

# InterJak Technical Brief

## Wireless Broadband Security

**Filanet Corporation**  
757 N. Pastoria Avenue  
Sunnyvale, CA 94087  
408.331.2900

Filanet Europe ApS  
Herlev Hovedgade 82c, 1  
2730 Herlev, Denmark  
+45 44 50 37 70

[www.filanet.com](http://www.filanet.com)

---

## Table of Contents

Introduction.....	3
Table of Contents.....	2
InterJak 200 802.11b Wireless Applications .....	4
Wireless Broadband Security Issues.....	5
InterJak 200 802.11b Wireless Broadband Security Options .....	6
Securing InterJak Management Interface .....	6
SSID and Closed Network Option.....	8
Interface Isolation and Firewall Protection.....	8
VPN (IPSec) Protection .....	9
WEP and Key Management.....	12
For Further Information .....	13

## ***InterJak 200 802.11b Wireless Broadband Security***




---

### **Introduction**

This technical brief provides information on wireless broadband security options available with the InterJak 200 802.11b product.

For general information on the InterJak Service Appliance product line, and services available, please see the main Filanet web site at <http://www.filanet.com>. For access to the *InterJak Technical Reference Manual* and other application notes, please see the Filanet support section at <http://www.filanet.com/support>.

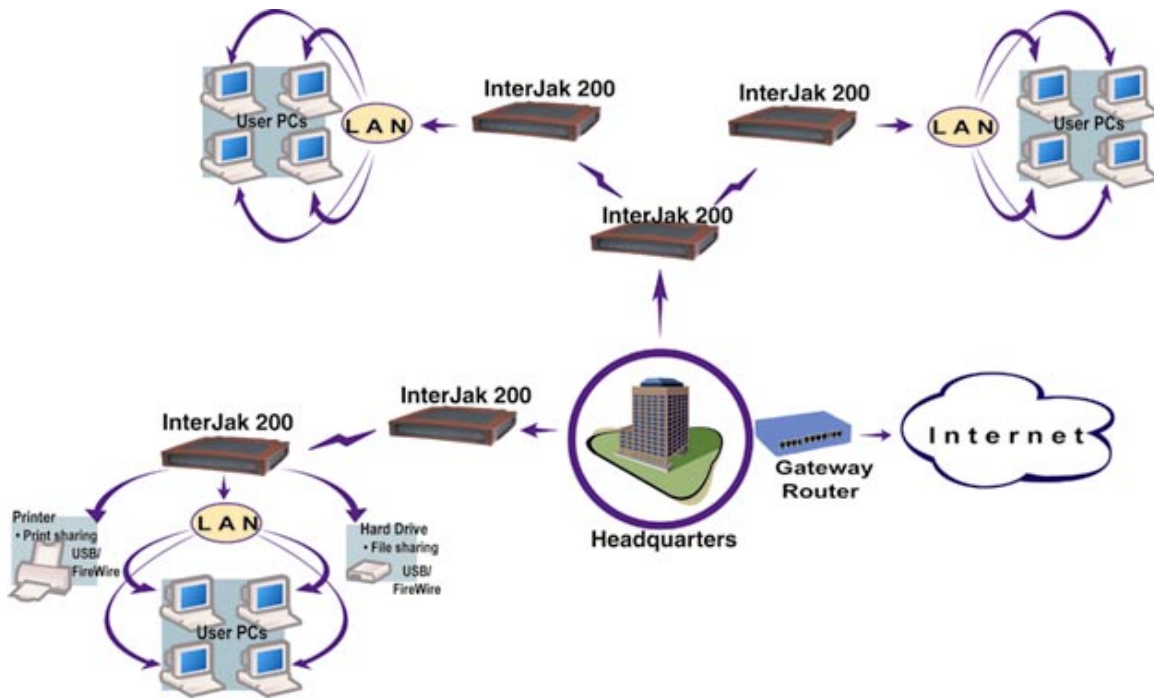
**InterJak 200 802.11b Wireless Applications**

The InterJak 200 802.11b contains a built-in 802.11b wireless interface, a simple external antenna, and supports connection to a variety of specialized external antennas and amplifiers for use in long distance wireless links. It supports two routable Ethernet interfaces for connection to headquarters infrastructure or end customer premises equipment. Depending upon the antennas used, and a number of other factors, distances of up to 20 miles for point-to-point and point-to-multipoint links are possible.

The InterJak 200 802.11b performs wireless router and gateway functions. This design allows for integrated networking services such as firewall, network address translation, file/print sharing, VPN (virtual private networking), and DHCP server. It also allows isolation of the wireless segment, both filtering unneeded IP traffic and securing the local wired segment (Figure 1).

The InterJak 200 802.11b is based on the IEEE 802.11b 2.4 GHz high-rate wireless networking standard (11 Mbps, with adaptive rate control), and uses Direct Sequence Spread Spectrum (DSSS) CSMA/CA with ACK (and RTS/CTS) for signaling and collision avoidance. The InterJak supports BSS access point, BSS station, and IBSS ad-hoc modes of operation, for configuration flexibility. The combination of flexible firewall, independent DMZ segment, and optional VPN service provides a number of wireless security options for wireless broadband applications.

For additional information on services available on the InterJak 200 802.11b and background on the InterJak in wireless broadband applications, please see the *InterJak 200 802.11b Wireless Broadband Technical Brief* at <http://www.filanet.com/support>.



**Figure 1: InterJak 200 802.11b Wireless Broadband Application**

---

## Wireless Broadband Security Issues

WEP (wired equivalent privacy) was developed for the 802.11 standard to offer basic access control, confidentiality, and data integrity for a wireless infrastructure. WEP is a popular mechanism for securing wireless broadband links. However, recently discovered shared secret and RC4 vulnerabilities in WEP have made it weak as a security mechanism.

In addition, there is no defined key management protocol, so WEP keys must be manually entered into each wireless router or access point individually. This is a large management task, complicated by the need to periodically change these WEP keys to provide some level of security.

**Note:** The InterJak 200 802.11b supports 64-bit and 128-bit WEP, and supports a method of securely distributing WEP keys (3DES encrypted key distribution) through the InterJak Service Provisioning Portal (SPP) or TFTP. These mechanisms may be used to periodically change WEP keys system-wide to help ensure a secure wireless broadband infrastructure.

MAC (media access control) filtering is another method used to attempt to secure a wireless broadband link. Unfortunately, it is extremely easy to spoof MAC addresses to obtain access to a wireless network. Also, management and maintenance of MAC addresses for wireless routers and access points is labor-intensive.

SSIDs (service set identifiers) are sometimes used as a simple shared password for access control of wireless broadband links. This can be used with special “closed network” options on wireless routers to prevent association from stations configured with SSIDs set to “ANY”, while also making it more difficult for wireless “war driving” access point detection programs. However, the SSID is shared, and it is possible with some effort to sniff traffic to determine a wireless network’s SSID.

**Note:** The InterJak 200 802.11b supports a “closed network” option, which protects the wireless broadband connection from being detected easily, prevents association from other wireless equipment using the “ANY” SSID, and disables the InterJak from broadcasting its own SSID.

A large number of articles and reports have been written on the current vulnerabilities of wireless LAN networks. Some of these vulnerabilities also apply to wireless broadband links.

There are several known types of wireless attacks that must be protected against:

- SSID (network name) sniffing
- WEP encryption key recovery attacks
- ARP poisoning (“man in the middle attacks”)
- MAC address spoofing
- Access Point management password and SNMP attacks
- Wireless end user (station) attacks
- Rogue AP attacks (AP impersonation)
- DOS (denial of service) wireless attacks

---

## Wireless Security Recommendations

For wireless broadband links, there are three areas of security to be concerned with.

**Confidentiality:** Eavesdropping of data on the wireless link must be avoided in some situations. Data targeted at (or across) the Internet requiring confidentiality should be protected with end-to-end encryption, not simply encryption across the wireless link. If the wireless link connects buildings or sites together, and is expected to handle internal company traffic, then confidentiality is crucial.

**Access Control:** Both the wireless and wired infrastructure must be protected against access from unauthorized users. A secure authentication and access control mechanism is necessary.

**Data Integrity:** A method to prevent tampering with transmitted messages on the wireless infrastructure is necessary. Again, if the data is targeted at the Internet, then end-to-end data integrity must be considered, not simply protection of the wireless link itself.

Following are a number of general security recommendations when implementing a wireless broadband infrastructure:

- **Secure wireless equipment and SNMP management:** Do not allow wireless router or access point management (web, telnet, or SNMP based) from the wireless interface. If this must be allowed, protect the management interface with a strong password and ensure that all management communication to the access point is securely authenticated and encrypted. **Note:** The InterJak provides an encrypted web management interface for remote management and monitoring.
- **Change SSID from default value, and use closed network options:** Do not leave the SSID (wireless network name) at its default value, and do not use an SSID that is easily guessed. Enable any closed network options (for preventing broadcast of SSID, etc.) to help prevent casual snoopers from detecting the wireless network. **Note:** The InterJak supports a closed wireless network option.
- **If using WEP, change keys often:** Key management can be difficult, but key changing must be done if running WEP. **Note:** The InterJak can provide coordinated secure WEP key management through its Service Provisioning Portal service or automatic TFTP based updates.
- **Isolate wireless network from wired network:** Completely isolate the wireless broadband link from the wired infrastructure through use of an independent wireless segment (do not use wireless bridges). This helps prevent several types of intrusion and denial of service attacks aimed at the wired infrastructure. **Note:** The InterJak provides the ability to assign logical roles to each physical interface, and provides interface isolation.
- **Protect wired network from the wireless broadband link with a firewall:** In addition to isolating the wireless segment, use of well thought-out firewall rules can control the type of traffic allowed from the wireless segment to the wired segment. **Note:** The InterJak provides a highly configurable firewall, as well as an optional intrusion detection service.
- **Use VPN (IPSec) tunnels across wireless links:** For best protection, allow only VPN (IPSec) tunnels through the firewalls at the headquarters and customer premises, and over the wireless links. VPN tunnels allow for secure authentication, encryption, integrity, and can provide transparent access to wired network resources.

---

## InterJak 200 802.11b Wireless Broadband Security Options

The InterJak 200 802.11b supports several levels of security, allowing for isolation and protection from both the Internet and unauthorized wireless access. Two independent Fast Ethernet interfaces and an independent wireless interface provide flexible deployment options. A highly configurable firewall, and the ability to classify interfaces as LAN, WAN, or DMZ segments allow protection in a variety of ways.

Also available are extended services supporting VPN (IPSec and PPTP) tunnels from either remote locations or from internal wireless clients, traffic shaping and network monitoring to provision and monitor network usage, and intrusion detection to help discover attacks from the Internet or wireless broadband link.

A secure encrypted web management interface is available for both local and remote configuration and management of the InterJak 200 802.11b. A Service Provisioning Portal (SPP) is also available to securely monitor, manage, and configure large numbers of InterJak devices (for large-scale deployments).

---

## Securing InterJak Management Interface

It is possible to securely manage and monitor the InterJak 200 802.11b remotely. This remote management might occur across a wireless link from a central infrastructure, or might occur across the

Internet. In either case, it is important to properly secure the management and monitoring interfaces on the InterJak.

The InterJak 200 802.11b supports several methods of management and monitoring. These include:

- 3DES encrypted web management interface
- Encrypted Service Provisioning Portal (SPP) management server
- TFTP of encrypted InterJak configuration file
- Command Line Interface (CLI)
- System log local, remote, telnet, and e-mail logging
- SNMP monitoring with traps

Please see the *InterJak Technical Reference Manual* for more information on these management and monitoring interfaces.

Normally, for wireless point-to-point or point-to-multipoint configurations, the InterJak 200 802.11b wireless interface will be configured as a WAN interface. This allows the firewall to protect access to both the internal wired networks and the InterJak itself. The firewall may then be further configured to allow access to particular internal networks and to the InterJak management services.

To configure the InterJak wireless port as a WAN interface type through the InterJak web management interface, select *System:Networking:Wireless 1*, select Interface Type of *WAN*, and click *Apply*.

From the InterJak firewall page, it is possible to open the firewall to allow secure remote web management of the InterJak. This may be enabled under *Services:Firewall*, clicking on *Edit* under Firewall Setup, selecting the *Allow WAN access to web management* checkbox, and clicking *Apply*. This allows remote management of the InterJak via a 3DES encrypted web management interface. The log-in to this web management interface is protected with an administrator, power user, or standard user name and password.

It is further possible to change the web management port from the default of TCP port 80, and limit access to the InterJak web management interface via more restrictive firewall rules. For example, perform the following steps to change the default web management port to 1234 and restrict access to a particular management source IP address.

- From the InterJak web management interface, click on *System:Management* and under *Web management server (HTTP TCP) port number*, replace the default of 80 with 1234, and click *Apply*.
- You will then need to log in again to the InterJak web management interface via this new management port number (e.g. `http://interjak:1234`).
- Under *Services:Firewall*, click on *Add Service*. Under *Name* enter “Alternate Web Management”, under *First Traffic Definition* click on *Enabled*, select *Protocol* of TCP, enter *Destination Port* of 1234, and click on *Apply*. This adds a firewall service definition for this alternate web management port.
- Under *Services:Firewall*, now click on *Add Rule* to add a more restrictive firewall rule.

<i>Firewall Service: Alternate Web Management</i>
<i>Source IP Address/Mask: “remote management IP address”/255.255.255.255</i>
<i>Destination IP Address/Mask: 0.0.0.0/0.0.0.0 (all destinations)</i>
<i>Action: ACCEPT</i>
<i>Chain: WAN to box</i>
<i>Log: No</i>

- Finally, under *Services:Firewall* click on *Edit* under *Firewall Setup*, deselect the *Allow WAN access to web management* checkbox, and click *Apply*. This removes the original WAN management firewall rule, allowing your new more restrictive alternative web management rule to take affect.

SNMP (read-only) support is built into the InterJak for local and remote monitoring. In its default configuration, the InterJak does not allow remote SNMP monitoring from the WAN through the

firewall. In order to enable restricted remote monitoring from a particular management source IP address, perform the following steps:

- Under *Services:Firewall*, now click on *Add Rule* to open the firewall for SNMP access (from a particular remote IP address).

<i>Firewall Service: SNMP</i>
<i>Source IP Address/Mask: "remote management IP address"/255.255.255.255</i>
<i>Destination IP Address/Mask: 0.0.0.0/0.0.0.0 (all destinations)</i>
<i>Action: ACCEPT</i>
<i>Chain: WAN to box</i>
<i>Log: No</i>

- Under *Monitor:SNMP*, enter the following to enable SNMP monitoring and traps.

<i>Enabled: Yes</i>
<i>Community name: "something secure"</i>
<i>Administrator must use fixed IP address range: Yes</i>
<i>Restricted access IP address/mask: "remote management IP address"/255.255.255.255</i>
<i>Note: Enable SNMP traps if desired along with a receiver IP address or host name.</i>

In addition to the Filanet encrypted web management interface and Service Provisioning Portal (SPP), the InterJak 200 802.11b may be managed and monitored through remote telnet sessions. Because all data is sent in clear text, remote telnet sessions across the WAN should be run on top of a VPN (PPTP or IPSec) tunnel. The InterJak supports VPN (PPTP or IPSec) as part of the InterJak optional VPN Service.

For additional information on InterJak monitoring and management through use of telnet sessions, and creation of VPN tunnels to the InterJak, please see the *InterJak Technical Reference Manual*.

---

## SSID and Closed Network Option

In order to secure wireless broadband links an important first step is to make automatic detection/discovery of the wireless network or link more difficult.

This can be done by changing the InterJak SSID (wireless network name) from its default value to something which is unique. Also important is enabling the closed wireless network option. This disables the broadcast of the configured InterJak SSID (wireless network name).

The InterJak SSID (network name) and closed wireless network options may be configured from the InterJak web management interface under *System:Networking:Wireless 1*.

---

## Interface Isolation and Firewall Protection

In addition to basic security recommendations listed earlier, it is possible to use the integrated firewall on the InterJak 200 802.11b to support both security of the wireless broadband link, as well as wired security at the headquarters infrastructure and end customer premises.

The InterJak allows basic firewall configuration to be managed by defining logical roles for each physical interface. For example, the wireless interface may be configured as a logical WAN or DMZ to enable firewall protection. Simple checkbox configuration settings are available to allow services such as remote web management, RADIUS server administration, VPN (IPSec or PPTP), SMTP, DNS, etc.

It is also possible to easily add sophisticated firewall rules to protect the InterJak itself, filter certain types of traffic, or filter particular source or destination IP addresses (or ranges) through the firewall. For example, the InterJak 200 802.11b at the customer premises may be configured to protect the local wired LAN from both unauthorized access on the wireless broadband link or the Internet. The InterJak

200 802.11b at the infrastructure may be configured to only allow traffic to or from the authorized IP subnet assigned to the end customer, protecting the infrastructure from unauthorized access. For a detailed example of how to configure the InterJak firewall to protect wired networks on either side of a wireless broadband link, please see the *InterJak 200 802.11b Wireless Broadband Technical Brief* at <http://www.filanet.com/support>. For background on the advanced features of the InterJak Firewall Service, please refer to the *InterJak Technical Reference Manual*.

**Note:** The InterJak offers a special Test Configuration Mode, allowing the InterJak administrator to more safely make wireless, firewall, WEP, or other changes from a remote location. After testing out the changes, the administrator would then “commit” the new configuration to the InterJak. If the process of making configuration changes results in the InterJak losing remote connectivity (e.g. adding incorrect firewall rules), the InterJak will revert to the original configuration after a 10 minute timeout period. For additional information on this feature, please see the *InterJak Technical Reference Manual*.

### VPN (IPSec) Protection

The InterJak 200 802.11b supports an optional VPN service, allowing secure tunnels across the Internet between remote sites, or between two or more InterJak devices across wireless broadband links.

VPNs are already used widely for intranets and remote access. The combination of VPN and 802.11 is an ideal solution for today’s wireless networking needs. With the InterJak VPN service, the wireless VPN handles security across the wireless broadband link. The VPN service provides encapsulation, authentication, and full encryption over the wireless broadband link.

The InterJak supports both IPSec and PPTP VPN connections. IPSec (Internet Protocol Security) is a widely used mechanism for securing VPN traffic. IPSec is most often used with 3DES for encrypting data, and MD5 for authenticating packets.

Figure 2 shows an example wireless broadband link where an IPSec VPN tunnel is used to authenticate and secure traffic over the wireless link.

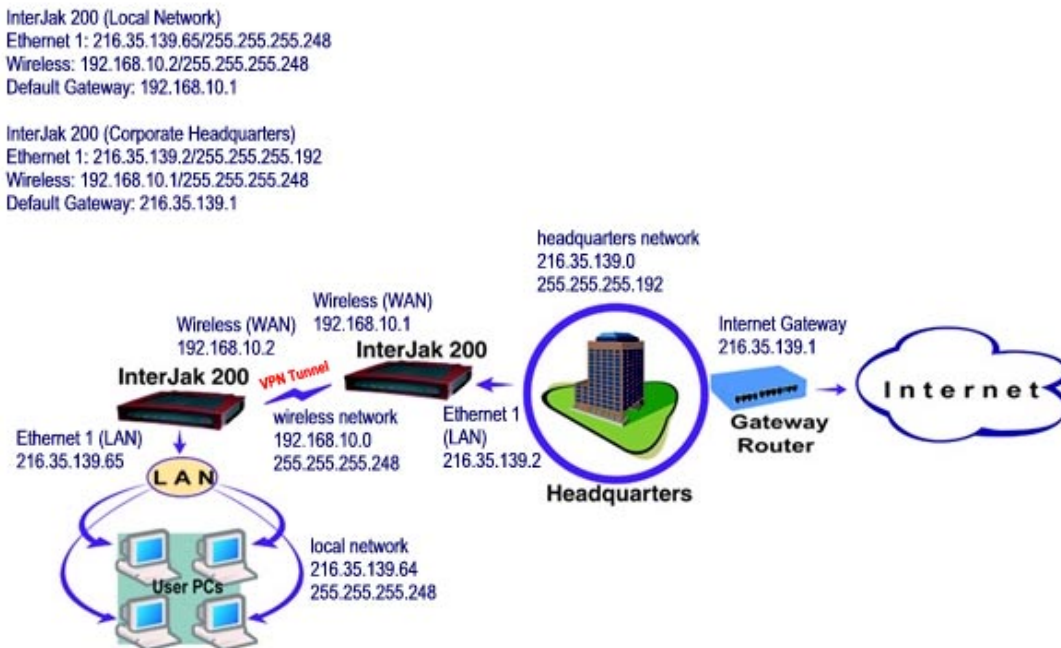


Figure 2: InterJak 200 802.11b with VPN Tunnel over Wireless Link

Depending upon security and performance requirements for the wireless link, varying IPSec options may be used for the VPN site-to-site tunnel.

Authentication Requirements (shared secret)	Data Integrity Requirements (signature)	Privacy Requirements (encryption)	Performance Requirements (bandwidth)	Recommendations
Low	Low	Low	High	Change SSID, enable closed wireless network option, and use firewall rules to protect wired networks. VPN tunnel not necessary.
High	High	Low	High	Change SSID, use closed wireless network, enable firewall. Enable VPN site-to-site using IPSec <i>ESP:No encryption:MD5 Signature</i> or <i>AH:MD5 Signature</i>
High	High	Medium	Medium	Change SSID, use closed wireless network, enable firewall. Enable VPN site-to-site using IPSec <i>ESP:Single DES:MD5 Signature</i>
High	High	High	Low	Change SSID, use closed wireless network, enable firewall. Enable VPN site-to-site using IPSec <i>ESP:Triple DES:MD5 Signature</i>

The following configuration steps are performed to enable a VPN (IPSec) tunnel over the wireless broadband link described in the example above (figure 2).

**1) Configure Internet Gateway Router with route to remote LAN network**

- Add a route to remote LAN network 216.35.139.64/255.255.255.248

<i>Network Address: 216.35.139.64</i>
<i>Network Mask: 255.255.255.248</i>
<i>Gateway: 216.35.139.2</i>

**2) Configure basic settings on InterJak 200 at local network**

- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and ensure that both NAPT options are disabled (in this configuration both InterJaks are used as pure routers).
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

<i>Enable: yes</i>
<i>IP address assignment: Manual</i>
<i>IP address: 216.35.139.65</i>
<i>Subnet mask: 255.255.255.248 (net of 8)</i>
<i>Enable DHCP server: yes</i>
<i>Allow direct IP: yes</i>
<i>Interface Type: LAN</i>

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

<i>Enable button: yes</i>
<i>Operation Mode: Infrastructure Station</i>
<i>Network name: InterJakVPN (or any other unique text)</i>
<i>Channel number: 6 (or any other unused wireless channel number)</i>
<i>IP address assignment: Manual</i>
<i>IP address: 192.168.10.2</i>
<i>Subnet mask: 255.255.255.248 (net of 8)</i>
<i>Enable DHCP server: no</i>
<i>Allow direct IP: yes</i>
<i>Interface Type: WAN</i>

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 192.168.10.1.

**3) Configure VPN settings on InterJak 200 at local network**

- Under *Services:VPN Site-to-Site/Client (IPSec)*, click on *Add Connection*, enter the following information, and click *Apply*:

<i>Name: WirelessVPN (or something appropriate)</i>
<i>Remote end-point (IP or host name): 192.168.10.1</i>
<i>Interface: Wireless 1</i>
<i>Enabled: yes</i>
<i>Local Subnet: 216.35.139.64/255.255.255.248</i>
<i>Remote Subnet: 0.0.0.0/0.0.0.0 (all traffic)</i>
<i>Shared secret: WirelessVPN (or any other unique text)</i>
<i>Protocol: ESP:No Encryption, MD5 Signature or AH:MD5 Signature (for best performance), or ESP:Single DES and MD5 Signature (for good performance), or ESP:Triple DES and MD5 Signature (for strongest security at expense of performance).</i>
<i>Perfect Forward Secrecy (PFS): yes</i>

#### 4) Configure basic settings on InterJak 200 at headquarters

- Under *Services:Address Translation (NAT/NAPT)*, click on *Edit* and ensure that both NAPT options are disabled (in this configuration both InterJaks are used as pure routers).
- Under *Services:Networking:Ethernet 1*, choose the following settings and then click *Apply*:

<i>Enable: yes</i>
<i>IP address assignment: Manual</i>
<i>IP address: 216.35.139.2</i>
<i>Subnet mask: 255.255.255.192 (net of 64)</i>
<i>Enable DHCP server: no</i>
<i>Allow direct IP: yes</i>
<i>Interface Type: LAN</i>

- Under *Services:Networking:Wireless 1*, choose the following settings and then click *Apply*:

<i>Enable button: yes</i>
<i>Operation Mode: Infrastructure Access Point</i>
<i>Network name: InterJakVPN (or any other unique text)</i>
<i>Channel number: 6 (or any other unused wireless channel number)</i>
<i>IP address assignment: Manual</i>
<i>IP address: 192.168.10.1</i>
<i>Subnet mask: 255.255.255.248 (net of 8)</i>
<i>Enable DHCP server: no</i>
<i>Allow direct IP: yes</i>
<i>Interface Type: WAN</i>

- Under *System:Routing*, under *Default Gateway*, click on *Edit*, and enter the *Gateway address* of 216.35.139.1 (Internet Gateway Router).

#### 5) Configure VPN settings on InterJak 200 at headquarters

- Under *Services:VPN Site-to-Site/Client (IPSec)*, click on *Add Connection*, enter the following information, and click *Apply*:

<i>Name: WirelessVPN (or something appropriate)</i>
<i>Remote end-point (IP or host name): 192.168.10.2</i>
<i>Interface: Wireless 1</i>
<i>Enabled: yes</i>
<i>Local Subnet: 0.0.0.0/0.0.0.0</i>
<i>Remote Subnet: 216.35.139.64/255.255.255.248</i>
<i>Shared secret: WirelessVPN (or any other unique text)</i>

*Protocol: ESP:No Encryption, MD5 Signature or AH:MD5 Signature (for best performance), or ESP:Single DES and MD5 Signature (for good performance), or ESP:Triple DES and MD5 Signature (for strongest security at expense of performance).*

*Perfect Forward Secrecy (PFS): yes*

The InterJak VPN Service will automatically create proper routes over the VPN tunnel, and these may be viewed under *System:Routing*, and clicking on the *Show Routing Table* button. To check the status of the VPN tunnel created over the wireless link, go to *Services:VPN Site-to-Site/Client (IPSec)* and look under *VPN Connection List*. For additional information on the InterJak VPN Service, please see the *InterJak Technical Reference Manual* and VPN Application Notes (available at <http://www.filanet.com/support>).

---

## WEP and Key Management

The InterJak 200 802.11b supports both 64 and 128-bit WEP. Recently discovered shared secret and RC4 vulnerabilities in WEP have made it somewhat weak as a security mechanism. WEP can, however, serve as an effective security means when used with a periodic WEP key rotation scheme and other security mechanisms.

When higher levels of security for a wireless link are desired or a periodic key rotation scheme is not practical for an installation, then use of the InterJak VPN Service is an extremely secure option. Please see the previous section on *VPN (IPSec) Protection* in this technical brief for details on this support. The InterJak supports manual and automated remote WEP key management and rotation through a variety of mechanisms, including:

- 3DES encrypted web management interface (manual)
- Encrypted Service Provisioning Portal (SPP) management server (manual or automated)
- TFTP of encrypted InterJak configuration file (manual or automated)
- Telnet Command Line Interface (manual or automated)

It is possible to select 64 or 128-bit WEP, choose up to four WEP keys, and designate the current default WEP key on the InterJak. The basic idea behind configuring four WEP keys and one default WEP key is to allow for key rotation schemes. The InterJak 200 802.11b will always use the current default WEP key for encoding packets, but will match any received packets against the appropriate WEP key configured (of the four entered).

For example, the following basic procedure may be followed to manually rotate keys (for InterJak 1 and InterJak 2 on either end of a wireless link):

1. Initially configure the first four keys on each InterJak with matching values, select 64 or 128-bit WEP, and set the default key on each InterJak to key 1. Each InterJak will now use the key 1 value for encoding packets for transmit, and will match each received packet against key 1.
2. Change the default key on InterJak 1 to key 2. Now, InterJak 1 will send packets using key 2, but will match packets received from InterJak 2 against key 1.
3. Change the default key on InterJak 2 to key 2. Now, InterJak 2 will also send packets using key 2.
4. After a rotation period (perhaps a week), change the 64 or 128 bit key 3 value on InterJak 1 to a new unique value. Follow this by doing the same (with the same new key 3 value) on InterJak 2.
5. Change the default key on InterJak 1 to key 3. Do the same for InterJak 2. You have now just rotated WEP keys.
6. After a rotation period (perhaps a week), continue with this process with key 4, and then start over again at key 1.

**Note:** Changing keys manually through the InterJak web management interface is secure as all data is 3DES encrypted on top of the WEP encryption.

A more automated method of rotating WEP keys among a large number of deployed InterJaks may be done through use of encrypted/signed InterJak partial config files and either a TFTP server or the Filanet Service Provisioning Portal (SPP). For more information on using these services, please refer to the *InterJak Technical Reference Manual*.

Rotating keys with InterJak config files may be done via a two step process (with either a TFTP server or Filanet SPP automating the update of InterJaks in the field).

1. Change an alternate WEP key in an InterJak partial config file to be updated to all InterJaks in the field. An alternate WEP key is defined as a key that is not currently set as the current default key. Following is an example config file for changing key 2 (assuming that key 1 is the current default key).

```
[ :wlan0]
  key2=12:34:56:ab:cb
```

This file must be encrypted/signed using the InterJak Administrator Client and may then be used to update InterJaks in the field using a TFTP server or Filanet SPP. Please see the section *Maintaining the Configuration File* in the *InterJak Technical Reference Manual* for details.

2. Change the default key on InterJak 1 to the new alternate WEP key you just updated. Following is an example config file for changing the default WEP key to key 2.

```
[ :wlan0]
  default key=key2
```

Again, this file must be encrypted/signed using the InterJak Administrator Client before it can be used with a TFTP server or Filanet SPP. Alternatively, these partial config files may be loaded in unencrypted form manually through the InterJak web management interface under *Maintenance:Transfer Configuration File or User Database to InterJak*.

It is critical that all InterJaks are updated with the new WEP key (step 1) before changing the default key to this new WEP key (step 2). It might be wise to space WEP key updates and default key changes by one or more days to ensure that all key updates are propagated via TFTP updates or SPP.

**Note:** Proper support for WEP on the InterJak requires InterJak 200 802.11b models which use a fully integrated wireless interface. Models of the InterJak 200 802.11b which use a removable wireless PC card cannot support WEP at full speed and should not be used with WEP enabled. For these systems it is best to use the InterJak VPN Service for authentication and encryption of wireless links.

---

## For Further Information

For general information on the InterJak Service Appliance product line, and services available, please see the main Filanet web site at <http://www.filanet.com>. For access to the InterJak Technical Reference Manual and other application notes, please see the Filanet support section at <http://www.filanet.com/support>.