New Automobile Systems:
Site-to-Site IPSec VPN for FTP
All Industry Test Technical Guideline

The purpose of this document is to provide the technical guideline in configuring a secured connection or a Virtual Private Networking (VPN) tunnel between IBC and the insurer over a public network like the Internet. Once the secured link is established, it can be used to transmit Automobile files to IBC using FTP.

This method is called Secured FTP using site-to-site IPSec VPN and is one of the three options supported to transfer Automobile files to IBC. The other two methods, Web Services (application-to-application) and Web Browser (manual), are described in separate material.

REQUIREMENTS

The following are the requirements for insurers to set up a site-to-site VPN connection with IBC:

- An IPSec-compliant VPN firewall or gateway
- High speed internet access
- Technical knowledge of their existing network infrastructure
- Technical knowledge in deploying Virtual Private Networking technology
- IBC-assigned FTP User ID (provided via email to the insurer's All Industry Test Primary Contact)

PARAMETERS

The following parameters have to be configured at the endpoint IPSec-compliant VPN gateways (IBC's and insurer):

VPN Peer Gateway IP Address:

IBC: 206.116.160.251
Insurer: x.x.x.x

Participating Nodes (encryption domain):

IBC: 206.116.160.23 and 206.116.160.24 (FTP Server IP addresses – All Industry Test period (Oct – Dec) and Production (January 2008))
Insurer: y.y.y.y (FTP Client IP address/es)

For IKE :

Key Exchange encryption: 3DES
Data integrity: SHA1
DH Group: 2
Authentication Method: pre-shared secret (this will be the FTP ID issued by IBC)

For IPSec tunnel properties:

Transform method: ESP
Encryption Algorithm: 3DES
Data Integrity: SHA1

TESTING THE CONNECTIVITY USING FTP

Once the VPN gateways are fully configured, the secured connection should be tested by the insurer (e.g. initiating a session to IBC's FTP server).

Sample Log:

c:\>**ftp ftptest.ibc.ca**
Connected to ftptest.ibc.ca.

At this point, the VPN gateways will exchange security parameters and if OK will set up a communications tunnel between the endpoints. Once successfully established, the following will be displayed:

220 Microsoft FTP Service
User (ftptest.ibc.ca:(none)): ← *enter IBC-supplied User ID*

331 Password required for *User ID*.
Password: ← *enter password*

230 User <*User ID*> logged in.
ftp> put *file name* ← *enter file name to transmit*

200 PORT command successful.
150 Opening ASCII mode data connection for *file name*
226 Transfer complete.
ftp: …. bytes sent in …..Seconds …..*Kbytes/sec*.
ftp> quit
221

SAMPLE FIREWALL/VPN LOG

Interface	Action	Service	Source	Destination	Prot	Rule	Source Port	Information
daemon	Key Install		Fw_FTPTest-NS	FW6				IKE: Main Mode completion [UDP].
daemon	Key Install		Fw_FTPTest-NS	FW6				IKE: Quick Mode completion; IKE IDs: host: 206.116.160.23 and host: 192.168.10.2
eth14	Decrypt	ftp	Ws_FTPTest	206.116.160.23	tcp	3	2025	service_id: ftp
daemon	Key Install		Fw_FTPTest-NS	FW6				IKE: Informational Exchange Received Delete IPSEC-SA from Peer: 206.47.88.25; SPIs: cea86563

OBTAINING TECHNICAL SUPPORT

If you require additional support in establishing connectivity please forward a request to ASP2008@IBC.ca indicating you require technical connectivity assistance. Please provide your name, phone number, company name and reporting company number and a member of the All Industry Test Support team will contact you.