ITUS
Networks

Shield Pro

OpenVPN Server
Setup Guide

This document assumes you are familiar with SSH/SCP and how to transfer files to/from your computer and that the Shields Web GUI is set in Advanced Mode. Also, as you progress through the setup please make note of all passwords, in a secure location, as there isn't a way to recover if lost.

Itus recommends using GRC's Ultra High Security Password Generator for generating the passwords required to setup OpenVPN: https://www.grc.com/passwords.htm

Step 1: Generate Necessary Directories/Files

1. At the Shield's command line copy & paste the below:

```
mkdir -p /etc/ssl/certs
mkdir -p /etc/ssl/crls
mkdir -p /etc/ssl/newcerts
mkdir -p /etc/ssl/private
touch /etc/ssl/index.txt
echo 01 > /etc/ssl/serial
```

Step 2: Update the CA_default section of the /etc/ssl/openssl.cnf file to match the below:

1. vi /etc/ssl/openssl.cnf (You could also utilize WinSCP)

```
[ CA_default ]

dir               = /etc/ssl                # Where everything is kept
certs             = $dir/certs              # Where the issued certs are kept
crl_dir           = $dir/certs              # Where the issued crl are kept
database          = $dir/index.txt          # database index file.
#unique_subject   = no
new_certs_dir     = $dir/newcerts           # default place for new certs.

certificate       = $dir/certs/ca.crt       # The CA certificate
serial            = $dir/serial             # The current serial number
crlnumber         = $dir/crlnumber          # the current crl number
crl              = $dir/crl.pem             # The current CRL
private_key      = $dir/certs/cakey.pem       # The private key
RANDFILE         = $dir/private/.rand        # private random number file
```

Step 3: Create the private key (cakey.pem)

1. cd /etc/ssl/certs
2. Enter OpenSSL by typing **openssl**
3. Within OpenSSL copy & paste the below:
   ```
   genrsa -aes256 -out cakey.pem 2048
   ```
4. Enter pass phrase for cakey.pem: ***<Enter New Unique Password Here>***

Step 4: Create the CA cert (ca.crt)

1. Within OpenSSL copy & paste the below:
   ```
   req -new -x509 -key cakey.pem -out ca.crt -days 365
   ```
2. Enter pass phrase for cakey.pem: ***<Enter Password from creating cakey.pem>***
3. Enter Requested Information:
   - Country Name (2 letter code) [AU]:
   - State or Province Name (full name) [Some-State]:
   - Locality Name (eg, city) []:
   - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
   - Organizational Unit Name (eg, section) []:

- Common Name (e.g. server FQDN or YOUR name) []:
- Email Address []:

Step 5: Create the OpenVPN server private key (server.key)

1. Within OpenSSL copy & paste the below:
   ```
   genrsa -aes256 -out server.key 2048
   ```
2. Enter pass phrase for server.key: ***<Enter New Unique Password Here>***

Step 6: Create the OpenVPN server cert signing request (server.csr)

1. Within OpenSSL copy & paste the below:
   ```
   req -out server.csr -new -key server.key
   ```
2. Enter pass phrase for server.key: ***<Enter Password from creating server.key>***
3. Enter Requested Information:
   - Country Name (2 letter code) [AU]:
   - State or Province Name (full name) [Some-State]:
   - Locality Name (eg, city) []:
   - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
   - Organizational Unit Name (eg, section) []:
   - Common Name (e.g. server FQDN or YOUR name) []:
   - Email Address []:
4. Enter a challenge password []: ***< Enter unique challenge password here, not same as above >***

Step 7: Create the OpenVPN server cert (server.crt)

1. Within OpenSSL copy & paste the below:
   ```
   ca -out server.crt -in server.csr -keyfile cakey.pem -cert ca.crt -policy policy_anything
   ```
2. Enter pass phrase for cakey.pem: ***<Enter Password from creating cakey.pem>***
3. Enter Requested Information:
   - Sign the certificate? [y/n]:
   - 1 out of 1 certificate requests certified, commit? [y/n]
   - Write out database with 1 new entries
   - Data Base Updated

Step 8: Create the cert signing request for each VPN client (<device name>-client.csr)

Note: Steps 8 & 9 will need to be repeated for each client you wish to have connect to the VPN

1. Within OpenSSL copy & paste the below:
   ```
   req -out <device name>-client.csr -new -keyout <device name>-client.key
   ```
2. Enter PEM pass phrase: ***<Enter New Unique Password Here>***
3. Enter Requested Information:
   - Country Name (2 letter code) [AU]:
   - State or Province Name (full name) [Some-State]:
   - Locality Name (eg, city) []:
   - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
   - Organizational Unit Name (eg, section) []:
   - Common Name (e.g. server FQDN or YOUR name) []:
   - Email Address []:
4. Enter a challenge password []: ***< Enter unique challenge password here, not same as above >***

Step 9: Create the cert for each VPN client (<device name>-client.crt)

1. Within OpenSSL copy & paste the below:
   ```
   ca -out <device name>-client.crt -in <device name>-client.csr -keyfile cakey.pem -cert ca.crt -policy policy_anything
   ```
2. Enter pass phrase for cakey.pem: **<Enter Password from creating cakey.pem>**
3. Enter Requested Information:
   - Sign the certificate? [y/n]: Y
   - 1 out of 1 certificate requests certified, commit? [y/n] Y
   - Data Base Updated

Step 10: Create Diffie-Hellman Parameters

1. Within OpenSSL copy & paste the below: (Note: This is going to take a long time)
   ```
   dhparam -out dh2048.pem 2048
   ```
2. Exit OpenSSL by typing **exit**

Step 11: Change Permissions on generated certs & keys

1. *At the command line copy & paste the below:*
   ```
   chmod 600 /etc/ssl/certs/*
   ```

Step 12: Create VPN Interface

1. At the command line copy & paste the below:
   ```
   uci set network.vpn0=interface
   uci set network.vpn0.ifname=tun0
   uci set network.vpn0.proto=none
   ```

Step 13: Create VPN Firewall rule

Note: If running in Bridge mode you will need to forward UDP port 1194 to the LAN IP of the Shield.

1. At the command line copy & paste the below:
   ```
   uci add firewall rule
   uci set firewall.@rule[-1].name=Allow-OpenVPN-Inbound
   uci set firewall.@rule[-1].target=ACCEPT
   uci set firewall.@rule[-1].src=*
   uci set firewall.@rule[-1].proto=udp
   uci set firewall.@rule[-1].dest_port=1194
   ```

Step 14: Create VPN Firewall zone

1. At the command line copy & paste the below:
   ```
   uci add firewall zone
   uci set firewall.@zone[-1].name=vpn
   uci set firewall.@zone[-1].input=ACCEPT
   uci set firewall.@zone[-1].forward=ACCEPT
   uci set firewall.@zone[-1].output=ACCEPT
   uci set firewall.@zone[-1].network=vpn0
   ```

Step 15: Redirect All Blocked Domains On The VPN To Shield

Note: Items you will need to change are marked in **bold** below.

Shield Block IP : To calculate this take the Shields LAN/Web GUI IP and increment the 4th octet by one. Example: 10.10.10.10 → 10.10.10.11

1. At the command line copy & paste the below:

   ```
   uci add firewall redirect
   uci set firewall.@redirect[-1].target=DNAT
   uci set firewall.@redirect[-1].src=vpn
   uci set firewall.@redirect[-1].proto=tcp
   uci set firewall.@redirect[-1].src_dip=<Shield Block IP>
   uci set firewall.@redirect[-1].src_dport=80
   uci set firewall.@redirect[-1].dest_ip=<Shield Block IP>
   uci set firewall.@redirect[-1].dest_port=88
   uci set firewall.@redirect[-1].dest=lan
   uci set firewall.@redirect[-1].name=vpn-Itusfilter
   ```

Step 16: Redirect all DNS Traffic On The VPN To Shield

Note: Items you will need to change are marked in **bold** below.

1. At the command line copy & paste the below:

   ```
   uci add firewall redirect
   uci set firewall.@redirect[-1].target=DNAT
   uci set firewall.@redirect[-1].src=vpn
   uci set firewall.@redirect[-1].proto=tcpudp
   uci set firewall.@redirect[-1].src_dip=any
   uci set firewall.@redirect[-1].src_dport=53
   uci set firewall.@redirect[-1].dest_ip=<Shield LAN/Web GUI IP>
   uci set firewall.@redirect[-1].dest_port=53
   uci set firewall.@redirect[-1].dest=lan
   uci set firewall.@redirect[-1].name='vpn-dns-traffic-to-shield'
   ```

Step 17: Commit Changes

1. At the command line copy & paste the below:

   ```
   uci commit network
   /etc/init.d/network reload
   uci commit firewall
   /etc/init.d/firewall reload
   ```

Step 18: Configure Dnsmasq To Respond To VPN DNS Queries

1. Edit the /etc/config/dhcp file and comment out or remove the below line

   ```
   option localservice '1'
   ```

2. Restart Dnsmasq

   ```
   /etc/init.d/dnsmasq restart
   ```

Step 19: Configure OpenVPN

Note: If the Shield is not on the 10.10.10.X network change the items marked in **bold** below.

1. At the command line copy & paste the below:

   ```
   echo >> /etc/config/openvpn
   uci set openvpn.SSLVPN_Server=openvpn
   uci set openvpn.SSLVPN_Server.enabled=1
   uci set openvpn.SSLVPN_Server.dev=tun
   uci set openvpn.SSLVPN_Server.port=1194
   uci set openvpn.SSLVPN_Server.proto=udp
   uci set openvpn.SSLVPN_Server.keepalive='10 120'
   uci set openvpn.SSLVPN_Server.log=/tmp/openvpn.log
   uci set openvpn.SSLVPN_Server.verb=3
   uci set openvpn.SSLVPN_Server.server='10.8.0.0 255.255.255.0'
   uci set openvpn.SSLVPN_Server.push='route 10.10.10.0 255.255.255.0'
   uci set openvpn.SSLVPN_Server.askpass=/etc/openvpn/cert.pass
   uci commit openvpn
   ```

Step 20: Configure OpenVPN Certificate Password

1. At the command line copy & paste the below:

   ```
   mkdir -p /etc/openvpn/
   touch /etc/openvpn/cert.pass
   chmod 600 /etc/openvpn/cert.pass
   echo Replace with Password from Step 5 creating server.key > /etc/openvpn/cert.pass
   ```

Step 21: Download Certs And Keys To Your Computer

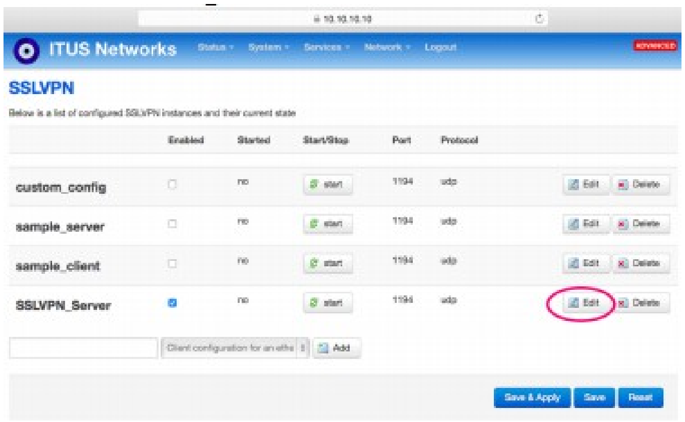
1. Utilizing your favorite SCP client download the below files to your computer
   - /etc/ssl/certs
     - ca.crt
     - dh2048.pem
     - server.crt
     - server.key
     - <device>-client.crt
     - <device>-client.key

Step 22: Upload Certs And Keys To SSLVPN Server Instance

1. Login to Shield Web GUI

2. Select **Services** then **SSLVPN** from the menu

3. Edit the **SSLVPN_Server instance**



SSLVPN

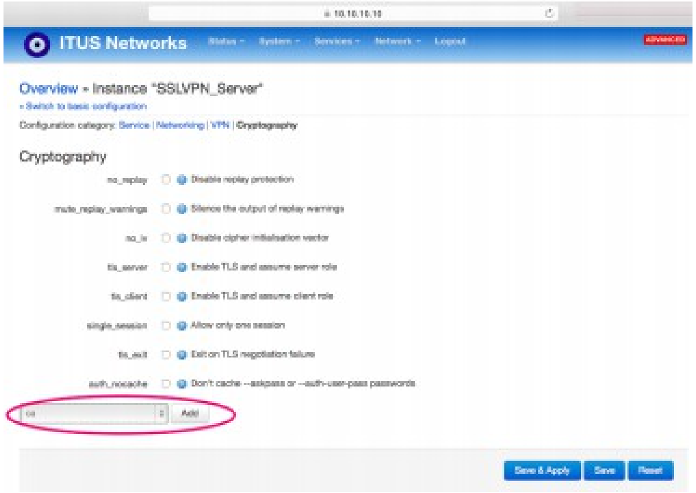
Below is a list of configured SSLVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	□	no	start	1194	udp	Edit Delete
sample_server	□	no	start	1194	udp	Edit Delete
sample_client	□	no	start	1194	udp	Edit Delete
SSLVPN_Server	☑	no	start	1194	udp	Edit Delete

4. Click **Switch to advanced configuration**

5. Click **Cryptography**

6. Choose **ca** from the drop down list and click **add**



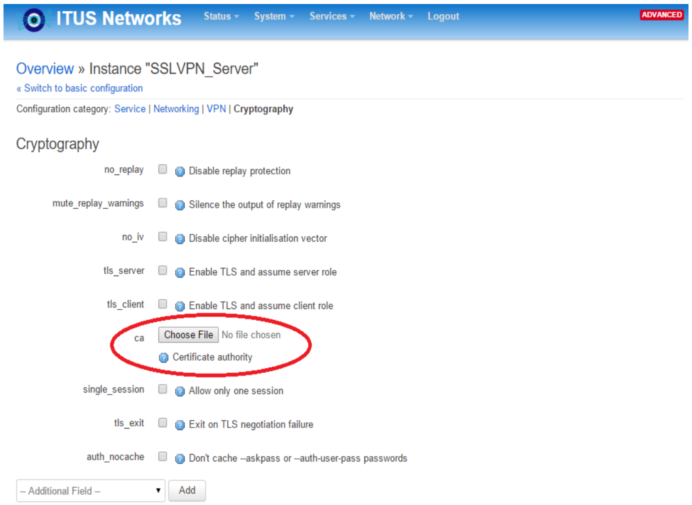
Overview » Instance "SSLVPN_Server"
« Switch to basic configuration
Configuration category: Service | Networking | VPN | Cryptography

Cryptography

no_replay □ Disable replay protection
mute_replay_warnings □ Silence the output of replay warnings
no_iv □ Disable cipher initialisation vector
tls_server □ Enable TLS and assume server role
tls_client □ Enable TLS and assume client role
single_session □ Allow only one session
tls_exit □ Exit on TLS negotiation failure
auth_nocache □ Don't cache --askpass or --auth-user-pass passwords

ca

7. Click **Choose File** next to **ca** and upload **ca.crt**



Overview » Instance "SSLVPN_Server"
« Switch to basic configuration
Configuration category: Service | Networking | VPN | Cryptography

Cryptography

no_replay □ Disable replay protection
mute_replay_warnings □ Silence the output of replay warnings
no_iv □ Disable cipher initialisation vector
tls_server □ Enable TLS and assume server role
tls_client □ Enable TLS and assume client role
ca Choose File No file chosen
Certificate authority
single_session □ Allow only one session
tls_exit □ Exit on TLS negotiation failure
auth_nocache □ Dont cache --askpass or --auth-user-pass passwords

8. Click **Save & Apply** when finished.

9. Choose **dh** from the drop down list and click **add**

10. Click **Choose File** next to **dh** and upload **dh2048.pem**

11. Click **Save & Apply** when finished.

12. Choose **cert** from the drop down list and click **add**

13. Click **Choose File** next to **cert** and upload **server.crt**

14. Click **Save & Apply** when finished.

15. Choose **key** from the drop down list and click **add**

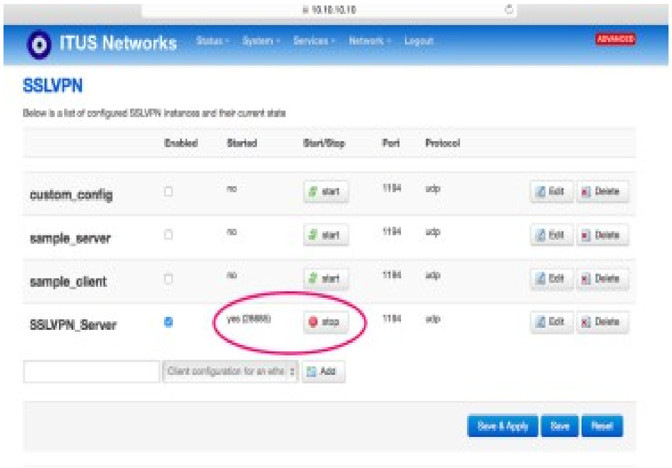
16. Click **Choose File** next to **key** and upload **server.key**

17. Click **Save & Apply** when finished.

18. Check **auth_nocache**

19. Click **Save & Apply** when finished.

20. Select **Overview** to return to the SSLVPN overview page and click start to **start** the SSLVPN_Server service. If the SSLVPN_Server service is already started, click **stop** and then **start** to restart it



SSLVPN

Below is a list of configured SSLVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	□	no	start	1194	udp	Edit Delete
sample_server	□	no	start	1194	udp	Edit Delete
sample_client	□	no	start	1194	udp	Edit Delete
SSLVPN_Server	☑	yes (28885)	stop	1194	udp	Edit Delete

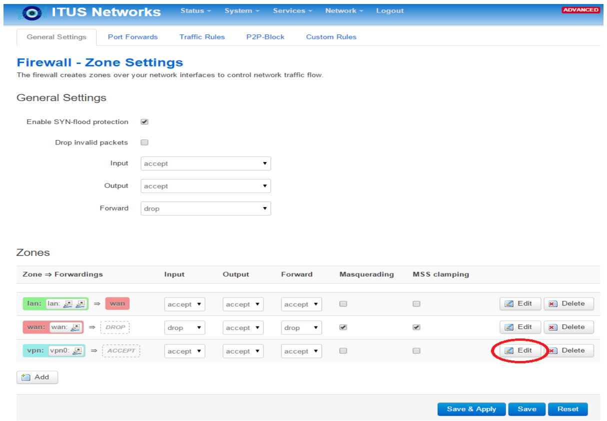
Step 23: Allow VPN Traffic Through WAN Connection

Note: You can skip this step if you do not want/need your OpenVPN clients to have access to the internet/WAN while connected.

1. Login to Shield Web GUI

2. Select **Network** then **Firewall** from the menu

3. Edit the **vpn: vpn0 Zone**



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

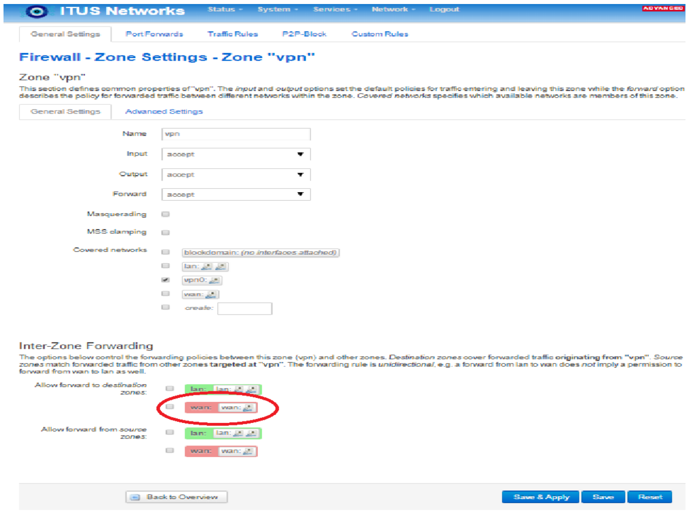
Output: accept

Forward: drop

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	accept	accept	accept	☐	☐	Edit Delete
wan: wan: ⇒ DROP	drop	accept	drop	☑	☑	Edit Delete
vpn: vpn0: ⇒ ACCEPT	accept	accept	accept	☐	☐	Edit Delete

4. Under **Inter-Zone Forwarding** next to **Allow forward to destination zones** check **wan**



Firewall - Zone Settings - Zone "vpn"

Zone "vpn"

This section defines common properties of "vpn". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: vpn

Input: accept

Output: accept

Forward: accept

Masquerading ☐

MSS clamping ☐

Covered networks:
☐ blockdomain: *(no interfaces attached)*
☐ lan:
☑ vpn0:
☐ wan:
☐ *create:*

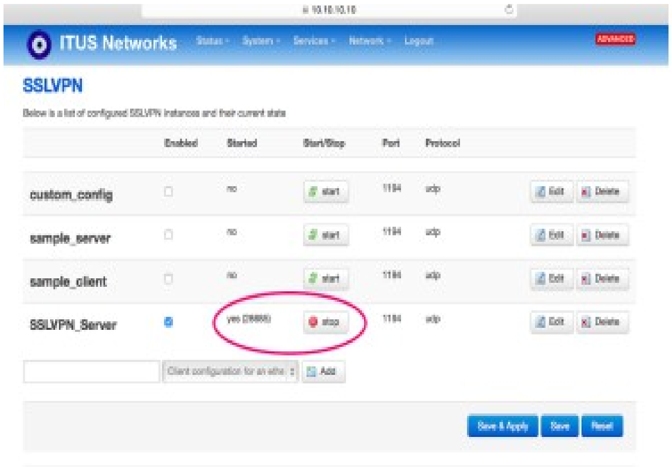
Inter-Zone Forwarding

The options below control the forwarding policies between this zone (vpn) and other zones. *Destination zones* cover forwarded traffic **originating from "vpn"**. *Source zones* match forwarded traffic from other zones **targeted at "vpn"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to destination zones:
☐ lan: lan:
☐ wan: wan:

Allow forward from source zones:
☐ lan: lan:
☐ wan: wan:

5. Click **Save & Apply** when finished.



SSLVPN

Below is a list of configured SSLVPN instances and their current state

	Enabled	Started	Start/Stop	Port	Protocol	
custom_config	☐	no	start	1194	udp	Edit Delete
sample_server	☐	no	start	1194	udp	Edit Delete
sample_client	☐	no	start	1194	udp	Edit Delete
SSLVPN_Server	☑	yes (26880)	stop	1194	udp	Edit Delete

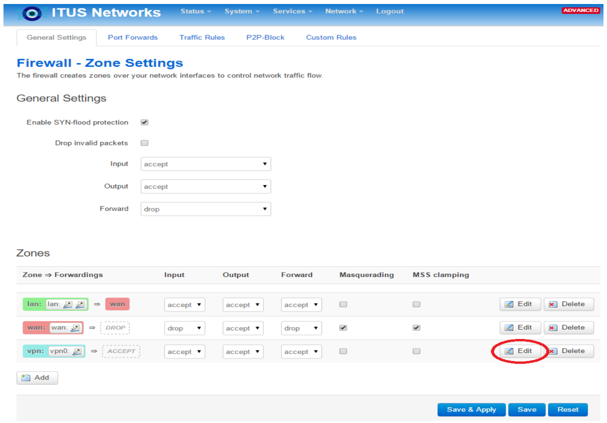
Step 24: Allow VPN Traffic To Other Devices Within Your Network

Note: You can skip this step if you do not want/need your OpenVPN clients to have access to the other devices within your network while connected.

1. Login to Shield Web GUI

2. Select **Network** then **Firewall** from the menu

3. Edit the **vpn: vpn0 Zone**



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

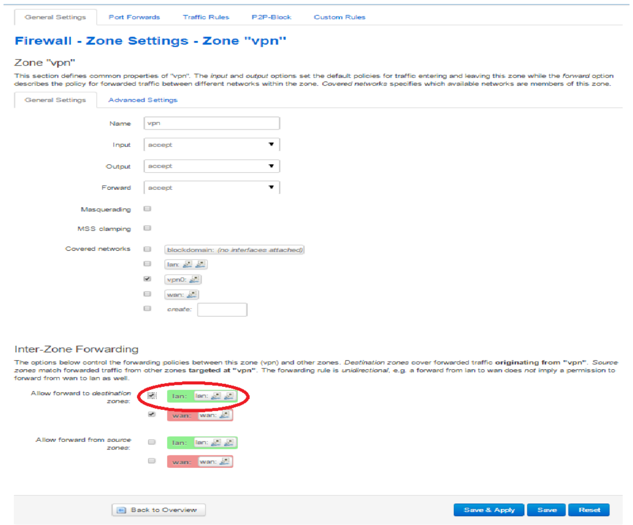
Output: accept

Forward: drop

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan: lan: ⇒ wan	accept	accept	accept	☐	☐	Edit	Delete
wan: wan: ⇒ DROP	drop	accept	drop	☑	☑	Edit	Delete
vpn: vpn0: ⇒ ACCEPT	accept	accept	accept	☐	☐	Edit	Delete

6. Under **Inter-Zone Forwarding** next to **Allow forward to destination zones** check **lan**



Firewall - Zone Settings - Zone "vpn"

Zone "vpn"

This section defines common properties of "vpn". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: vpn

Input: accept

Output: accept

Forward: accept

Masquerading ☐

MSS clamping ☐

Covered networks:
☐ blockdomain: *(no interfaces attached)*
☐ lan:
☑ vpn0:
☐ wan:
☐ *create:*

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (vpn) and other zones. *Destination zones* cover forwarded traffic **originating from "vpn"**. *Source zones* match forwarded traffic from other zones **targeted at "vpn"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to destination zones:
☑ lan: lan:
☑ wan: wan:

Allow forward from source zones:
☐ lan: lan:
☐ wan: wan:

7. Click **Save & Apply** when finished.

Step 25: Setup Dynamic DNS

1. Create account/hostname at noip.com

2. Login to Shield Web GUI

3. Select **Services** then **Dynamic DNS** from the menu

4. Edit the **myddns_ipv4** configuration

5. Check **Enabled**

6. Set **DDNS Service Provider** to **No-IP.com**

7. Enter **Hostname/Domain** created during the noip.com registration process

8. Enter **Username & Password** created during the noip.com registration process

9. Click **Save & Apply** when finished.

10. **Start** the **mydddns_ipv4** configuration

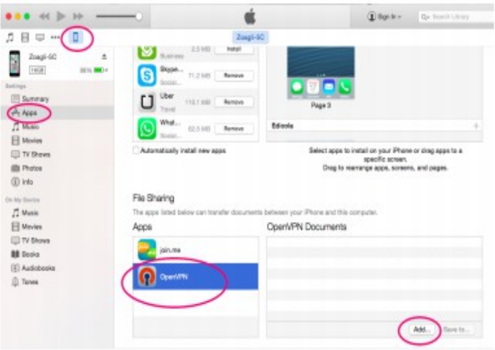
    Note: If myddns fails to start you can view the log file by clicking edit and selecting Log File Viewer

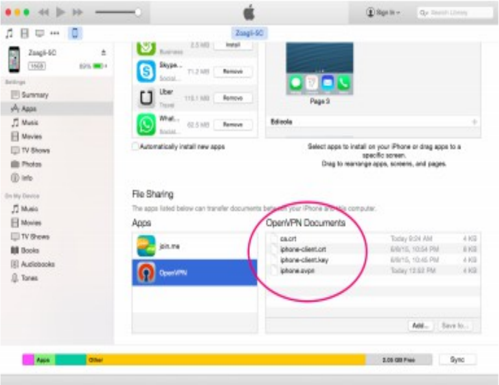
Step 26: OpenVPN Client Configuration

- **Configure OpenVPN client for iPhone**
  1. Install the OpenVPN Connect client from the App Store
  2. Create a text file called **iphone.ovpn** with the following entries.
     a. Items you will need to change are marked in **bold** below.
     b. The entry ***<no-ip.com hostname>*** needs to resolve to the Shield's WAN IP
     c. If you do not want to direct all traffic through the VPN you can remove "redirect-gateway"

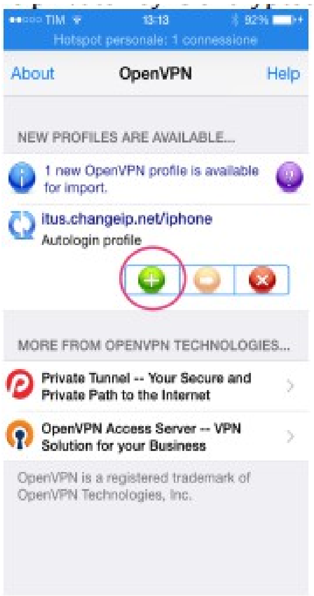
     ```
     redirect-gateway
     dev tun
     tls-client
     float
     remote <no-ip.com hostname> 1194
     pull
     proto udp
     reneg-sec 3600
     ca ca.crt
     cert iphone-client.crt
     key iphone-client.key
     ```

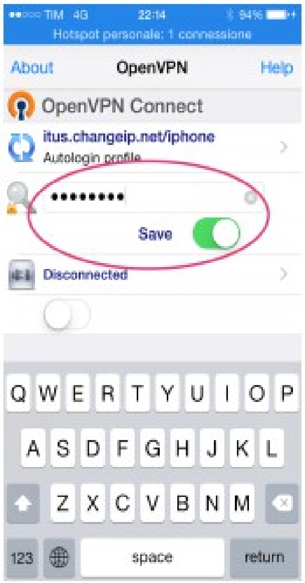
  3. Using iTunes Sync, select the **iphone device** > **Apps** > **OpenVPN** > **Add** in order to upload iphone.ovpn, ca.crt, iphone-client.crt, and iphone-client.key


Zoagli-5C
Summary
Apps
Music
Movies
TV Shows
Photos
Info
Skype
Uber
WhatsApp
Automatically install new apps
Page 3
Select apps to install on your iPhone or drag apps to a specific screen.
Drag to rearrange apps, screens, and pages.
File Sharing
The apps listed below can transfer documents between your iPhone and this computer.
Apps
OpenVPN Documents
join.me
OpenVPN
Add...
Save to...

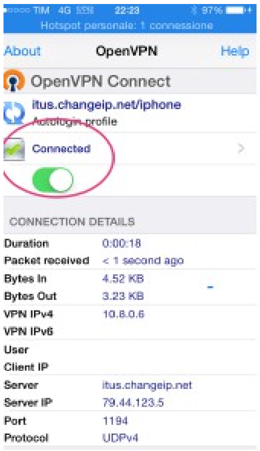


4. In the OpenVPN Connect app, click the plus sign to add the iphone profile. You will be prompted to enter the password from when you created the <device name>-client.csr during Step 8.


TIM
13:13
92%
Hotspot personale: 1 connessione
About
OpenVPN
Help
NEW PROFILES ARE AVAILABLE...
1 new OpenVPN profile is available for import.
itus.changeip.net/iphone
Autologin profile
MORE FROM OPENVPN TECHNOLOGIES...
Private Tunnel -- Your Secure and Private Path to the Internet
OpenVPN Access Server -- VPN Solution for your Business
OpenVPN is a registered trademark of OpenVPN Technologies, Inc.



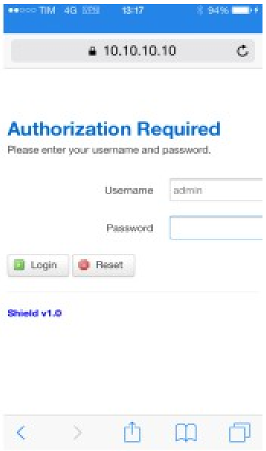
5. In the OpenVPN Connect client, click the button to connect. Once connected, you should be able to access the internal network.



itus.changeip.net/iphone
Autologin profile
Connected

CONNECTION DETAILS

```
Duration          0:00:18
Packet received   < 1 second ago
Bytes In          4.52 KB
Bytes Out         3.23 KB
VPN IPv4          10.8.0.6
VPN IPv6
User
Client IP
Server            itus.changeip.net
Server IP         79.44.123.5
Port              1194
Protocol          UDPv4
```



Authorization Required

Please enter your username and password.

Username admin

Password

Shield v1.0

- **Configure OpenVPN client for Windows**

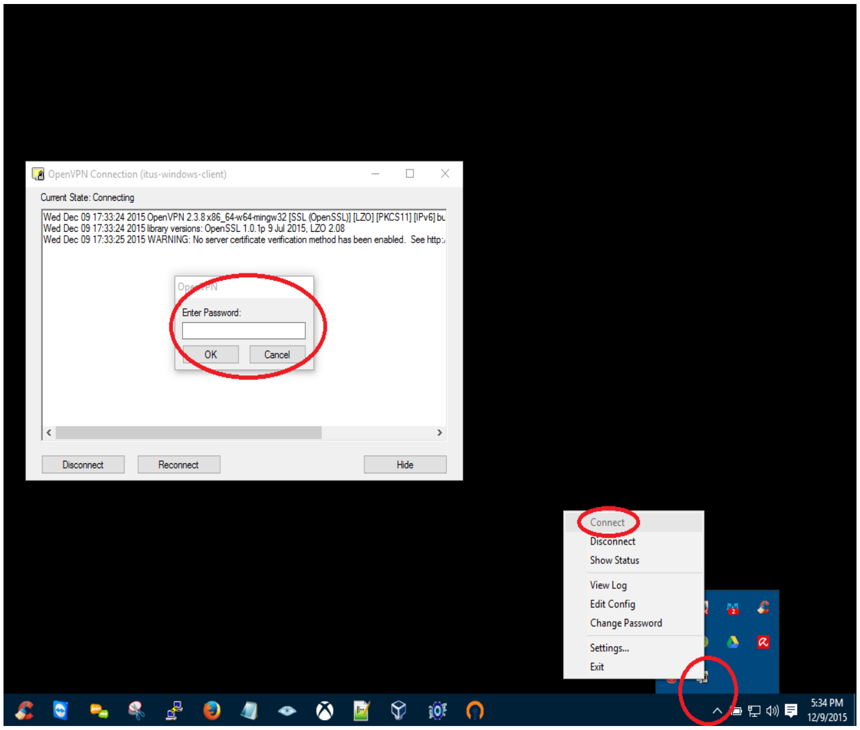
6. Download and install OpenVPN keeping all defaults during installation https://openvpn.net/index.php/open-source/downloads.html

7. Create a text file called **windows.ovpn** with the following entries.
   a. Items you will need to change are marked in **bold** below.
   b. The entry ***<no-ip.com hostname>*** needs to resolve to the Shield's WAN IP
   c. If you do not want to direct all traffic through the VPN you can remove "redirect-gateway"

```
redirect-gateway
dev tun
tls-client
float
remote <no-ip.com hostname>1194
pull
proto udp
reneg-sec 3600
ca ca.crt
cert windows-client.crt
key windows-client.key
```

8. Copy **windows.ovpn, ca.crt, windows-client.crt, and windows-client.key** to the **C:\Program Files\OpenVPN\config** directory

9. Launch **OpenVPN GUI**, it goes to the system tray, and click **Connect.** You will be prompted to enter the password from when you created the <device name>-client.csr during Step 8.



```
Wed Dec 09 17:33:24 2015 OpenVPN 2.3.8 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [PKCS11] [IPv6] bu
Wed Dec 09 17:33:24 2015 library versions: OpenSSL 1.0.1p 9 Jul 2015, LZO 2.08
Wed Dec 09 17:33:25 2015 WARNING: No server certificate verification method has been enabled.  See http:/
```

- **Configure the Tunnelblick client for Mac OS X**

1. Install the tunnelblick client for Mac OS X

2. Create a text file called **mac.ovpn** with the following entries.

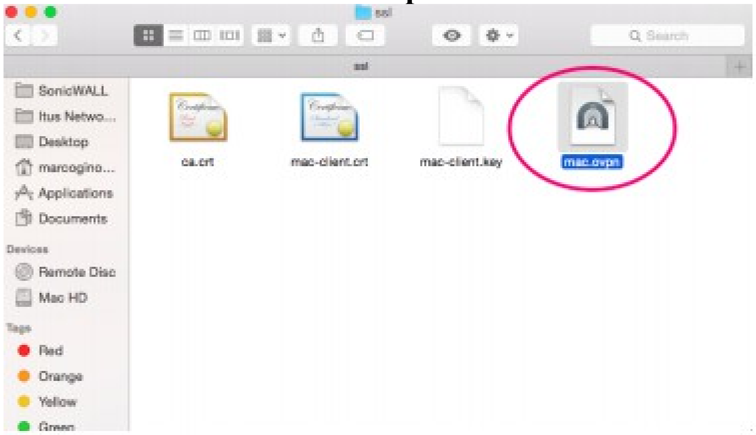
a. Items you will need to change are marked in **bold** below.

b. The entry ***<no-ip.com hostname>*** needs to resolve to the Shield's WAN IP

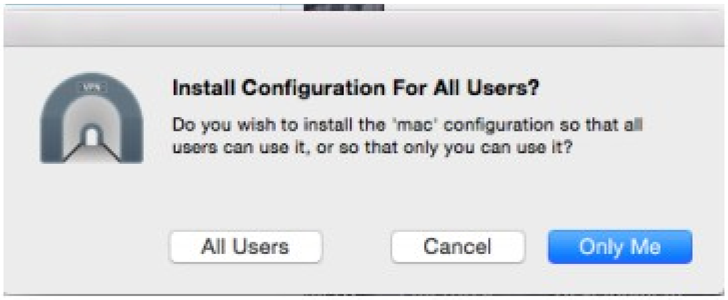
c. If you do not want to direct all traffic through the VPN you can remove "redirect-gateway"

```
redirect-gateway
dev tun
tls-client
remote <no-ip.com hostname>1194
pull
proto udp
reneg-sec 3600
ca /users/<username>/ssl/ca.crt
cert /users/<username>/ssl/mac-client.crt
key /users/<username>/ssl/mac-client.key
```

3. Put **ca.crt, mac-client.key, mac-client.crt, and mac.ovpn** in the /users/**<username>**/ssl/ folder and double-click the **mac.ovpn** file

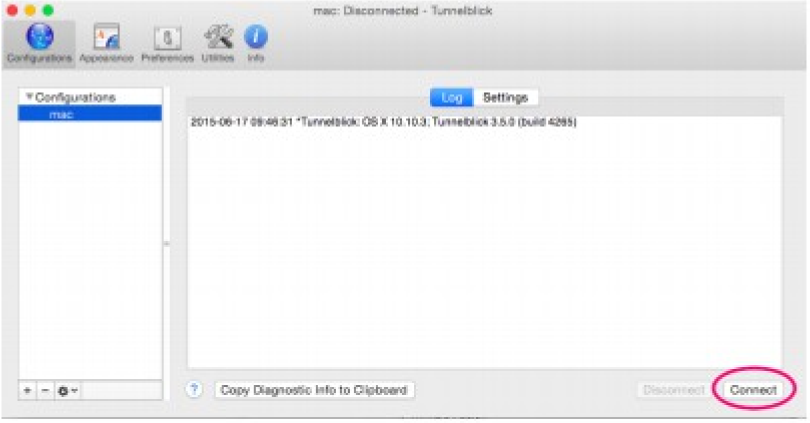


4. Select **Only Me** to install the configuration file. Enter your Mac OS X password when prompted



Install Configuration For All Users?

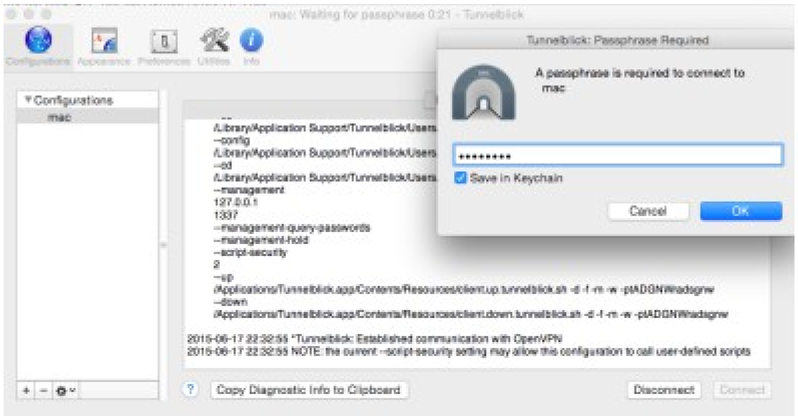
Do you wish to install the 'mac' configuration so that all users can use it, or so that only you can use it?



```
2015-06-17 09:46:31 *Tunnelblick: OS X 10.10.3; Tunnelblick 3.5.0 (build 4265)
```

5. Launch the Tunnelblick client and select **Connect**

6. You will be prompted to enter the password from when you created the <device name>-client.csr during Step 8.


mac: Waiting for passphrase 0:21 - Tunnelblick
Configurations
Appearance
Preferences
Utilities
Info
Configurations
mac
Tunnelblick: Passphrase Required
Cancel
OK
Copy Diagnostic Info to Clipboard
Disconnect
Connect

A passphrase is required to connect to mac

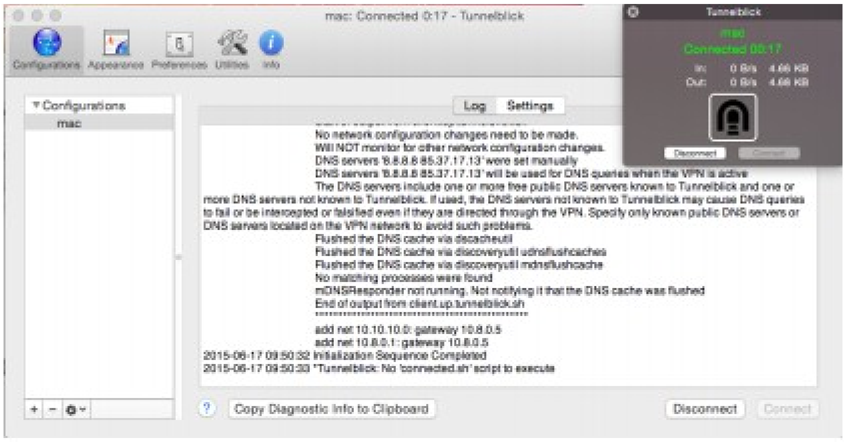
`*********`

☑ Save in Keychain

```
              /Library/Application Support/Tunnelblick/Users
              --config
              /Library/Application Support/Tunnelblick/Users
              --cd
              /Library/Application Support/Tunnelblick/Users
              --management
              127.0.0.1
              1337
              --management-query-passwords
              --management-hold
              --script-security
              2
              --up
              /Applications/Tunnelblick.app/Contents/Resources/client.up.tunnelblick.sh -d -f -m -w -ptADGNWradsgnw
              --down
              /Applications/Tunnelblick.app/Contents/Resources/client.down.tunnelblick.sh -d -f -m -w -ptADGNWradsgnw

2015-06-17 22:32:55 *Tunnelblick: Established communication with OpenVPN
2015-06-17 22:32:55 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
```

7. Once connected, you should be able to access the internal network



mac
Connected 00:17
In: 0 B/s 4.66 KB
Out: 0 B/s 4.66 KB

```
                         No network configuration changes need to be made.
                         Will NOT monitor for other network configuration changes.
                         DNS servers '8.8.8.8 85.37.17.13' were set manually
                         DNS servers '8.8.8.8 85.37.17.13' will be used for DNS queries when the VPN is active
                         The DNS servers include one or more free public DNS servers known to Tunnelblick and one or
more DNS servers not known to Tunnelblick. If used, the DNS servers not known to Tunnelblick may cause DNS queries
to fail or be intercepted or falsified even if they are directed through the VPN. Specify only known public DNS servers or
DNS servers located on the VPN network to avoid such problems.
                         Flushed the DNS cache via dscacheutil
                         Flushed the DNS cache via discoveryutil udnsflushcaches
                         Flushed the DNS cache via discoveryutil mdnsflushcache
                         No matching processes were found
                         mDNSResponder not running. Not notifying it that the DNS cache was flushed
                         End of output from client.up.tunnelblick.sh
                         **********************************************
                         add net 10.10.10.0: gateway 10.8.0.5
                         add net 10.8.0.1: gateway 10.8.0.5
2015-06-17 09:50:32 Initialization Sequence Completed
2015-06-17 09:50:33 *Tunnelblick: No 'connected.sh' script to execute
```