

- **DEPRECATED** : by the IPSEC Openwrt Router Configuration
- Trillion – VPN Gateway
 - 192.168.137.1
 - private
 - acts as the gateway for the Wifi : **WRT1900ACS**
 - 192.168.0.66
 - public side of the ip
- every time IPSEC connects it gets given an IP Address of the form
 - ipsec statusall
 - get the ipaddress
 - 10.6.x.x
 - need to run automatically via the scripts :
 - iptables -flush -t nat
 - iptables -t nat -A POSTROUTING -s 192.168.137.0/24 -o enx00909e9aa9e3 -j SNAT -to-source 10.6.x.x
- I have setup up and down scripts.
 - /etc/strongswan.d/scripts/connected
 - Connected
 - finds the IPSEC address and sets up the SNAT ipstables
 - Disconnected
 - flushes the NAT table and sets up a general MASQUERADE
- There is an ipsec.conf file
 - edit this file to determine which VPN server to connect to and in which country.
 - best countries are Japan and USA
 - Nordvpn Instructions

trillion:/etc/ipsec.conf

```
config setup
conn NordVPN_16_US
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=300s
    eap_identity="FEaYDjUGWcnUuFW4gDfVR1kk"
    leftauth=eap-mschapv2
    left=%defaultroute
    leftsourceip=%config
    leftupdown=/etc/strongswan.d/scripts/connected
    right=45.79.89.28
    rightauth=pubkey
    rightsubnet=0.0.0.0/0
    rightid=@us5784.nordvpn.com
    rightca=/etc/ipsec.d/cacerts/NordVPN.pem
    type=tunnel
    #auto=add
    auto=start
```

```
conn NordVPN_21_JP
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=300s
    eap_identity="FEaYDjUGWcnUuFW4gDfVR1kk"
    leftauth=eap-mschapv2
    left=%defaultroute
    leftsourceip=%config
    leftupdown=/etc/strongswan.d/scripts/connected
    right=172.105.236.221
    rightauth=pubkey
    rightsubnet=0.0.0.0/0
    rightid=@jp599.nordvpn.com
    rightca=/etc/ipsec.d/cacerts/NordVPN.pem
    type=tunnel
    auto=add
```

```
conn NordVPN_22_JP
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=300s
    eap_identity="FEaYDjUGWcnUuFW4gDfVR1kk"
    leftauth=eap-mschapv2
    left=%defaultroute
    leftsourceip=%config
    leftupdown=/etc/strongswan.d/scripts/connected
    right=172.104.103.149
    rightauth=pubkey
    rightsubnet=0.0.0.0/0
    rightid=@jp599.nordvpn.com
    rightca=/etc/ipsec.d/cacerts/NordVPN.pem
    type=tunnel
    auto=add
```

/etc/strongswan.d/scripts/connected

```
#!/bin/bash
case "$PLUTO_VERB:$1" in
up-client:)
    iptables --flush -t nat
    iptables -t nat -A POSTROUTING -s 192.168.137.0/24 -o enx00909e9aa9e3 -j SNAT --to-source
$PLUTO_MY_SOURCEIP
    ;;
down-client:)
    iptables --flush -t nat
    iptables -t nat -A POSTROUTING -o enx00909e9aa9e3 -j MASQUERADE
    ;;
esac
```

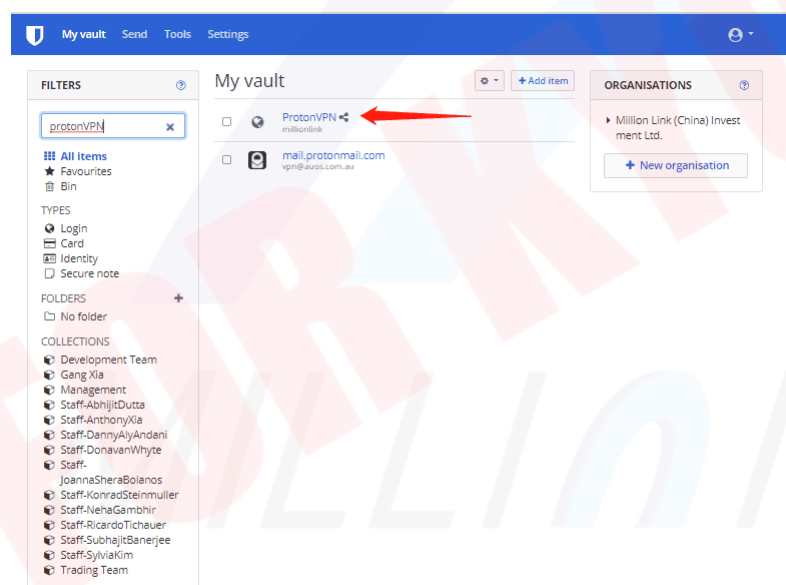
I have multiple VPN connections available for use.

Name	Owner	Username	Password	Speed	China?	Notes
SoftEther	Million Link	millionlink	<vault.millionlink.us>	Medium	Mostly	Connects to Million Link's server
VyprVPN	Konrad	konrad	<vault.millionlink.us>	Fast	Chameleon	Only Chameleon works in China
NordVPN	Konrad	konrad	<vault.millionlink.us>	Fast	IPSec	Only Hidden IPSec servers work reliably in China
ProtonVPN	Konrad	konrad	<vault.millionlink.us>	Fast	Only Secret Servers	Works fine outside China Choose Switzerland #16 for inside China
QuickQ						Possible new VPN if others stop working
VPS000	Anthony				YES	Anthony Recommended; Works on Iphone

If you need passwords please ask for the password to be transferred to you via <https://vault.millionlink.us>


If you are inside China, try to use Softether first.

If you are outside China, try to use ProtonVPN first.



EDIT ITEM

Name: ProtonVPN Folder: No folder

Username: millionlink Password: [masked] 

Authenticator key (TOTP): [masked] 10 878 724

Notes: [empty text area]

CUSTOM FIELDS: New custom field Text

Updated: 26 Aug 2021, 20:15:55
Password updated: 26 Aug 2021, 20:15:52
Password history: 1

OPTIONS: ☐ Master password re-prompt

Save Cancel

Click to copy Password

This OpenWRT Router replaces the Linux IPsec VPN setup on Trillian.

Install Openwrt

1. Install OpenWrt 21.02.7
 - not all versions have Strongswan available as installed software
 - as of 2023-08-31 this was the latest version that had strongswan_ipsec as an option to install.

Basic Setup of Router

1. System -> System
 - Hostname
 - choose a cool name for the router
 - Logging
 - set the logging to 256kb
 - Time Synchronization
 - Enable NTP client
2. Set the Root password & SSH keys
 - System -> Administration
 - password
 - ssh-keys
 - drag and drop an id_rsa.pub file from your ~/.ssh folder
3. Set the local LAN network
 - do not use
 - 192.168.1.0/24
 - 192.168.0.0/24
 - recommended
 - 192.168.[100 - 110].0/24

4. Set the update mechanism

- System -> Scheduled Tasks
- Add an update task to be run daily

```
25 3 * * * root /etc/strongswan.d/scripts/update
```

5. Setup DNSmasq

- Network -> DHCP & DNS -> Advanced Settings
- Set "Strict Order"
- This will prioritize the VPN name servers over the China Nameserver

6. Update the firewall with custom rules

```
iptables -t mangle -A FORWARD -m policy --pol ipsec --dir in -p tcp -m tcp --tcp-flags SYN,RST
SYN -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
iptables -t mangle -A FORWARD -m policy --pol ipsec --dir out -p tcp -m tcp --tcp-flags SYN,RST
SYN -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
iptables -t nat -A POSTROUTING -m policy --dir out --pol ipsec -j ACCEPT
```

mrsniffles
Status
System
Network
Logout
REFRESHING

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings
Logging
Time Synchronization
Language and Style

Local Time2023-09-05 04:49:57

Sync with browser
Sync with NTP-Server

Hostnamemrsniffles

Description

? An optional, short description for this device

Notes

? Optional, free-form notes about this device

TimezoneUTC

Save & Apply

Save

Reset

Page 5

Million Link is an International Trading Group based out of Hong Kong with branches in Tianjin (China), India, Pakistan, Peru, USA and Egypt. We specialize in Ferroalloys and have been supplying raw materials to the Steel Industry since 1997. We are ISO 9001:2015 Quality Management System certified and we are an A-Licensed exporter of FerroAlloys.

Updated : 2025-08-04

No password set!

There is no password set on this router. Please configure a root password to protect the web interface.

Router Password SSH Access SSH-Keys

Router Password

Changes the administrator password for accessing the device

Password

Confirmation



Save

Router Password SSH Access SSH-Keys

SSH-Keys

Public keys allow for the passwordless SSH logins with a higher security compared to the use of plain passwords. In order to upload a new key to the device, paste an OpenSSH compatible public key line or drag a `.pub` file into the input field.

konrad@THREADRIPPER
RSA, 3072 Bit

Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.

# these are to help the fragmentation of packets over the IPSEC vpn
iptables -t mangle -A FORWARD -m policy --pol ipsec --dir in -p tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
iptables -t mangle -A FORWARD -m policy --pol ipsec --dir out -p tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1361:1536 -j TCPMSS --set-mss 1360
iptables -t nat -A POSTROUTING -m policy --dir out --pol ipsec -j ACCEPT
```

Save

FOR KYC ONLY

MILLIONLINK

FOR KYC ONLY

MILLIONLINK

FOR KYC ONLY

MILLIONLINK

DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

General Settings Resolv and Hosts Files TFTP Settings **Advanced Settings** Static Leases

Suppress logging ☐

Suppress logging of the routine operation of these protocols

Allocate IP sequentially ☐

Allocate IP addresses sequentially, starting from the lowest available address

Filter private ☒

Do not forward reverse lookups for local networks

Filter useless ☐

Do not forward requests that cannot be answered by public name servers

Localise queries ☒

Localise hostname depending on the requesting subnet if multiple IPs are available

Expand hosts ☒

Add local domain suffix to names served from hosts files

No negative cache ☐

Do not cache negative replies, e.g. for not existing domains

Additional servers file

This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.

Strict order ☒

DNS servers will be queried in the order of the resolvfile

All Servers ☐

Query all available upstream DNS servers

Bogus NX Domain Override

67.215.65.132 +

List of hosts that supply bogus NX domain results

DNS server port

53

Listening port for inbound DNS queries

DNS query port

any

Fixed source port for outbound DNS queries

Max. DHCP leases

unlimited

Maximum allowed number of active DHCP leases

Max. EDNS0 packet size

1232

Maximum allowed size of EDNS.0 UDP packets

Max. concurrent queries

150

Maximum allowed number of concurrent DNS queries

Size of DNS query cache

150

Number of cached DNS entries (max is 10000, 0 is no caching)

Save & Apply

Save

Reset

Install Software

1. SSH into the Router
 - `ssh root@192.168.101.1`
2. Update all opkg packages
 - `opkg update`
3. Get the list of software to install
 - `FILES=`cat installed_extra``
 - `opkg install $FILES`
 - you will need to split \$FILES up into 4 equal parts to install
 - there isn't enough buffer

```
root@openwrt:~# opkg install adblock banip bind-dig bind-host bind-libs coreutils coreutils-sort diffutils ip-full ip-tiny ipset iptables-mod-contrack-extra iptables-mod-ipopt iptables-mod-iptable iptables-mod-ipsec iptables-mod-nat-extra kmod-crypto-acompress kmod-crypto-aead kmod-crypto-authenc kmod-crypto-cbc kmod-crypto-deflate kmod-crypto-des kmod-crypto-echainiv kmod-crypto-hash kmod-crypto-hmac kmod-crypto-kpp
```

```
root@openwrt:~# opkg install kmod-crypto-lib-chacha20 kmod-crypto-lib-chacha20poly1305 kmod-crypto-lib-curve25519 kmod-crypto-lib-poly1305 kmod-crypto-manager kmod-crypto-md5 kmod-crypto-null kmod-crypto-pcompress kmod-crypto-sha1 kmod-crypto-user kmod-ibf kmod-ipsec kmod-ipsec4 kmod-ipsec6 kmod-ipt-contrack-extra kmod-ipt-ipopt
```

```
root@openwrt:~# opkg install kmod-ipt-iptable kmod-ipt-ipsec kmod-ipt-ipset kmod-ipt-nat-extra kmod-ipt-raw kmod-iptunnel4 kmod-iptunnel6 kmod-lib-zlib-deflate kmod-lib-zlib-inflate kmod-nftnl kmod-sched-contrack kmod-sched-core kmod-tun kmod-udptunnel4 kmod-udptunnel6 kmod-wireguard
```

```
root@openwrt:~# opkg install libatomic1 libbpf0 libbz2-1.0 libcurl4 libelf1 libev libexif libffmpg-mini libflac libgcrypt libgmp10 libgpg-error libid3tag libipset13 libjpeg-turbo libmariadb3 libmbd2 libmnl0 libncurses6 libnftnl0 libnftnl14 libogg0 libopenldap libopenssl1.1 libpcap1 libpcre libreadline8 librt libsasl2 libsodium libsqlite3-0 libuv1 libvorbis libxml2 luci-app-adblock luci-app-advanced-reboot luci-app-banip luci-app-commands luci-app-minidlna luci-app-qos luci-app-shadowsocks-libev luci-app-softether luci-app-wireguard luci-compat luci-proto-wireguard minidlna net-tools-route qos-scripts shadowsocks-libev-config shadowsocks-libev-ss-local shadowsocks-libev-ss-tunnel sipcalc softethervpn5-client softethervpn5-libs tc-mod-iptables tc-tiny tcpdump terminfo vim wireguard-tools zlib
```

```
root@openwrt:~# opkg install strongswan strongswan-charon strongswan-charon-cmd strongswan-default strongswan-full strongswan-ipsec strongswan-isakmp strongswan-libtls strongswan-mod-adblock strongswan-mod-aes strongswan-mod-af-alg strongswan-mod-agent strongswan-mod-attr strongswan-mod-attr-sql strongswan-mod-blowfish strongswan-mod-ccm strongswan-mod-cmac strongswan-mod-contrack strongswan-mod-constraints strongswan-mod-coupling strongswan-mod-ctr strongswan-mod-curl strongswan-mod-curve25519 strongswan-mod-des strongswan-mod-dhcp strongswan-mod-dnskey strongswan-mod-duplicheck strongswan-mod-eap-identity strongswan-mod-eap-md5 strongswan-mod-eap-mschapv2 strongswan-mod-eap-radius strongswan-mod-eap-tls strongswan-mod-farp strongswan-mod-fips-prf strongswan-mod-forecast strongswan-mod-gcm strongswan-mod-gcrypt
```

strongswan-mod-gmp strongswan-mod-gmpdh strongswan-mod-ha strongswan-mod-hmac strongswan-mod-kernel-libipsec strongswan-mod-kernel-netlink strongswan-mod-ldap strongswan-mod-led strongswan-mod-load-tester strongswan-mod-md4 strongswan-mod-md5 strongswan-mod-mysql strongswan-mod-nonce strongswan-mod-openssl strongswan-mod-pem strongswan-mod-pgp strongswan-mod-pkcs1 strongswan-mod-pkcs11 strongswan-mod-pkcs12 strongswan-mod-pkcs7 strongswan-mod-pkcs8 strongswan-mod-pubkey strongswan-mod-random strongswan-mod-rc2 strongswan-mod-resolve strongswan-mod-revocation strongswan-mod-sha1 strongswan-mod-sha2 strongswan-mod-smp strongswan-mod-socket-default strongswan-mod-socket-dynamic strongswan-mod-sql strongswan-mod-sqlite strongswan-mod-sshkey strongswan-mod-stroke strongswan-mod-test-vectors strongswan-mod-uci strongswan-mod-unity strongswan-mod-updown strongswan-mod-vici strongswan-mod-whitelist strongswan-mod-x509 strongswan-mod-xauth-eap strongswan-mod-xauth-generic strongswan-mod-xcbc strongswan-pki strongswan-scepclient strongswan-swanctl

Setup the IPSEC connection

- List of files to be edited
 - /etc/hosts
 - /etc/rc.local
 - /etc/ipsec.conf
 - /etc/ipsec.secrets
 - /etc/strongswan.d/charon.conf
 - /etc/strongswan.d/charon/constraints.conf
 - /etc/strongswan.d/charon/resolv.conf
 - /etc/strongswan.d/scripts/connected
 - make this file executable
 - chmod +x connected
 - IMPORTANT
 - match this file with the IP address range
 - /etc/strongswan.d/scripts/connected
 - make this file executable
 - chmod +x connected
 - /etc/ipsec.d/cacerts/NordVPN.pem
 - /etc/config/luci

/etc/hosts

127.0.0.1 localhost

110.242.68.66 baidu.com

39.156.66.10 baidu.com

110.242.68.4 www.baidu.com

110.242.68.3 www.baidu.com

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

/etc/rc.local

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

# table 220 is the ipsec routing table
# all chinese IP addresses don't need to go through the IPSEC vpn
# designating "throw" will have the route drop to a higher IP routing table 254

/sbin/ip route add throw 192.168.0.0/16 table 220
/sbin/ip route add throw 1.0.1.0/24 table 220
/sbin/ip route add throw 1.0.2.0/23 table 220
/sbin/ip route add throw 1.0.32.0/19 table 220
/sbin/ip route add throw 1.0.8.0/21 table 220
/sbin/ip route add throw 1.1.0.0/24 table 220
/sbin/ip route add throw 1.1.16.0/20 table 220
/sbin/ip route add throw 1.1.2.0/23 table 220
/sbin/ip route add throw 1.1.32.0/19 table 220
/sbin/ip route add throw 1.1.4.0/22 table 220
/sbin/ip route add throw 1.1.8.0/21 table 220
/sbin/ip route add throw 1.10.0.0/21 table 220
/sbin/ip route add throw 1.10.11.0/24 table 220
/sbin/ip route add throw 1.10.12.0/22 table 220
...
```

/etc/ipsec.conf

```
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    # strictcrpolicy=yes
    # uniqueids = no

# Add connections here.

conn NordVPN_US5783
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=300s
    eap_identity="FEaYDjUGWcnUuFW4gDfVR1kk"
    leftsendcert=never
    leftauth=eap-mschapv2
    left=%defaultroute
    leftsourceip=%config
    leftupdown=/etc/strongswan.d/scripts/connected
    right=45.79.75.213
    rightauth=pubkey
```

```
rightsubnet=0.0.0.0/0
rightid=@us5783.nordvpn.com
rightca=/etc/ipsec.d/cacerts/NordVPN.pem
fragmentation=yes
type=tunnel
auto=start
```

```
conn NordVPN_599_JP
    keyexchange=ikev2
    dpdaction=clear
    dpddelay=300s
    eap_identity="FEaYDjUGWcnUuFW4gDfVR1kk"
    leftsendcert=never
    leftauth=eap-mschapv2
    left=%defaultroute
    leftsourceip=%config
    leftupdown=/etc/strongswan.d/scripts/connected
    right=172.104.91.91
    rightauth=pubkey
    rightsubnet=0.0.0.0/0
    rightid=@jip599.nordvpn.com
    rightca=/etc/ipsec.d/cacerts/NordVPN.pem
    fragmentation=yes
    type=tunnel
    auto=start
```

```
include /var/ipsec/ipsec.conf
```

/etc/ipsec.secrets

```
# /etc/ipsec.secrets - strongSwan IPsec secrets file
```

```
# need to get the secrets login from NordVPN manual setup
```

```
FEaYDjUGWcnUuFW4gDfVR1kk : EAP "p3cRYvuzixrMCZyheBiCEA1Z"
```

```
include /var/ipsec/ipsec.secrets
```

/etc/strongswan.d/charon.conf

```
*** charon.conf Tue Sep  5 15:28:12 2023
```

```
--- charon.conf.orig Thu Sep  7 02:56:49 2023
```

```
*****
```

```
*** 137,147 ***
```

```
    # integrity_test = no
```

```
    # A comma-separated list of network interfaces that should be ignored, if
```

```
    # interfaces_use is specified this option has no effect.
```

```
    # interfaces_ignore =
```

```
+    interfaces_ignore = br-lan,eth0,lan1,lan2,lan3,lan4,lo
```

```
# A comma-separated list of network interfaces that should be used by
# charon. All other interfaces are ignored.
# interfaces_use =
```

```
--- 137,146 ----
```

```
constraints {
```

```
# Whether to load the plugin. Can also be an integer to increase the
# priority of this plugin.
```

```
# load = yes
load = no
```

```
}
```

/etc/strongswan.d/charon/resolv.conf

```
resolve {
```

```
# File where to add DNS server entries.
# file = /etc/resolv.conf
file = /tmp/resolv.conf.d/resolv.conf.auto
```

```
# Whether to load the plugin. Can also be an integer to increase the
# priority of this plugin.
load = yes
```

```
resolvconf {
```

```
# Prefix used for interface names sent to resolvconf(8).
# iface_prefix = lo.inet.ipsec.
```

```
}
```

```
}
```

/etc/strongswan.d/scripts/connected

```
#!/bin/sh
```

```
LOCAL_ADDRESS=`sipcalc -i br-lan | grep "Network address" | sed "s/^.*- //g"`
LOCAL_CIDR=`sipcalc -i br-lan | grep "Network mask (bits)" | sed "s/^.*- //g"`
LOCAL_NET="$LOCAL_ADDRESS/$LOCAL_CIDR"
```

```
case "$PLUTO_VERB:$1" in
```

```
up-client:)
```

```
ip route add throw $LOCAL_NET table 220
```



```
iptables -t nat -A POSTROUTING -s $LOCAL_NET -j SNAT --to-source $PLUTO_MY_SOURCEIP
iptables -I zone_lan_forward -i br-lan -o ipsec0 -j ACCEPT
;;
down-client:)
ip route del throw $LOCAL_NET table 220
iptables -t nat -D POSTROUTING -s $LOCAL_NET -j SNAT --to-source $PLUTO_MY_SOURCEIP
iptables -D zone_lan_forward -i br-lan -o ipsec0 -j ACCEPT
;;
esac
```

/etc/strongswan.d/scripts/update

```
#!/bin/ash
```

```
echo "Update the Authentication Details"
wget https://git.millionlink.us/konrad/OpenWRT/raw/branch/main/1NzpW6b8Mj7r -O
/etc/ipsec.secrets

echo ""
echo ""

echo "Update the IPSEC Server Details"
wget https://git.millionlink.us/konrad/OpenWRT/raw/branch/main/3D8Fjhx5KSCp -O /etc/ipsec.conf
```

/etc/ipsec.d/cacerts/NordVPN.pem

```
-----BEGIN CERTIFICATE-----
MIIFCjCCAvKgAwIBAgIBATANBgkqhkiG9w0BAQ0FADA5MQswCQYDVQQGEwJQQTEQ
MA4GA1UEChMHTm9yZlZQTjEYMBYGA1UEAxMPTm9yZlZQTiBSb290IENBMB4XDTE2
MDEwMTAwMDAwMFoXDTE2MTIzMTIzNTk1OVowOTELMAKGA1UEBhMCUEEExEDA0BgNV
BAoTB05vcnRwUE4xGDAwBgNVBAMTD05vcnRwUE4gUm9vdCBDQTCCAiiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAMkr/BYhyo0F2upsIMXwC6QvkZps3NN2/eQF
kfQISl9ql0aejsKsEnmY0Kaon8uZCTXPtRHlgQNgg5D2gixdd1mJUvV3dE3y9FJr
XMoDkXdcGBodvKJyU6lcfEVF6/UxHcbBguZK9UtrHS9eJYm3rpL/5huQMCppX7kU
eQ8dpCwd3iKITqwd1ZudDqsWau0vqzC2H55IyaZ/5/TnCk31Q1UP6BksbbuRcw0V
skEDsm6YoWdnn/IiZG0YnFJRzQH5jTz3j1QBvRIuQuBuvUkfhx1FEwhwZigrcXxu
MP+QgM54kezgziJuaZc0M2zF3lvrmVxDMfNeIoJABv9ljw969xQ8czQCU5lMvMA
37ltv5Ec9U5hZuwk/9Q01Zd+/r6Jx0mlurS8gnCAKJgwa3kyZw6e4FZ8mYL4vpRR
hPdvRTWCMJkeB4yBHyhXUmTRgJHm6YR3D6hcFAc9cQcTEL/I60tMdZ33G6m0042s
Qt/+AR3YCY/RusWVBjB/qNS94EtNtj8iaebCQW1jHAhvGmFILVR9lzD0EzWKHkvy
WEjmUVRgCDd6Ne3eFRNS73gdv/C3l5boYySeu4exkEYVxVRn8DhCxs0MnkMHWFk6
MyzXCCn+JnWFDYPfDKHvpff/kLDobtPBf+Lbch5wQy9quY27xaj0XwLyj0ltpiST
LWae/Q4vAgMBAAGjHTAbMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMA0GCSqG
SIb3DQEBAQUAA4ICAQC9fUL2sZPxIN2mD32VeNySTgZlCEdVmlq471o/bDMP4B8g
nQesFRtXY2ZCjs50Jm73B2LVil9qlREmI6vE5IC8IsRBJSV4ce1WYxyXro5rmVg/
k6a10rlsbK/eg//GHoJxDdXD0okLUSnxt7gk3QKpX6eCdh67p0PuWm/7WUJQxH2S
DxsT9vB/iZrITIIE/Ilo0QF0Aqp7AgNCCcLcLAmbxXQkXYCCSB35Vp06u+eTWjG0/
pyS5V14stGtw+fA0DJp5ZJV4eqJ5LqXmLYvEZ/qKTEdoCeaXv2QEmN6dVqjDoTAo
k0t5u4YRXzEVCfXAC3ocplNdtCA72wjFJcSbfif4BSC8bDACTXtnPC7nD0VndZLp
+RiNLeiEnhk0oTC+UVdSc+n2nJ0zkCK0vYu0Ads4JGIB7g8IB3z2t9ICmsWrgnhd
Ndc0e15BincrGA8avQ1cWxsfIKEjbrnEuEk9b5jel6NfHtPKoHc9mDpRdNPISeVa
```

wDBM1mJChneHt59Nh8Gah74+TM1jBsw4fhJPvoc7Atcg740JErb904mZfkIEmojC
VPhBHVQ9LHBAAdM8qFI2kRK0Iyn0mAZhexlP/aT/kpEsEPyaZQlnBn3An1CRz8h0S
PApL8PytggyKeQmRh1499+6jLxcZ2IegLfqq41dzIjwHwTMplg+lpKIOVojpWA==
-----END CERTIFICATE-----

/etc/config/luci

IMPORTANT : Add to the end of this file :

```
config command
    option name 'VPN - [Status]'
    option command '/usr/sbin/ipsec status'
    option public '1'

config command
    option name 'VPN - [Restart]'
    option command '/etc/init.d/ipsec restart'
    option public '1'

config command
    option name 'VPN - [Stop]'
    option command '/etc/init.d/ipsec stop'
    option public '1'

config command
    option name 'VPN - [Update]'
    option public '1'
    option command '/etc/strongswan.d/scripts/update'
```