Application Note

This document describes the CLI to configure a VPN connection with Ubicom VPN Middleware.

1. General VPN Profile

`vpn_commit_changes`

Saves changed settings to flash. This API has to be called after calling one or more of the VPN "set" APIs below.

`vpn_start_all_enabled_profiles`

Starts all VPN profiles that are already enabled.

`vpn_start_profile [profile_name]`

Starts the given VPN profile if it is enabled.

- **profile_name**: name of profile

`vpn_stop_profile [profile_name]`

Stops the given VPN profile, if it is started.

- **profile_name**: name of profile

`vpn_stop_all_profiles [profile_name]`

Stops all VPN profiles that are started.

`vpn_show_enabled_profile_names`

Shows the names of the enabled profiles.

`vpn_show_started_profile_names`

Shows the names of the started profiles.

`vpn_show_status`

Shows current VPN status.

`vpn_show_profile [profile_name]`

Displays all options of the requested profile.

- **profile_name**: name of profile

`vpn_show_all_profiles [profile_name]`

Displays all profiles, including options.

- **profile_name**: name of profile

`vpn_enable_profile [profile_name]`

Enable the VPN profile.

- **profile_name**: name of profile

`vpn_disable_profile [profile_name]`

Disable the VPN profile.

- **profile_name**: name of profile

`vpn_add_empty_profile [profile_name] [profile_type]`

This API creates an empty profile.

- **profile_name**: name of profile
- **profile_type**: ipsec, l2tp_ipsec, pptp_vpn

`vpn_add_new_option_to_profile [profile_name] [new_option] [value]`

Adds new options to a new profile after profile is created.

- **profile_name**: name of profile
- **new_option**: the option to add
- **value**: the value of the option

`vpn_remove_profile [profile_name]`

Delete the VPN profile.

- **profile_name**: name of profile

`vpn_add_new_user_to_database [username] [password] [group_number]`

- **username**: New user name to be added
- **password**: Password for the user name
- **group_number**: The group which the new user should be added to.

`vpn_add_new_group_to_database`

Adds a new user group with the next available group number. For example, if there are 3 groups currently, when you call this API, group number 4 is added. This API also returns the number of the new group.

`vpn_get_number_of_groups`

Returns the number of groups.

`vpn_get_number_of_users`

Returns the total number of users in all groups.

2. IPSEC

`vpn_ipsec_enable_nat_traversal`

Enables NAT traversal.

`vpn_ipsec_disable_nat_traversal`

Disables NAT traversal.

```
vpn_add_new_ipsec_profile[profile_name][tunnel_name][tunnel_type][auth_type]
```

Adds a new IPsec profile, getting the basic options as parameters and setting the rest to default or empty.

- **profile_name**: name of profile
- **tunnel_name**: name of the tunnel
- **tunnel_type**: type of the tunnel (remote-user or site-to-site)
- **auth_type**: authentication type (psk or rsasig)

```
vpn_ipsec_set_tunnel_type [profile_name] [tunnel_type]
```

- **profile_name**: name of profile
- **tunnel_type**: type of the tunnel (remote_user or site_to_site)

```
vpn_ipsec_set_tunnel_name [profile_name] [tunnel_name]
```

- **profile_name**: name of profile
- **tunnel_name**: name of the tunnel

```
vpn_ipsec_set_remote_id [profile_name] [remote_id]
```

Only for site-to-site VPN profiles.

- **profile_name**: name of profile
- **remote_id**: ID of remote VPN router

```
vpn_ipsec_set_remote_ip [profile_name] [remote_ip]
```

Only for site-to-site VPN profiles.

- **profile_name**: name of profile
- **remote_ip**: IP address of remote VPN router

```
vpn_ipsec_set_remote_src [profile_name] [remote_src]
```

Only for site-to-site VPN profiles.

- **profile_name**: name of profile
- **remote_src**: remote LAN IP; e.g. 192.168.1.1

```
vpn_ipsec_set_remote_net [profile_name] [remote_net]
```

Only for site-to-site VPN profiles.

- **profile_name**: name of profile
- **remote_net**: remote LAN subnet mask; e.g. 192.168.1.0/24

```
vpn_ipsec_set_auth_type [profile_name] [auth_type]
```

Sets the authentication type.

- **profile_name**: name of profile
- **auth_type**: authentication type (psk or rsasig)

```
vpn_ipsec_set_psk [profile_name] [psk]
```

Sets the preshared key for PSK authentication type.

- **profile_name**: name of profile
- **psk**: preshared key

```
vpn_ipsec_set_local_certificate [profile_name] [local_cert_path]
```

Sets the full path of the local certificate for RSA authentication type.

- **profile_name**: name of profile
- **local_cert_path**: full path of the local certificate

```
vpn_ipsec_set_local_private_key [profile_name] [local_key_path]
```

Sets the full path of the local private key for RSA authentication type.

- **profile_name**: name of profile
- **local_key_path**: full path of the local private key

```
vpn_ipsec_set_local_key_passwd [profile_name] [local_key_passwd]
```

Sets the password of the local private key for RSA authentication type.

A private key can (should) be encrypted 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.

- **profile_name**: name of profile
- **local_key_passwd**: password of the local private key.

```
vpn_ipsec_set_remote_certificate [profile_name] [remote_cert_path]
```

Sets the full path of the remote certificate for RSA authentication type.

Needed only for site-to-site VPN profile.

- **profile_name**: name of profile
- **remote_cert_path**: full path of the remote certificate

```
vpn_ipsec_set_ike_enc_alg [profile_name] [ike_enc_alg]
```

Sets the IKE (IPsec phase 1) encryption algorithm to be selected.

- **profile_name**: name of profile
- **ike_enc_alg**: IKE encryption algorithm; supported algorithms are des, 3des, aes128, aes192, aes256.

```
vpn_ipsec_set_ike_auth_alg [profile_name] [ike_auth_alg]
```

Sets the IKE (IPsec phase 1) authentication algorithm to be selected.

- **profile_name**: name of profile
- **ike_auth_alg**: IKE authentication algorithm; supported algorithms are md5 and sha1.

```
vpn_ipsec_set_ike_dh_group [profile_name] [ike_dh_group]
```

Sets the IKE (IPsec phase 1) DH group to be selected.

- **profile_name**: name of profile
- **ike_dh_group**: IKE DH group ; supported groups are modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192

```
vpn_ipsec_set_esp_enc_alg [profile_name] [esp_enc_alg]
```

Sets the ESP (IPsec phase 2) encryption algorithm to be selected.

- **profile_name**: name of profile
- **esp_enc_alg**: ESP encryption algorithm; supported algorithms are des, 3des, aes128, aes192, aes256.

```
vpn_ipsec_set_esp_auth_alg [profile_name] [esp_auth_alg]
```

Sets the ESP (IPsec phase 2) authentication algorithm to be selected.

- **profile_name**: name of profile
- **esp_auth_alg**: ESP authentication algorithm; supported algorithms are md5 and sha1.

```
vpn_ipsec_set_esp_pfs_group [profile_name] [esp_pfs_group]
```

Sets the ESP (IPsec phase 2) PFS group to be selected.

- **profile_name**: name of profile
- **iesp_pfs_group**: ESP PFS group ; supported groups are modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp819

```
vpn_ipsec_enable_dpd [profile_name]
```

Enable dead peer detection.

- **profile_name**: name of profile

```
vpn_ipsec_disable_dpd [profile_name]
```

Disable dead peer detection.

- **profile_name**: name of profile

```
vpn_ipsec_set_dpd_delay [profile_name] [dpd_delay]
```

Set the period of sending R_U_THERE packets.

- **profile_name**: name of profile
- **dpd_delay**: period of R_U_THERE packets to be sent.

```
vpn_ipsec_set_dpd_timeout [profile_name] [dpd_timeout]
```

Set the timeout value for DPD.

If we do not get an R_U_THERE_ACK from the remote party in ***dpd_timeout*** seconds, then we declare the peer dead, and clear the SA + eroute (the entire tunnel is removed).

- **profile_name**: name of profile
- **dpd_timeout**: timeout for R_U_THERE_ACK

```
vpn_ipsec_enable_xauth [profile_name]
```

Enable XAUTH authentication for remote user VPN.

- **profile_name**: name of profile

```
vpn_ipsec_disable_xauth [profile_name]
```

Disable XAUTH authentication.

- **profile_name**: name of profile

```
vpn_ipsec_set_xauth_group [profile_name] [group]
```

- **profile_name**: name of profile
- **group**: authentication database group (for server mode) – e.g. 1, 2, 3, etc.

```
vpn_ipsec_set_xauth_mode [profile_name] [mode]
```

- **profile_name**: name of profile
- **mode**: server or client

```
vpn_ipsec_set_xauth_group [profile_name] [group]
```

- **profile_name**: name of profile
- **group**: authentication database group (for server mode)

3. L2TP/IPSec

```
vpn_l2tp_ipsec_set_server_ip [profile_name] [server_ip]
```

- **profile_name**: name of profile
- **server_ip**: server IP address

```
vpn_l2tp_ipsec_set_remote_ip_range [profile_name] [remote_ip_start]
  [remote_ip_end]
```

- **profile_name**: name of profile
- **remote_ip_start**: start of remote IP address range
- **remote_ip_end**: stop of remote IP address range

```
vpn_l2tp_ipsec_enable_pap
```

Enable PAP authentication support

```
vpn_l2tp_ipsec_disable_pap
```

Disable PAP authentication support

```
vpn_l2tp_ipsec_enable_chap
```

Enable CHAP authentication support

```
vpn_l2tp_ipsec_disable_chap
```

Disable CHAP authentication support

```
vpn_l2tp_ipsec_enable_mschap
```

Enable MSCHAP authentication support

```
vpn_l2tp_ipsec_disable_mschap
```

Disable MSCHAP authentication support

```
vpn_l2tp_ipsec_enable_mschapv2
```

Enable MSCHAPv2 authentication support

```
vpn_l2tp_ipsec_disable_mschapv2
```

Disable MSCHAPv2 authentication support

```
vpn_l2tp_ipsec_set_user_group[profile_name] [user_group]
```

Note that user groups and users should be added to the database before calling this API.

- **profile_name**: name of profile
- **user_group**: user group name

```
vpn_l2tp_ipsec_set_auth_type [profile_name] [auth_type]
```

- **profile_name**: name of profile
- **auth_type**: psk or rsasig

4. PPTP

```
vpn_pptp_set_server_ip [profile_name] [server_ip]
```

- **profile_name**: name of profile
- **server_ip**: server IP address

```
vpn_pptp_set_remote_ip_range [profile_name] [remote_ip_start]
  [remote_ip_end]
```

- **profile_name**: name of profile
- **remote_ip_start**: start of remote IP address range
- **remote_ip_end**: stop of remote IP address range

```
vpn_pptp_enable_pap
```

Enable PAP authentication support

```
vpn_pptp_disable_pap
```

Disable PAP authentication support

```
vpn_pptp_enable_chap
```

Enable CHAP authentication support

```
vpn_pptp_disable_chap
```

Disable CHAP authentication support

```
vpn_pptp_enable_mschap
```

Enable MSCHAP authentication support

`vpn_pptp_disable_mschap`

Disable MSCHAP authentication support

`vpn_pptp_enable_mschapv2`

Enable MSCHAPv2 authentication support

`vpn_pptp_disable_mschapv2`

Disable MSCHAPv2 authentication support

`vpn_pptp_set_mppe [mppe_option]`

Sets the encryption option for PPTP VPN.

- **`mppe_option`**: Default value is "mppe required,no40,no56,stateless"

`vpn_pptp_set_user_group [profile_name] [user_group]`

Note that user groups and users should be added to the database before calling this API.

- **`profile_name`**: name of profile
- **`user_group`**: user group name

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