet Connection Sharing for this connection**, if other computers on the network are to be accessed through this dial-up connection.
- Click **Next** to access the final wizard page. Type in the name of this VPN account and check **Add a shortcut to my desktop**. Click **Finish** to create the VPN account.
- Right click on the VPN account icon in the **Network and Dial-up Connections** window and click on **Properties**.
- Click on **Networking** tab and select **Internet Protocol (TCP/IP)**. Click **Properties** to open **General** window.
- Click **Advanced** in **General** window to open **Advanced TCP/IP setting** window. Click open **Options** tab and select **IP security** in the **Optional settings**.
- Click **Properties** in the **Options** tab to open **IP security** window. Click radio button **Use the IP security policy**. And select one of the three security policy options and click **OK** to get back to the **Network and Dial-up Connection**.

Once the VPN account is established, double-click on the shortcut on the desktop or double-click on the VPN account in the **Network and Dial-up Connections** window and then follow steps to connect to the InterJak.

Site-to-Client VPN Solution

The third option available with the InterJak is Site-to-Client VPN for mobile clients based on IPsec protocol (also known as Dynamic VPN). This solution is similar to the Site-to-Site IPsec VPN solution except that the IP address of the mobile client does not have to be set in the InterJak configuration. The connection is instead initiated by the client, when the client needs access to the InterJak. Up to 4 simultaneous Site-to-Client connections are supported.

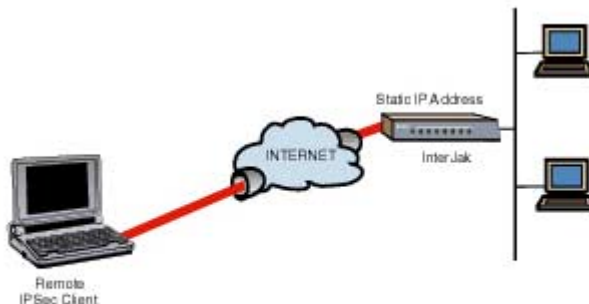


Figure 7: Site-to-Client VPN Connection

Site-to-Client VPN Configuration of InterJak

The following conditions must be fulfilled to create an IPsec VPN tunnel between the InterJak and the remote device:

- The client computer must have IPsec client software installed on it.
- A shared secret must be available at both ends. This is used for authentication and must be sent using a secure medium.

Dynamic VPN is configured using the **Services: VPN Site-to-Site/Client (IPsec):Dynamic VPN**.

- WAN interface for the VPN connection
- Checkbox to enable the VPN connection
- Local IP Address and subnet mask (the subnet the VPN client will access)
- Shared secret
- Encryption Protocol
- Perfect Forward Key Secrecy (PFS)
- Lifetimes of the IPsec and ISAKMP SA
- Click **Apply** to save the above information.

The screenshot displays the 'Services: VPN Site-to-Site/Client: Dynamic VPN' configuration page. On the left is a navigation sidebar with buttons for SYSTEM, MONITOR, SERVICES (highlighted), and USERS, along with status icons. The main content area is divided into several sections:

- Dynamic VPN:** Interface: Ethernet 2 (dropdown), Enabled:
- Local Subnet:** IP subnet: 192.168.1.0, IP subnet mask: 255.255.255.0
- Dynamic Gateways:** Allow dynamic gateways: . Allowed remote subnet range: IP subnet: 10.1.78.0, IP subnet mask: 255.255.255.0
- Shared Secret:** Shared secret: secret
- Note:** all mobile VPN users will use the same secret.
- Advanced Settings:** Protocol: ESP: Triple DES and SHA1 Signature (dropdown), Perfect Forward Key Secrecy (PFS): . ISAKMP security association lifetime: 1 hours 00 minutes. IPSec security association lifetime: 0 hours 00 minutes.

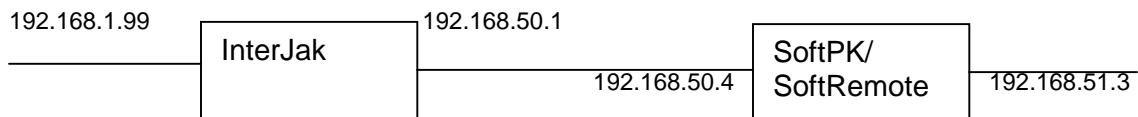
At the bottom right are buttons for Reset, Cancel, and Apply.

Figure 8: Site-to-Client VPN Configuration Screen

IPsec based Clients

SafeNet's Soft-PK or SoftRemote Client

SafeNet's Soft-PK (formerly IRE) is a client for Windows 98 that can be used with the InterJak as a so-called mobile VPN client. SafeNet's SoftRemote Client is a client for Windows 98 and Windows 2000 that can be used with the InterJak as a so-called mobile VPN client. Below is an example configuration for these clients (the setup is the same for both).



InterJak configuration

Enabled:	Yes
Local Subnet	
IP subnet:	192.168.1.0
IP subnet mask:	255.255.255.0
Dynamic gateways	
Allow dynamic gateways	<i>Not selected</i>
Allowed remote subnet range	
IP subnet	<i>Empty</i>
IP subnet mask	<i>Empty</i>
Shared Secret	
Shared secret:	mobile_secret
Advanced Settings	
Protocol:	ESP: Triple DES and MD5 Signature
Perfect Forward Secrecy (PFS):	Yes
ISAKMP security association lifetime:	1 hours 00 minutes
IPSec security association lifetime:	8 hours 00 minutes

IRE SafeNet/SoftPK Client Configuration

In Windows start the Policy Editor from the Start menu: Start -> Programs -> SafeNet Soft-PK -> Security Policy Editor.

Click the "New Connection" icon, and give a name for the connection. E.g. InterJak.

Select the new connection, and set the following properties:

Connection Security: Secure

Remote Party Identity and Addressing: Select IP Subnet

ID Type: IP Subnet

Subnet: 192.168.1.0

Mask: 255.255.255.0

Protocol: All

Select "Connect using Secure Gateway Tunnel"

ID Type: IP Address

The IP address should be set to the address of the InterJak: 192.168.50.1

Expand the properties of the connection.

Select "My Identity", and set the following properties:

Select Certificate: None

IP Type: IP address

Port: Select All

Local Network Interface: *Select the interface that the Windows PC uses to reach the network*

Click on "Pre-Shared key" and enter the pre-shared key (in this example:

mobile_secret)

Select "Security Policy", and set the following properties:

Phase 1 negotiation: Main mode

Perfect Forward Secrecy: Enabled

PFS Key Group: Diffie-Hellman Group 2

Enable Replay Protection: Enabled

Expand "Security Policy"

Expand "Authentication (Phase 1)"

Select "Proposal 1" and set the following properties: Authentication: Pre-shared key

Encrypt Alg: Triple DES

Hash Alg: MD5

SA Life: Seconds - 3600

Key Group: Diffie-Hellman Group 2

Expand "Key Exchange"

Select "Proposal 1" and set the following properties:

SA Life: Seconds - 28800

Compression: None

Encapsulation Protocol: Selected

Encrypt Alg: Triple DES

Hash Alg: MD5

Save the properties by clicking on the Save-icon.

The connection can be tested by pinging the "inside" of the InterJak (192.168.1.99).