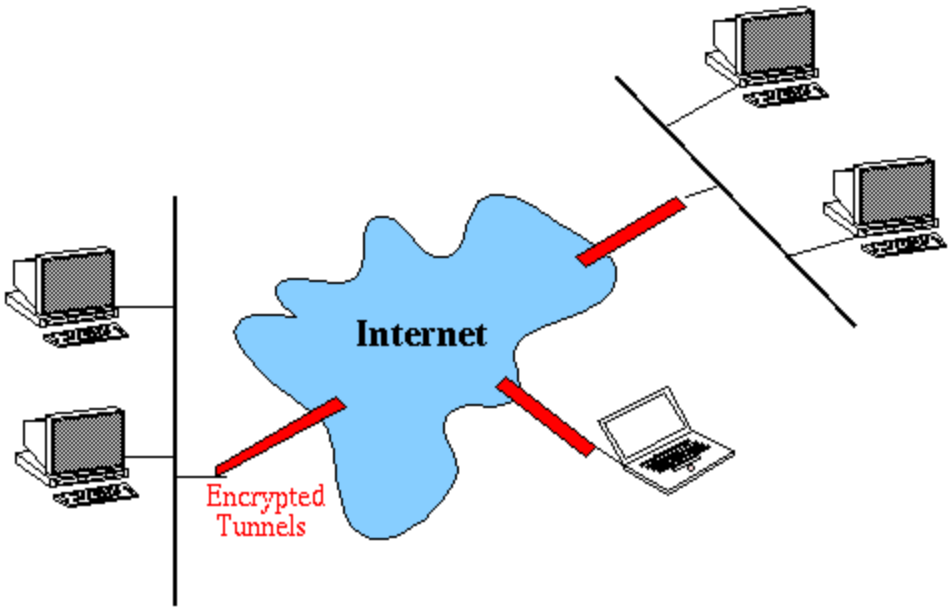
Application Note

This application note explains the options in the **vpn_profile config** file.



Contents

1 IPSec VPN Profile Common Options

```
config vpn_profile ipsec_common
```

```
  option enable_natt          "yes"
```

- **yes** - enable NAT traversal,
- **no** - disable NAT traversal.

```
  option pluto_virt_priv_opts
    "%v4:192.168.0.0/16,%v4:10.0.0.0/8,%v4:172.16.0.0/12" #
```

We allow all private networks within the IP address space reserved by IANA (see RFC 1918) to be on the remote site. We add our own LAN subnet to this option to be disallowed in **vpn_manager** script.

```
option remote_user_enabled "0"
```

Only one remote user profile is allowed at a time. We set and use this flag at run time to check if there is an enabled remote user profile. No need to change anything here.

2 IPSec VPN Profile

```
config vpn_profile ipsec_remote_psk

option profile_type         "ipsec"
option enable               "0"

option started              "0"
```

Normally, when "**vpn_manager start**" is called, all profiles with **enable=1** are started. But if "**vpn_manager start profile_name**" is used, only the specified profile is started, even though other profiles might be enabled. So, This flag keeps track of started profiles.

```
option tunnel_name          "remote-user-psk"
```

Tunnel name keep tracks of **ipsec** tunnels in the low level.

```
option tunnel_type          "remote-user"
```

We support "remote-user" and "site-to-site" tunnel types.

```
option local_id             ""
```

Local ID of the router. It may be needed if the remote party sets it.

```
option local_ip             ""
```

WAN IP of the router, automatically set by the VPN script. No need to set manually.

```
option local_net            ""
```

LAN subnet of the router, automatically set by the VPN script. No need to set manually.

```
option local_src            ""
```

LAN IP of the router, automatically set by the VPN script. No need to set manually.

```
option remote_id            ""
```

ID of the remote party. If we set it here, it should match the one set by the remote party for itself.

```
option remote_ip            "%any"
```

Needed only for site-to-site VPN connection. WAN IP of the remote VPN router.

```
option remote_net           ""
```

Needed only for site-to-site VPN connection. LAN subnet of the remote VPN router.

```
option remote_src           ""
```

Needed only for site-to-site VPN connection. LAN IP of the remote VPN router.

```
option remote_ike_port          "500"
```

IKE uses UDP port 500 by default. But we can set it here as long as the remote party also uses the same.

```
option auth_type                "psk"
```

IPsec authentication type: psk or rsasig.

```
option psk                  '"boo"'
```

If auth type is psk, then this is where you can set the preshared key, which should match the key at the remote party.

```
option local_cert           ""
option local_private_key    ""
```

If the auth type is **rsasig**, then you should set which local certificate and key to be used. You should write the full path of the certificate and private key files. See the **ipsec_remote_cert** profile in Section 2.1 for an example. An example certificate file is put in **/etc/ipsec.d/certs** and key file in **etc/ipsec.d/private**. We also need the CA (certificate authority) certificates to be put into **/etc/ipsec.d/cacerts**. They are used to verify the certificate of the remote party. We put an example CA certificate there. This is the certificate of the CA, which issued the server and client certificates we use as examples. We also put example client certificates in **/etc/ipsec.d/client-cert** so that we can test certificate authentication. They are not used at the router actually. You need to load them to the remote party before starting the connection. We use the name "server certificate" for us and the "client certificate" for the remote party, but this is just for convenience. Names may change.

```
  option local_key_passwd          '"'
```

A private key can (and should) be encrypted so as not to be captured by others. If the router's private key is encrypted, you have to write its password here so that it can be used for **ipsec**.

```
option ike_enc_alg               ""
option ike_auth_alg              ""
option ike_dh_group              ""
option esp_enc_alg               ""
option esp_auth_alg              ""
option esp_pfs_group             ""
option dpd_enable                ""
```

You can set IKE (Phase 1) and ESP (Phase 2) encryption and hash algorithms to be selected during negotiation.

Supported values for **ike_enc_alg** and **esp_enc_alg**: des, 3des, aes128, aes192, aes256

Supported values for **ike_auth_alg** and **esp_auth_alg**: md5, sha1

Supported values for **ike_dh_group** and **esp_pfs_group**: modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192

```
  option dpd_enable          "yes"
```

This is for enabling/disabling Dead Peer Detection. The value "no" disables.

```
  option dpd_delay           "30"
```

Send R_U_THERE packets every **dpd_delay** seconds.

```
  option dpd_timeout         "120"
  option dpd_action          "clear"
```

If the tunnel is idle and we haven't received an R_U_THERE_ACK from our peer in **dpd_timeout** seconds, we declare the peer dead, and clear the SA + eroute (the entire tunnel is removed).

```
  option xauth_enable        ""
```

You can enable XAUTH (extended authentication) by setting **xauth_enable** to "1".

```
  option xauth_group          "1"
```

Select the user group to be used for XAUTH from **user_database**. All the users in this group will be copied to the **/etc/ipsec.d/passwd** file with computed password hashes.

2.1 Example Remote Profile

```
config vpn_profile ipsec_remote_cert
   option profile_type         "ipsec"
   option enable               "0"
   option started              "0"

   option tunnel_name          "remote-user-cert"
   option tunnel_type          "remote-user"
   option local_id             ""
   option local_ip             ""
   option local_net            ""
   option local_src            ""
   option remote_id            ""
   option remote_ip            "%any"
   option remote_net           ""
   option remote_src           ""
   option remote_ike_port            "500"
   option auth_type                "rsasig"
   option psk                  ""
   option local_cert           "/etc/ipsec.d/certs/serverCert.pem"
   option local_private_key    "/etc/ipsec.d/private/server.key"
   option local_key_passwd           '"server"'
   option ike_enc_alg          ""
   option ike_auth_alg         ""
   option ike_dh_group         ""
   option esp_enc_alg          ""
   option esp_auth_alg         ""
   option esp_pfs_group        ""
   option dpd_enable           "yes"
   option dpd_delay            "30"
   option dpd_timeout          "120"
   option dpd_action           "clear"
   option xauth_enable         "0"
   option xauth_group          "1"
```

2.2 Example Site-To-Site Profile

```
config vpn_profile ipsec_site_to_site
   option profile_type         "ipsec"
   option enable               "0"
   option started              "0"

   option tunnel_name          "site-to-site-psk"
   option tunnel_type          "site-to-site"
```

```
  option local_id             ""
  option local_ip             ""
  option local_net            ""
  option local_src            ""
  option remote_id            ""
  option remote_ip            ""
  option remote_net           ""
  option remote_src           ""
  option remote_ike_port            "500"
  option auth_type                "psk"
  option psk                  '"boo"'
  option local_cert           ""
  option local_private_key    ""
  option local_key_passwd           '""'
  option ike_enc_alg          ""
  option ike_auth_alg         ""
  option ike_dh_group         ""
  option esp_enc_alg          ""
  option esp_auth_alg         ""
  option dpd_enable           "yes"
  option dpd_delay            "30"
  option dpd_timeout          "120"
  option dpd_action           "clear"
```

3 L2TP/IPSec and PPTP VPN profiles

The L2TP/IPSec and PPTP VPN profiles are only for remote-user tunnel type. They cannot be used for site-to-site VPN connection.

3.1 L2TP/IPSec VPN Profile

```
config vpn_profile l2tp_ipsec
  option profile_type         "l2tp_ipsec"
  option enable               "1"
  option started              "0"

  option remote_ip_range            "192.168.0.202-192.168.0.210"
```

The IP range from which we will lease IP addresses to the remote users.

```
  option server_ip            "192.168.0.200"
```

Our own IP address for the created PPP interface.

```
option pap                  "require-pap"
option chap                 "require-chap"
option mschap               "require-mschap"
option mschapv2             "require-mschap-v2"
```

We can allow more than one authentication type simultaneously. Set the corresponding option to "require-xxx" to enable an authentication type. Set to "refuse-xxx" to disable it. All of them are enabled by default.

```
option user_group           "1"
```

Select the user group to be used for authentication from **user_database**. All the users in this group will be copied from **user_database** to **/etc/ppp/pap-secrets** for PAP and **/etc/ppp/chap**-secrets for all chap variants.

```
option tunnel_name          "l2tp-remote-user-psk"
option tunnel_type          "remote-user"
option local_id             ""
option local_ip             ""
option local_net            ""
option local_src            ""
option remote_ip            "%any"
option remote_ike_port            "500"
option auth_type            "psk"
option psk                  '"boo"'
option local_cert           ""
option local_private_key    ""
option local_key_passwd           '""'
option dpd_enable           "yes"
option dpd_delay            "30"
option dpd_timeout          "120"
option dpd_action           "clear"
```

3.2 PPTP VPN profile

```
config vpn_profile pptp_vpn
   option profile_type          "pptp_vpn"
   option enable                "0"
   option started               "0"
```

```
   option remote_ip_range             "192.168.0.234-238,192.168.0.245"
```

The IP range from which we will lease IP addresses to the remote users.

```
   option server_ip             "192.168.0.222"
```

Our own IP address for the created PPP interface.

```
   option pap                   "refuse-pap"
   option chap                  "refuse-chap"
   option mschap                "require-mschap"
   option mschapv2              "require-mschap-v2"
```

We can allow more than one authentication type simultaneously. Set the corresponding option to "require-xxx" to enable an authentication type. Set to "refuse-xxx" to disable it. We enable all except PAP by default. PAP is a weak authentication type and PPTP does not have secure **ipsec** tunnel below, so we disable PAP by default.

```
   option mppe                  "mppe required,no40,no56,stateless"
```

We can enable MPPE (Microsoft Point to Point Encryption) only if MSCHAPv2 is enabled for authentication. The settings mean: “128-bit encrypted stateless PPTP connection is enabled; 40 bit and 56 bit encryption are not allowed”.

```
   option user_group            "1"
```

Select the user group to be used for authentication from **user_database**. All the users in this group will be copied from **user_database** to **/etc/ppp/pap**-secrets for PAP and **/etc/ppp/chap**-secrets for all chap variants.

Application Note

Ubicom®, Inc.

Ubicom develops networking and media processor solutions that address the unique demands of real-time interactive applications and multimedia content delivery in the digital home. The company provides optimized system-level solutions for a wide range of products including wireless routers, access points, bridges, VoIP gateways, networked digital photo frames, and streaming media players.

195 Baypointe Parkway
San Jose, CA 94134

Tel 408.433.3300
Fax 408.433.3339

Email sales@ubicom.com
Web www.ubicom.com