[Foreword]

Set up Shrew Sofr VPN tool to connection IKE Config mode VPN.

Please follow my other KM "How to set up IKE Config Mode VPN".

[Topology]



[Setup in PC1]

General Page

- 1. Set up DFL-260 IP in "Host Name or IP Address"
- 2. Change Address Method "Use a virtual adapter and assigned address"

|      | Client    | Name R    | esolution | Authe   | enticatic 🕚 |
|------|-----------|-----------|-----------|---------|-------------|
| Remo | te Host   |           |           |         |             |
| Host | Name or   | IP Addres | s         |         | Port        |
| 61.2 | 8.67.126  | a i       |           |         | 500         |
| Auto | Configura | ition     | ike confi | ia pull | -           |
| мти  |           |           | 🔽 Obtair  | n Autor | natically   |
| 111  | 30        | Address   |           |         |             |
| 138  |           |           | 14        |         |             |

3. If PC1 IKE service port it's not setting default. You have to change this tool port number and firewall port number.

| Services | ices<br>are pre-defined or user-defined obj | ects representing various IP proto | cools, such as HTTP, FTP and Teinet. |   |
|----------|---|------------------------------------|--------------------------------------|---|
| 60       | 🧭 ike                                       | UDP                                | 500                                  | Internet Key Exchange -<br>key management for IPsec |

# Client Page

1. Setting by default. Make sure NAT traversal port number.

| General | Client   | Name Res      | olution  | Authe  | enticatio | • |
|---------|----------|---------------|----------|--------|-----------|---|
| Firewal | l Option | IS            |          |        |           |   |
| NAT T   | raversa  | al            | ena      | ible   |           | - |
| NAT T   | raversa  | al Port       |          |        | 450       | 0 |
| Keep-a  | alive pa | cket rate     |          | 15     | Secs      |   |
| IKE Fr  | agment   | ation         | ena      | ble    |           | - |
| Maxim   | um pac   | ket size      |          | 540    | Bytes     |   |
| Other C | )ptions  |               |          |        |           |   |
| 🔽 En    | able De  | ad Peer Dete  | ection   |        |           |   |
| 🔽 En    | able IS/ | AKMP Failure  | Notifica | ations |           |   |
| V En-   | able Cli | ent Login Bar | nner     |        |           |   |

2. You can check firewall port number.

|   | es<br>re pre-defined or user-defined objects r | representing various IP pro | stocols, such as HTTP, FTP and Telnet. |   |  |
|---|--|-----------------------------|--|---|--|
| 4 | 🧑 ipsec-natt                                   | UDP                         | 4500                                   | IPsec NAT-traversal<br>(through udp/4500) |  |

## Name Resolution

1. Setting by default.

| General            | Client                     | Name F        | Resolution | Authe  | enticatic |  |
|--------------------|----------------------------|---------------|------------|--------|-----------|--|
| WINS<br>Er<br>WINS | /DNS<br>hable WI<br>Server | NS<br>Address | 🔽 Obtai    | n Auto | matically |  |
| DNS 2              | iable DN<br>Server A       | IS<br>Iddress | 🔽 Obtai    | n Auto | matically |  |
| DNS                | Suffix                     |               |            |        |           |  |
| 🔽 Er               | able Sp                    | lit DNS       | 🔽 Obtai    | n Auto | matically |  |
|                    |                            |               |            |        | Add       |  |
|                    |                            |               |            |        | Modify    |  |
|                    |                            |               |            |        | Delete    |  |

Authentication Page

- 1. Authentication Method chose "Mutual PSK"
- 2. Local Identity Type chose "IP Address"
- 3. Remote Identity Type chose "IP Address"
- 4. Credentials enter your Pre Shared Key

| VPN Site Configuration  | VPN Site Configuration   | VPN Site Configuration  |
|---|--|---|
| Client Name Resolution Authentication Phase ( Authentication Method Mutual PSK Local Identity Remote Identity Credentials Identification Type IP Address Address String Use a discovered local host address | Name Resolution       Authentication       Phase 1       Pha         Authentication       Method       Mutual PSK         Local Identity       Remote Identity       Credentials         Identification       Type       IP         Address       V         Address       V         Address       V         Use a discovered remote host address | Name Resolution       Authentication       Phase 1       Pha • • •         Authentication       Method       Mutual PSK       •         Local Identity       Remote Identity       Credentials         Server Certificate Autority File          Client Certificate File          Client Private Key File          Pre Shared Key |
| Save Cancel   | Save Cancel  | Save Cancel   |

Phase 1

- 1. Exchange Type "Main"
- 2. DH Exchange chose "group2"
- 3. Cipher Algorithm "3des" (Any type like your firewall setting)
- 4. Hash Algorithm "md5"
- 5. Key Life Time limit "28800" (Setting like your fire setting)

| Authentication      | Phase 1  | Phase 2 | Policy |      |
|---------------------|----------|---------|--------|------|
| Proposal Par        | ameters  |         |        |      |
| Exchange T          | уре      | main    |        | •    |
| DH Exchang          | je       | group 2 |        |      |
| Cipher Algorithm    |          | 3des 🔹  |        | •    |
| Cipher Key L        | .ength   |         | ÷)     | Bits |
| Hash Algorit        | hm       | md5     |        | •    |
| Key Life Tim        | ie limit | 28800   |        | Secs |
| Kev Life Data limit |          |         | Kbytes |      |

# Interfaces > IPsec

| General A   | LINNE<br>I item is used to define IPsec er<br>uthentication XAuth | dpoint and will appear as a logical interface in the system. Routing IKE Settings Keep-alive Advanced |
|---|---|---|
| Algorithms IKE Algorithms: IKE Lifetime:                | Medium  | seconds   |
| IPsec Algorithms:<br>IPsec Lifetime:<br>IPsec Lifetime: | Medium  | seconds   |
| General A   | uthentication XAuth   | Routing IKE Settings Keep-alive Advanced  |
| Main DH G   | roup  |   |
| Aggressive 2  | IKE Algorithms  |   |

| Add 🗸 |        |   |                    |
|-------|--------|---|--------------------|
| -     | Name - | Algorithms -                                      | Comments -         |
|       | 🚱 High | 3DES, AES, Blowfish, MD5, SHA1                    | High security      |
|       | Medium | 3DES AES, Blowfish, Twofish,<br>CAST128, MDS SHA1 | High compatibility |

#### Phase 2

- 1. Transform Algorithm chose "esp-3des".
- 2. HMAC Algorithm chose md5.
- 3. Disable PFS Exchange and Compress Algorithm.
- 4. Key Life Time limit have same as firewall. (Interfaces > IPsec)

| Authentication      | Phase 1  | Phase 2    | Policy | 4    |
|---------------------|----------|------------|--------|------|
| Proposal Para       | meters   |            |        |      |
| Transform Alg       | gorithm  | esp-3de    | s      | •    |
| Transform Ke        | y Length |            | *      | Bits |
| HMAC Algori         | thm      | md5        |        | •    |
| PFS Exchange        |          | disabled 🔹 |        |      |
| Compress Alg        | gorithm  | disabled   |        |      |
| Key Life Time       | e limit  | 1          | 3600   | Secs |
| Kev Life Data limit |          | -          | Kbytes |      |

## Policy

- 1. Policy Generation Level "unique".
- 2. Cancel "Obtain Topology Automatically or Tunnel All" and add PC2 LAN net.

| uthentication | Phase 1     | Phase 2      | Policy      | 4   |
|---------------|-------------|--------------|-------------|-----|
| IPSEC Policy  | Configura   | tion         |             |     |
| Policy Gene   | ration Leve | el u         | nique       | -   |
| 📄 Maintain    | Persistent  | Security A:  | ssociations |     |
| 📄 Obtain T    | opology Au  | utomatically | or Tunnel   | All |
| Remo          | e Network   | Resource     |             |     |
| ↔ 192.16      | 68.1.0 / 25 | 5.255.255.   | 0           |     |
| -             |             |              |             |     |
|               |             |              |             |     |
| _             |             |              |             |     |
| Add           |             | lodifu       | Dalah       |     |
| Add           |             | iouily       | Delet       | -   |

When you login VPN tunnel you can check information in Shrew Soft.

