FreeNAS Remote Access via an Untangle Firewall

The purpose of this How-to is to document the installation; configuration and testing of the UnTangle firewall solution in regards to providing secure remote access to FreeNAS via a free Firewall / VPN solution.

The forum includes several suggestions about how to gain remote access to your FreeNAS server, this is just ***one more way*** that you can access the web interface, the console via SSH or even mount shares remotely. Depending on your upstream and downstream bandwidth your mileage may vary remotely mounting shares, but it can be done.

To be completely transparent, I use Untangle personally at home with my family, I use it in my offices and I deploy it and manage it for companies that do not have the internal IT resources to do so themselves. Most of my friend's homes have Untangle deployed as well! I do not work for Untangle and I do not sell Untangle – I send people to an online reseller to get their licenses. I am also absolutely certain that the same thing I am showing here can be accomplished using Pfsense, Tomato, Smoothwall, Streisand, or any number of other firewall applications or solutions.

What is Untangle?

My preferred method of accessing any of my equipment is via VPN and Untangle provides (for free in most cases) the perfect solution for doing this simply and easily. Untangle is a software solution that you install onto a dedicated computer or VM. Depending on your network traffic and what you are going to do with the firewall this can be a very simple single processor computer with 1GB of RAM, 80GB hard drive and two network cards. I manage a fair number of Untangle firewalls for my friends ranging in size from very small (ie – my home) to very large (1,500 network devices and over 2,000 people). Untangle provides the basic firewall and several other packages *completely for free*. This includes:

- Firewall
- OpenVPN VPN Server
- Virus Blocker Lite
- Phish Blocker
- Web Monitor
- Spam Blocker Lite
- Application Control Lite
- Ad Blocker
- Captive Portal
- Tunnel VPN
- Reports

If you opt to pay for Untangle, then it upgrades various components to full commercial version such as the Virus and Spam blockers and Application Control (think deep packet inspection) and adds the following additional components:

- Web Filter
- SSL Inspector
- Web Caching
- Bandwidth Control (Full QOS)
- WAN Balancer
- WAN Failover

- IPsec VPN (persistent VPN tunnels with routing)
- Policy Manager
- AD Directory Connector
- Live Support
- Branding Manager

For home users, Untangle provides a full license for all available applications for $50 *per year - total*. It is an amazing deal if you need or want some of the nicer applications. We have four kids still at home and I can tell you that the web filtering, application control, policy manager and bandwidth control are absolutely essential in our house, otherwise the kids and their friends will dominate our network and our bandwidth and my Plex watching will suffer! Captive Portal is also an invaluable tool for allowing our kid's friends limited access to our network without having to give out our WiFi passwords all the time.

In short, Untangle is a very powerful firewall and network management software platform that you can pay for - however, in order to follow these instructions, you do not have to pay a single penny for Untangle, *everything you will need is built into the free version*.

Included with Untangle is a very informative dashboard. They have a demo server setup that you can go take a look at and play around with – you can find it here:

http://demo.untangle.com/admin/index.do

Hardware Requirements

Like any firewall solution, there are many different ways to deploy a firewall and I will be going through a very simple installation. Depending on the situation, I run some of my Untangle installs in a VM using Proxmox. I have quite a few installs running under Proxmox now and they all run well. There have been discussions about the pros and cons of running Untangle (and other) firewall solutions within a virtual environment, so I would highly recommend that you do some research and decide for yourself if the pros and cons of virtualizing your firewall meet your needs. In my main Proxmox Untangle install, I use Untangle to provide firewalling services for all of my VMs as opposed to using the built-in Proxmox firewall. My reasoning is that I know Untangle very well and it works well for me in this configuration.

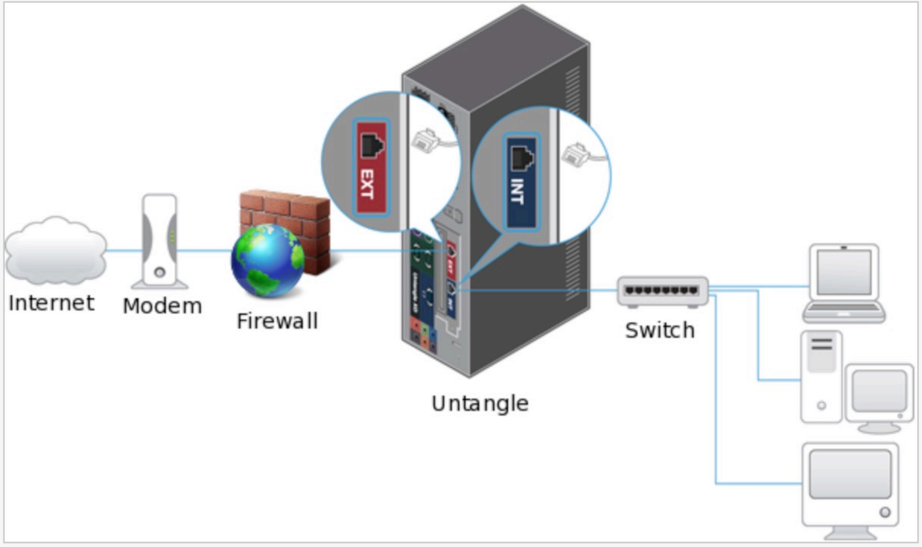
Other installations I run on small-dedicated firewall appliances that are available all over the Internet. Here is just one example. At home we have Cox GigaBlast with a 1Gbps connection. I use the Intel i5 version of this firewall with Untangle and get over 900Mbps download speeds. For most people, you will not need this powerful of a box for your firewall.

I have one installation that runs on a Dual Xeon system with mirrored 1TB SSD drives and 512GB of ram. This install secures over 1,500 network devices and 2,000 people. It is one of the larger installs according to Untangle.

Untangle is a Linux box, so pretty much anything that will run Linux will run Untangle, including that 5-year-old Dell Optiplex with 2GB of ram and 300GB hard drive. But it will need two network cards!

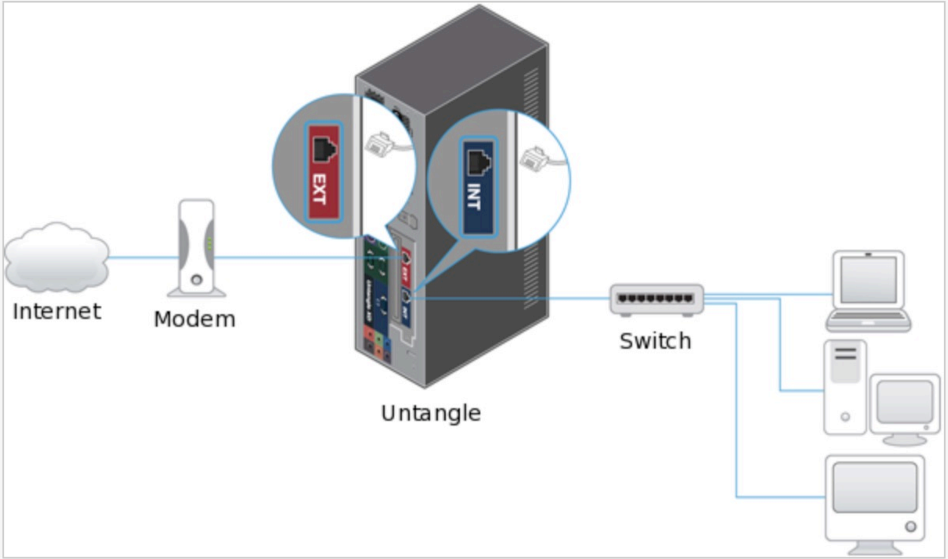
Deployment Strategies

Untangle can be installed in one of two ways. The first is a transparent bridge and is generally designed to be used if you already have a firewall device and you just want to add in the Untangle device to handle your VPN connections.



Untangle in Bridge mode

The second is in routed mode and is recommended if the external connection on the firewall is going to be directly connected to your Internet connection (cable modem, DSL, etc). This How-To will focus on this particular configuration.



Untangle in Router mode

Further information about deployment strategies can be found on the Untangle WiKi.

Downloading

When you download the Untangle firewall you can use all applications for free for 14 days before Untangle disables the paid elements. Regardless of if you are going to use the paid or free version, the download is the same. To download the latest version, please visit:

https://www.untangle.com/get-untangle/

As of March 14, 2018 the latest version is 13.2 and this document is based on this version.

You should download the 32-bit version if your firewall appliance had 4GB of memory or less or download the 64-bit version if your appliance has over 4GB of memory. It is interesting to note that Untangle can also run on the Linksys WRT 1900ACS. I have never played with that device, but it is supported. Next choose ISO (if you plan on burning to CD or installing on a VM) or IMG if you plan on installing from a USB device. Once your download is complete, create your bootable media and insert it into your device.

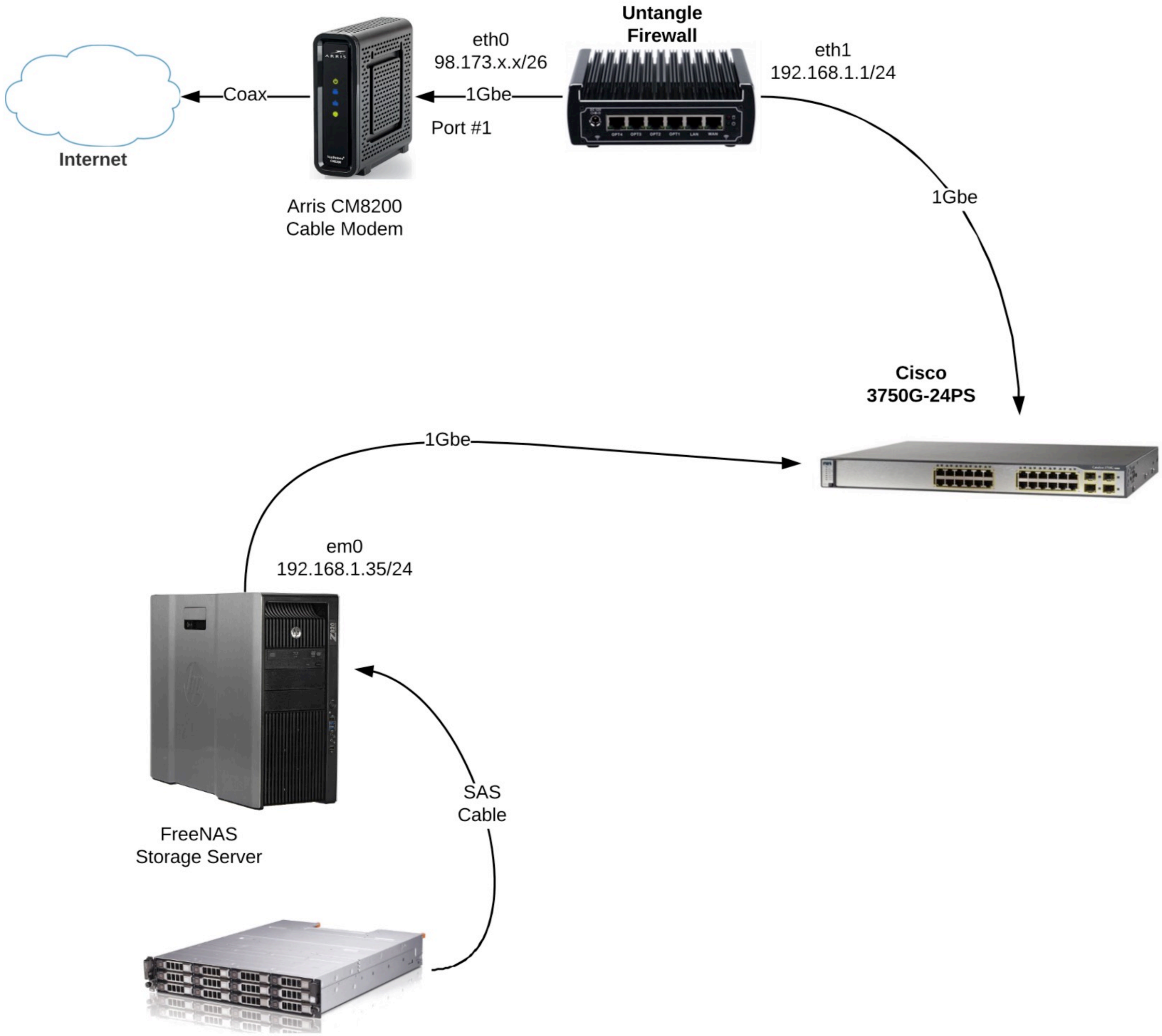
Installation

CAUTION: *The installation will **WIPE** your **ENTIRE** hard drive. Do not attempt to install it on a system you "dual boot" or use for some other purpose; you WILL lose ALL of your data!*

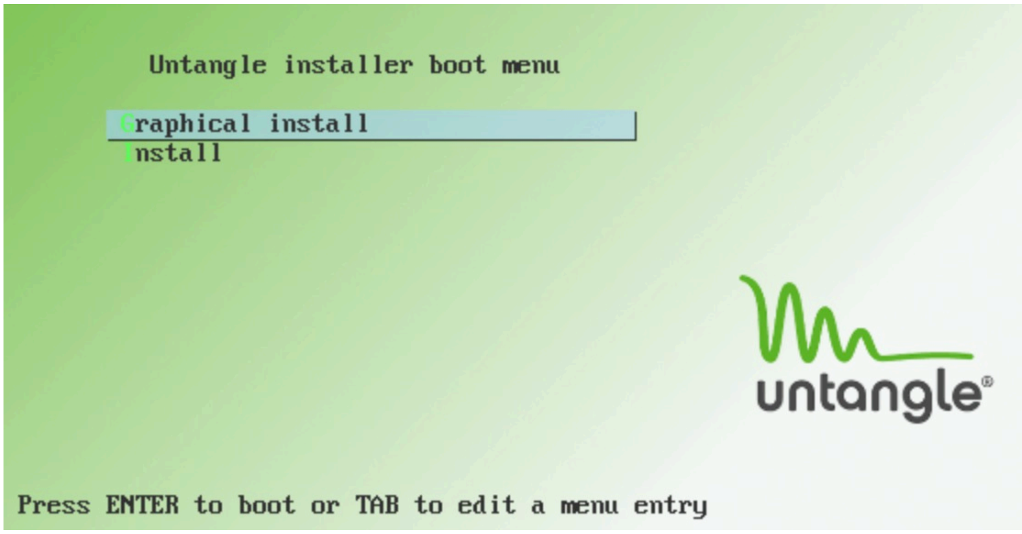
In our "test" installation, we have a live, "external" Internet connection that we will be connecting directly to the firewall (our external interface) and an internal network connection going from our firewall to our internal switch (our internal interface). We will be utilizing non-routable IP space internally (192.168.1.x/24) and we will also be utilizing our firewall to provide DHCP services to our internal network utilizing a range of IPs from 192.168.1.50 – 192.168.1.100.

Our firewall's internal IP address will be 192.168.1.1/24. Our FreeNAS server is already connected to our internal switch and has an IP address of 192.168.1.34 which has been statically assigned with 192.168.1.1 as it's default gateway and DNS server.

Here is our test network configuration:



Once you have downloaded and created your installation media, it is time to start the actual installation. Make sure you have your boot media selected in your BIOS and power on your firewall. You should be greeted with this screen:

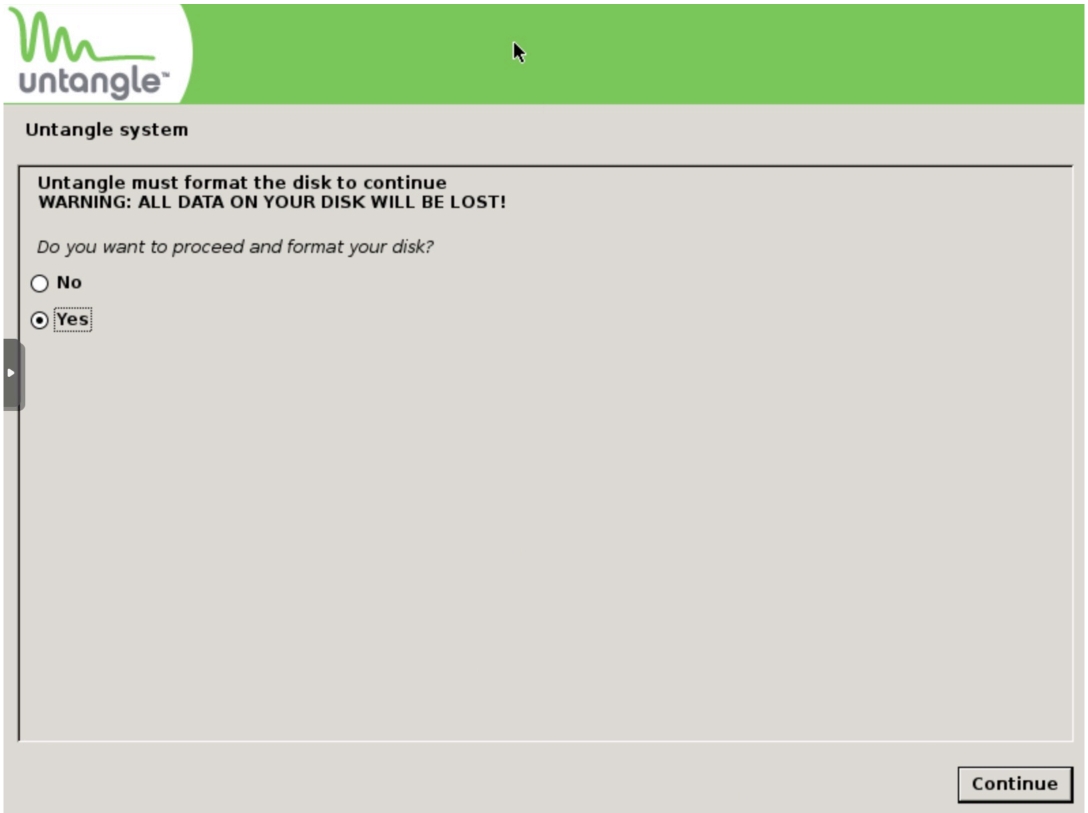


Untangle installer boot menu

Press ENTER to boot or TAB to edit a menu entry

You will then be prompted to select your Language, Location and Keymap. Once you have completed those selections, the installer will begin. It will test your hardware and give you a summary of your memory and processor speed. Click Continue.

You will then be notified that Untangle must format your disk and that you will lose all of your data if you proceed. Select "Yes" and click Continue.



Untangle system

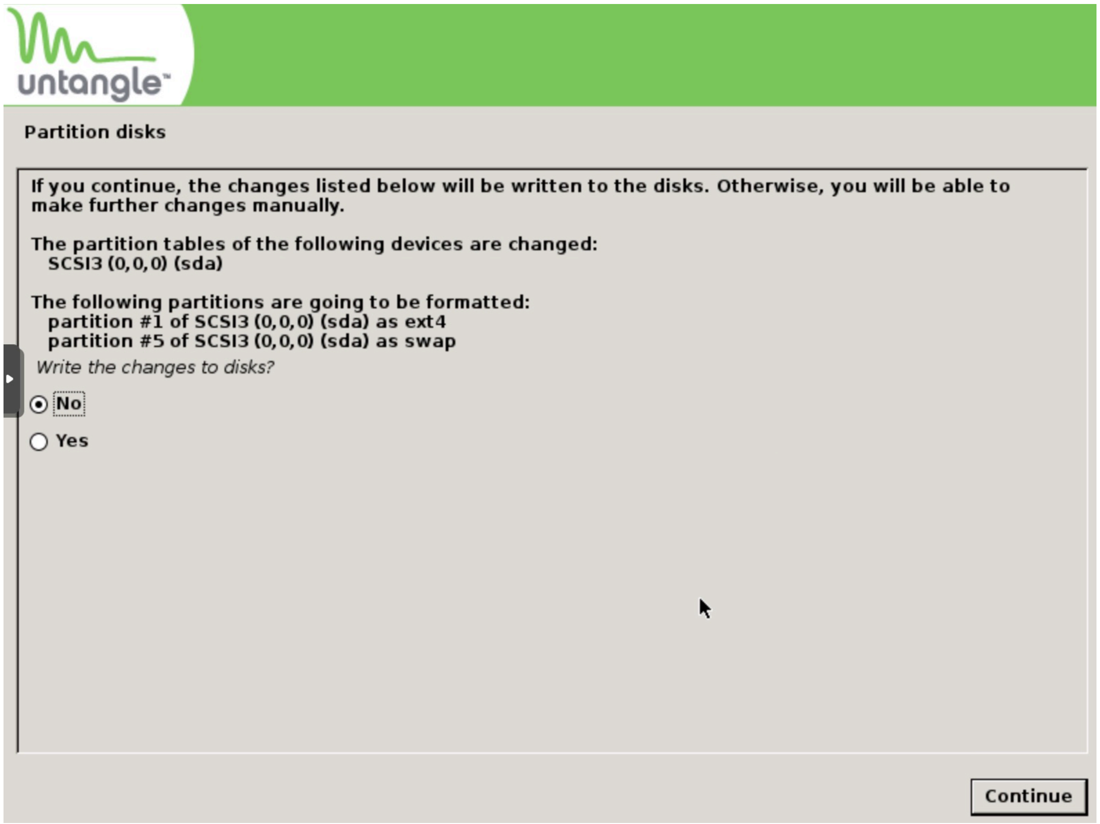
Untangle must format the disk to continue
WARNING: ALL DATA ON YOUR DISK WILL BE LOST!

Do you want to proceed and format your disk?

○ No

● Yes

Next it will tell you the changes that are going to be written to your disk. Select "Yes" and click "Continue":



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
  SCSI3 (0,0,0) (sda)

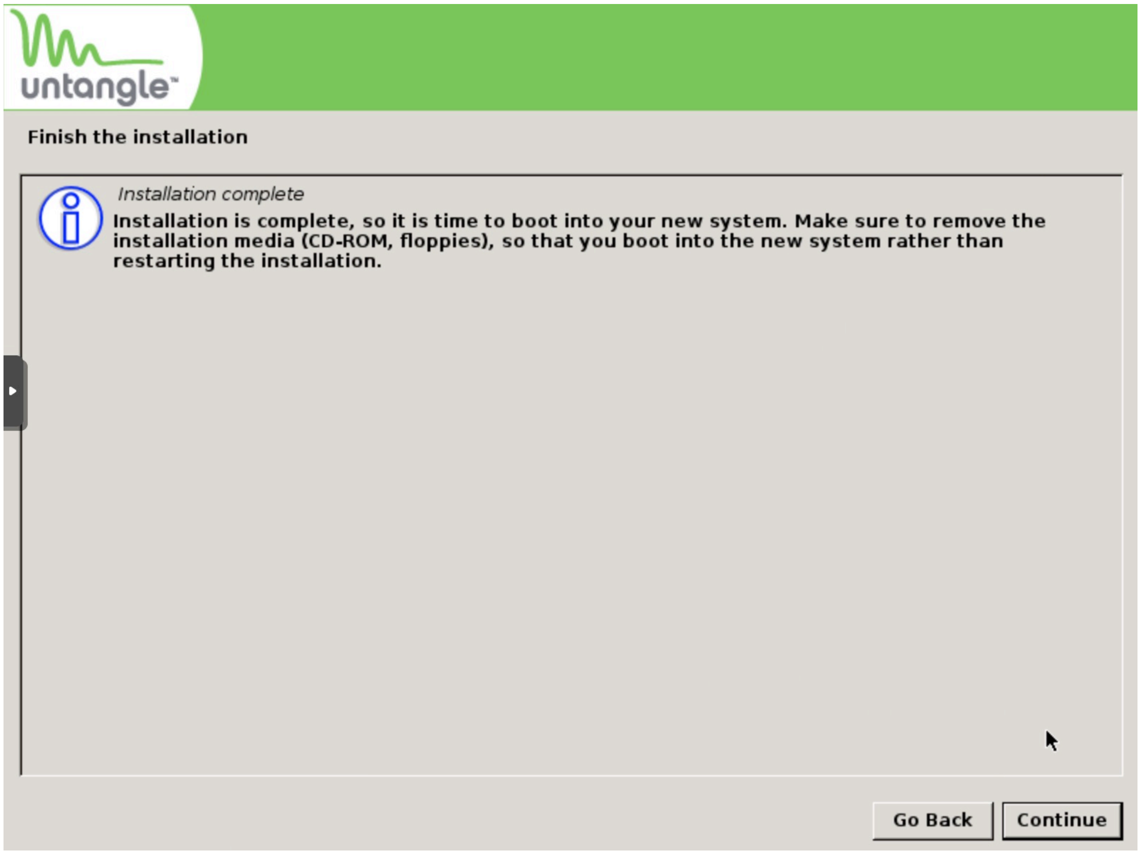
The following partitions are going to be formatted:
  partition #1 of SCSI3 (0,0,0) (sda) as ext4
  partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

● No

○ Yes

Once the basic install has finished, you will be presented with this screen:



Finish the installation

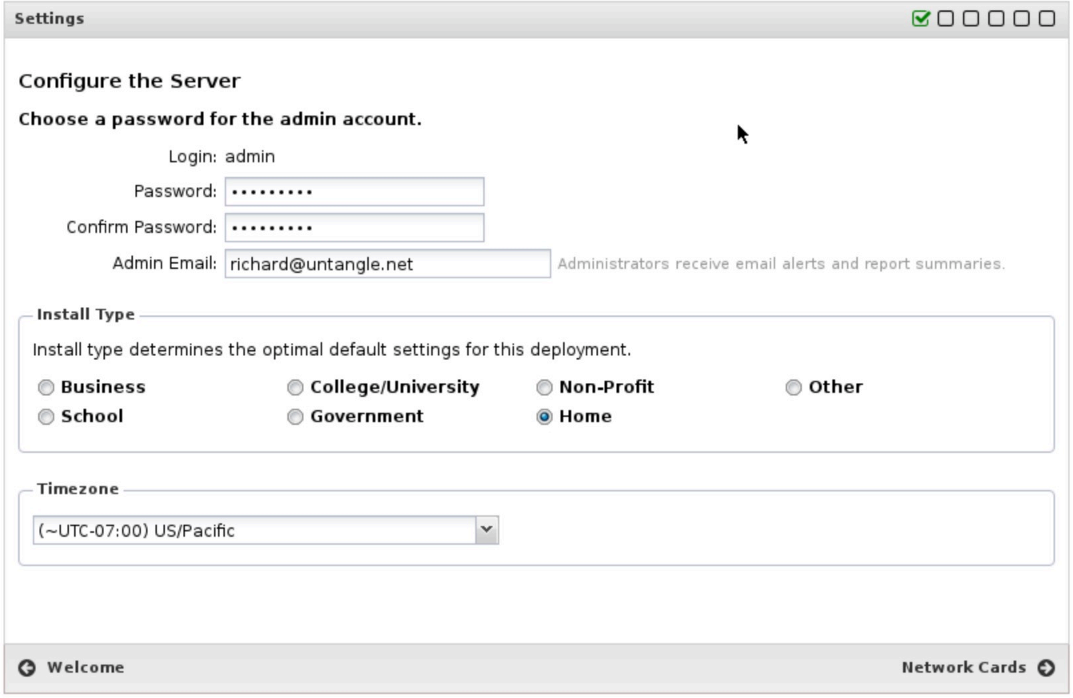
Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

Congratulations – The first part of your firewall install is now complete!

Post Installation Configuration

Once your firewall reboots, it will (again) ask you your language and then you will move on to setting the password, email for admin notifications and your timezone:



Configure the Server

Choose a password for the admin account.

Login: admin

Password: •••••••••

Confirm Password: •••••••••

Admin Email: richard@untangle.net Administrators receive email alerts and report summaries.

Install Type

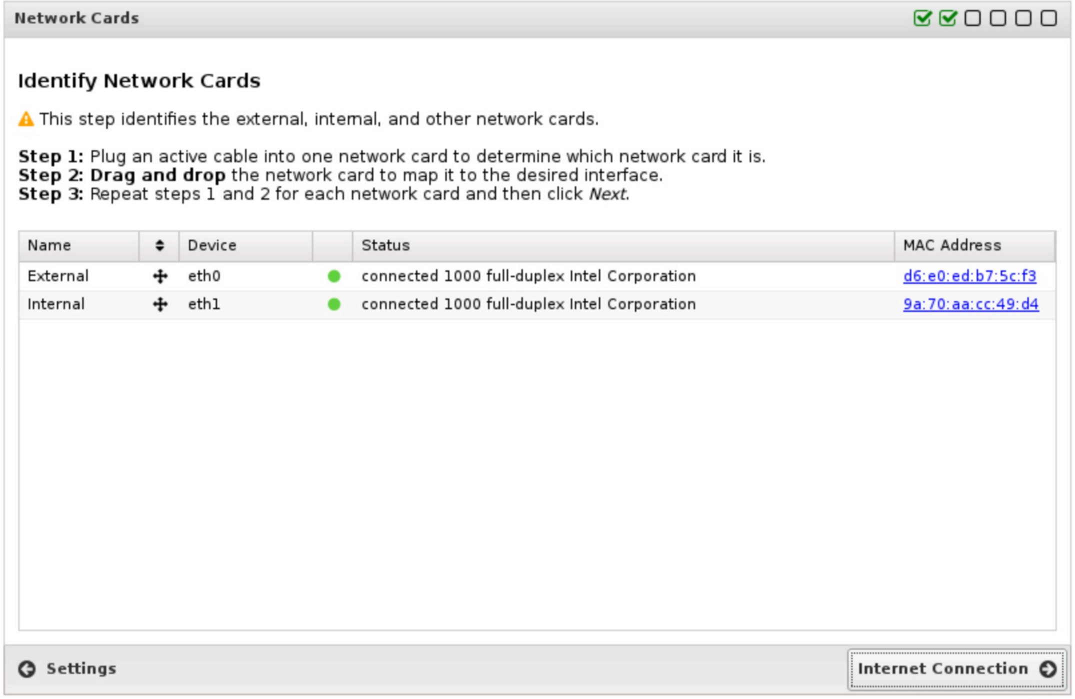
Install type determines the optimal default settings for this deployment.

○ **Business** ○ **College/University** ○ **Non-Profit** ○ **Other**
○ **School** ○ **Government** ● **Home**

Timezone

(~UTC-07:00) US/Pacific

The next step is to identify your network cards and make sure that they are labeled correctly. If they are not, then you can rearrange them by dragging and dropping them in the correct order. To determine which interface is which, plug in an Ethernet cable into each interface to see which one goes active:



Identify Network Cards

This step identifies the external, internal, and other network cards.

Step 1: Plug an active cable into one network card to determine which network card it is.
Step 2: Drag and drop the network card to map it to the desired interface.
Step 3: Repeat steps 1 and 2 for each network card and then click *Next*.

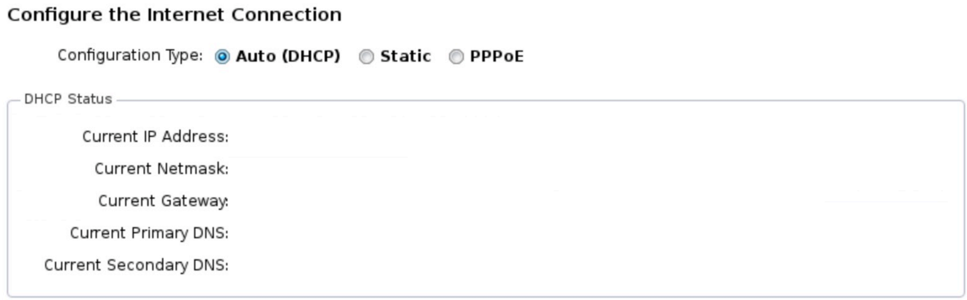
Name		Device		Status	MAC Address
External	✣	eth0	●	connected 1000 full-duplex Intel Corporation	d6:e0:ed:b7:5c:f3
Internal	✣	eth1	●	connected 1000 full-duplex Intel Corporation	9a:70:aa:cc:49:d4

The next step will be to configure your Internet connection. In most cases unless your provider has assigned you a STATIC external IP address, you should select "Auto (DHCP)" for Configuration Type.

NOTE*: If you had another device (Linksys, etc) previously connected to this same internet connection, you may have to reboot your cable modem or DSL router, otherwise you may not have connectivity as some of those devices "learn" the mac address of the connected device and it won't reset until you power cycle your hardware. I recommend power cycling your cable modem or DSL router prior to testing network connectivity on this page.*

If you have a static IP address, click "Static" and fill in the necessary information. The same is true for PPPoE, select it and enter in your credentials. Once you have completed these settings, click "Test Connectivity" and make sure you have Internet access.

DHCP:



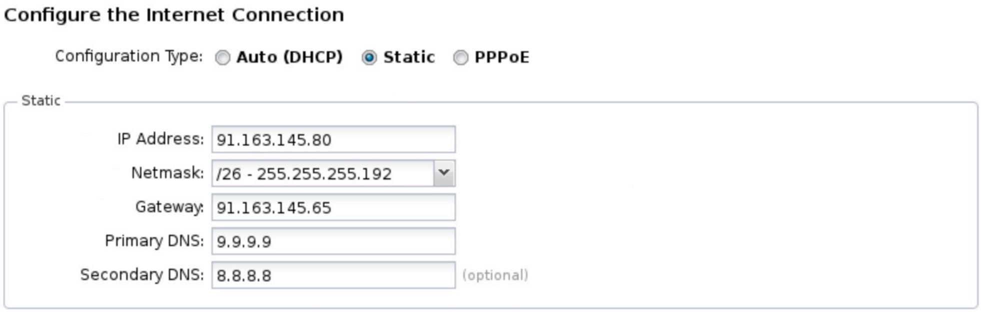
Configure the Internet Connection

Configuration Type: ● Auto (DHCP) ○ Static ○ PPPoE

DHCP Status

Current IP Address:
Current Netmask:
Current Gateway:
Current Primary DNS:
Current Secondary DNS:

STATIC:



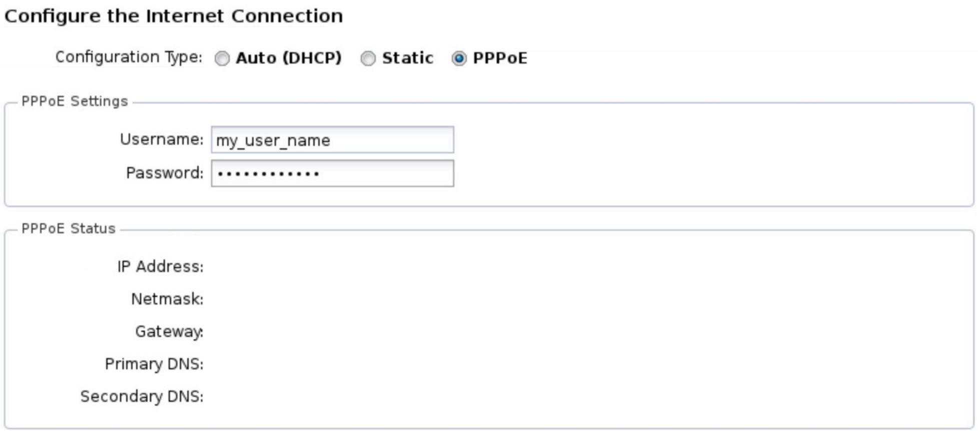
Configure the Internet Connection

Configuration Type: ○ Auto (DHCP) ● Static ○ PPPoE

Static

IP Address: 91.163.145.80
Netmask: /26 - 255.255.255.192
Gateway: 91.163.145.65
Primary DNS: 9.9.9.9
Secondary DNS: 8.8.8.8 (optional)

PPPoE:



Configure the Internet Connection

Configuration Type: ○ Auto (DHCP) ○ Static ● PPPoE

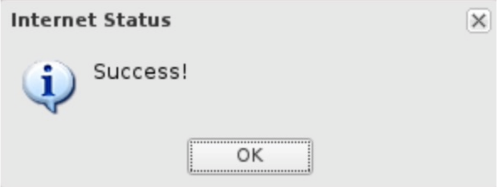
PPPoE Settings

Username: my_user_name
Password: ••••••••••••

PPPoE Status

IP Address:
Netmask:
Gateway:
Primary DNS:
Secondary DNS:

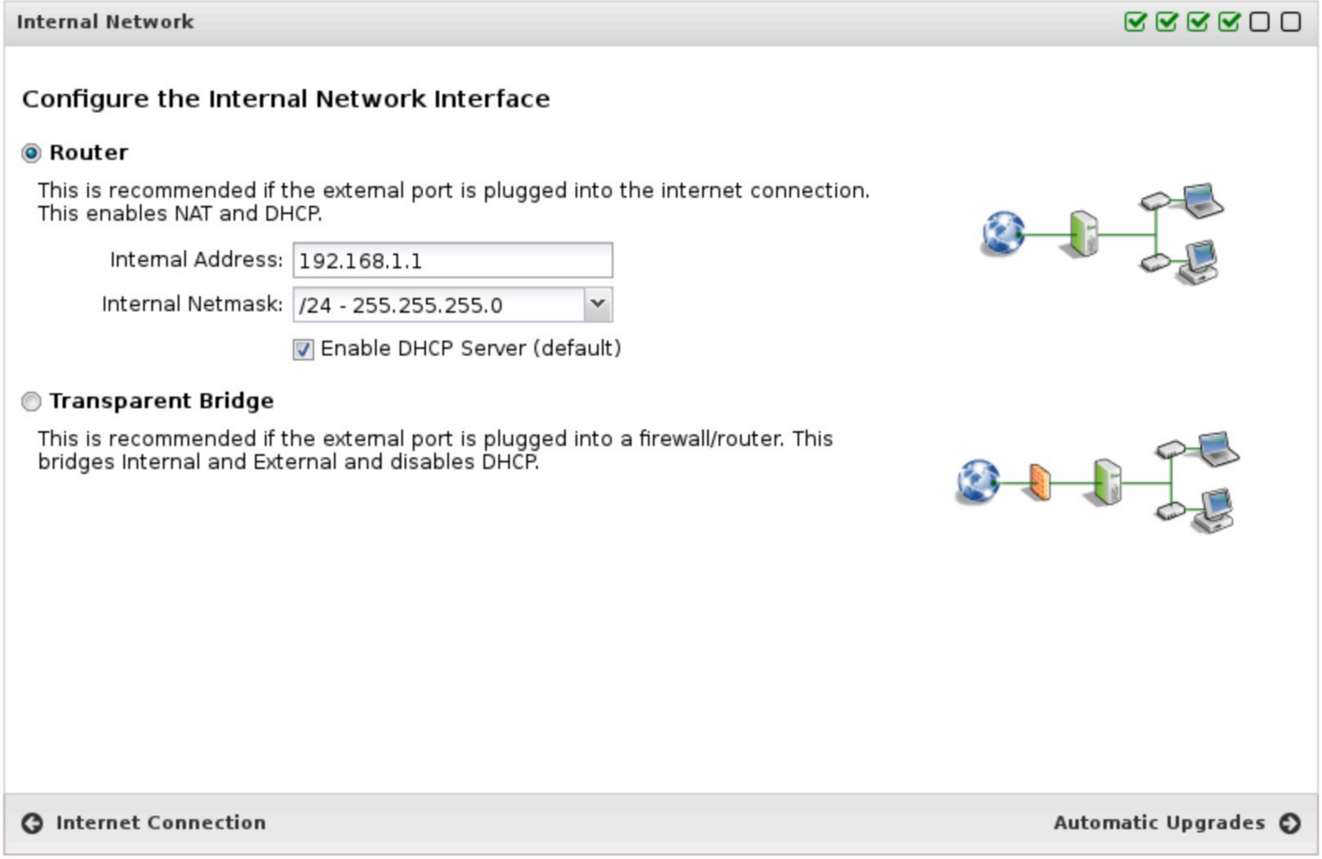
If your connection was successful, you should see this:



Internet Status

Success!

The next step will be to configure your internal network. If you already have an IP configuration that you use internally, set up all that information here. This device will become the DEFAULT GATEWAY on your network and (if you select) your DHCP server on your network. This is where you select those settings:



Internal Network

Configure the Internal Network Interface

● Router

This is recommended if the external port is plugged into the internet connection. This enables NAT and DHCP.

Internal Address: 192.168.1.1

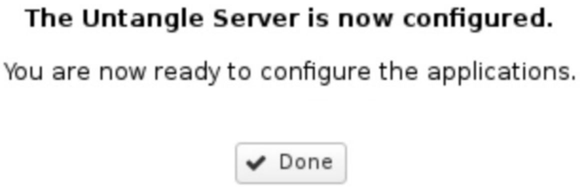
Internal Netmask: /24 - 255.255.255.0

☑ Enable DHCP Server (default)

○ Transparent Bridge

This is recommended if the external port is plugged into a firewall/router. This bridges Internal and External and disables DHCP.

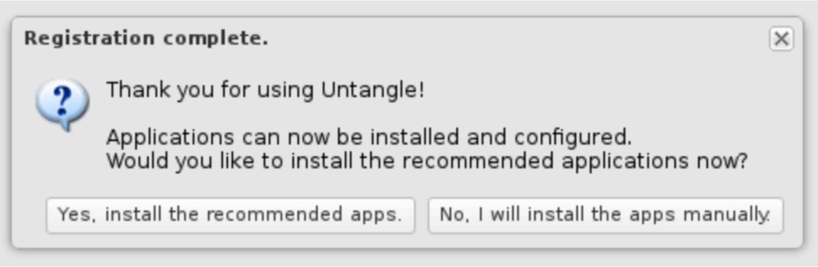
The next screen is where you will setup Automatic Updates and Connection to Untangle Cloud where you can manage and monitor your firewall from the Internet. Select setting appropriate for your particular configuration and click Finished:



The Untangle Server is now configured.

You are now ready to configure the applications.

You will then be asked to register your untangle installation and once you have completed that it will ask you what applications you wish to install. There are two options here – to install the recommended apps (which will install everything) and to install the apps manually, which allow you to select which apps you want to install. If you install the recommended apps, you will get all of the commercial apps as well as the free apps. This is not a bad thing if you want to "play around" with the apps and see what you like. For home users, Untangle provides an all-you-can-eat price of $50.00 per year which is an amazing price, however for this installation, we are going to manually install only the apps that we want.



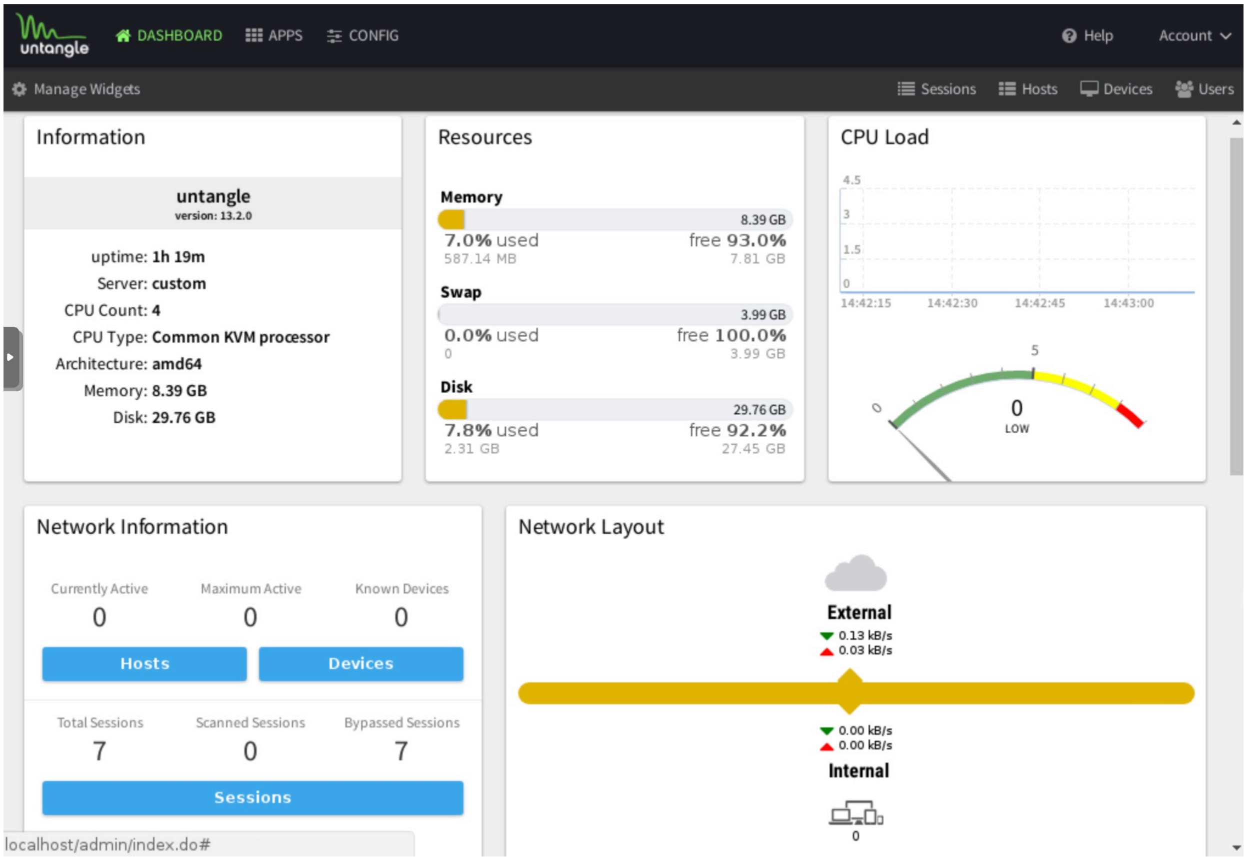
Registration complete.

Thank you for using Untangle!

Applications can now be installed and configured.
Would you like to install the recommended applications now?

Yes, install the recommended apps.
No, I will install the apps manually.

In the next screen you will be presented with a list of available free and paid applications. From here, we are going to install the Firewall and the OpenVPN Service Apps. Once you have selected both of these items, you can go back to the top and select "Dashboard" to go to your firewall dashboard. Here you will see basic information about your firewall, memory, CPU, swap and disk utilization, and more:



Information

untangle
version: 13.2.0

uptime: 1h 19m
Server: custom
CPU Count: 4
CPU Type: Common KVM processor
Architecture: amd64
Memory: 8.39 GB
Disk: 29.76 GB

Resources

Memory
8.39 GB
7.0% used — free 93.0%
587.14 MB — 7.81 GB

Swap
3.99 GB
0.0% used — free 100.0%
0 — 3.99 GB

Disk
29.76 GB
7.8% used — free 92.2%
2.31 GB — 27.45 GB

CPU Load

Network Information

Currently Active 0
Maximum Active 0
Known Devices 0

Total Sessions 7
Scanned Sessions 0
Bypassed Sessions 7

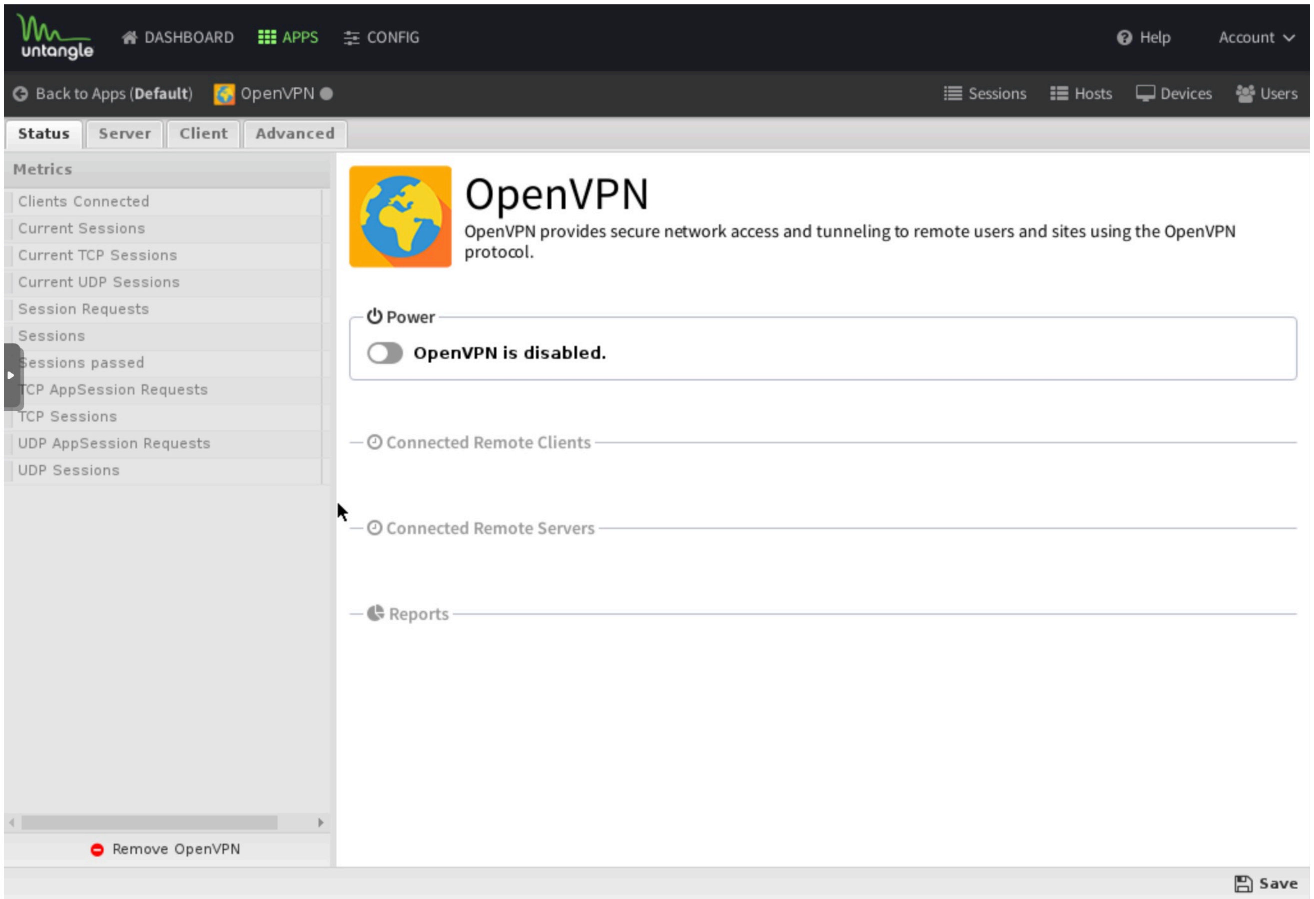
Network Layout

localhost/admin/index.do#

The system is up and running and you should now be able to access it by going to https://192.168.1.1/admin and login with the username and password you selected during the installation. Replace 192.168.1.1 with the IP address you assigned to the firewall's internal interface above if it is different. By default, you CANNOT access or manage your firewall from outside of your local internal network. It is possible to allow this type of access, but doing so is outside the scope of this document.

Configuring OpenVPN

The next step is to configure and activate the OpenVPN server. At the top of the dashboard, select "APPS" and then OpenVPN. You should be presented with this screen:

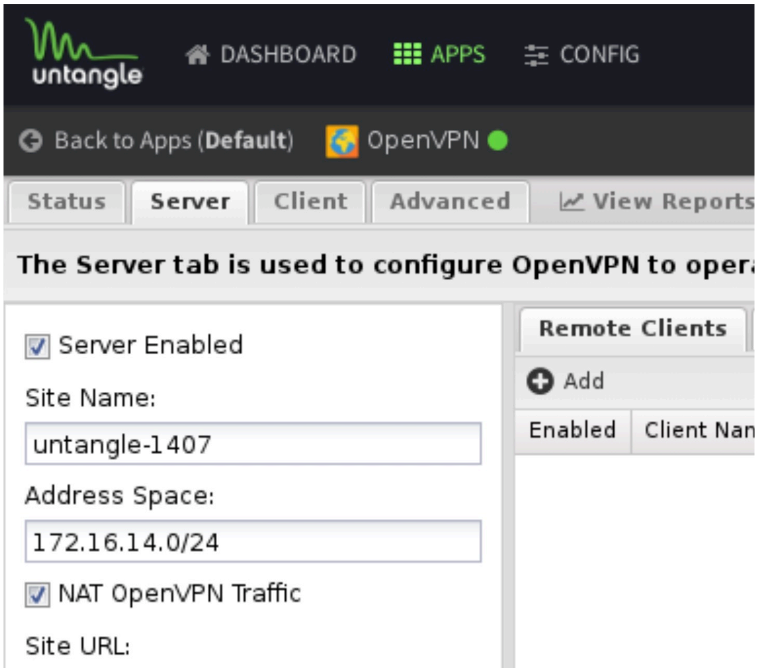


OpenVPN

OpenVPN provides secure network access and tunneling to remote users and sites using the OpenVPN protocol.

OpenVPN is disabled.

"Turn On" the power to the OpenVPN and in a few seconds it will show enabled. Next, click on the "Server" tab at top of the screen and click the checkbox next to the "Server Enabled" setting. Enter a site name and change the address space (if necessary) and leave the NAT OpenVPN Traffic enabled. You can also setup Username/Password Authentication if you like.



The Server tab is used to configure OpenVPN to oper

☑ Server Enabled

Site Name: untangle-1407

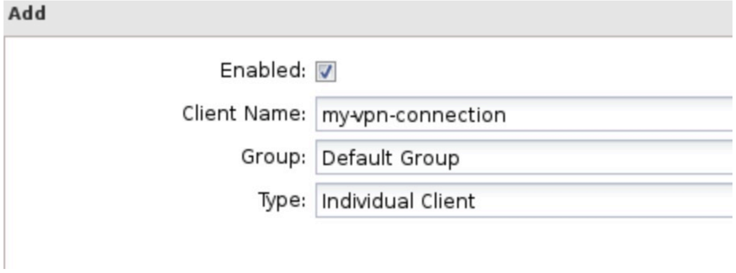
Address Space: 172.16.14.0/24

☑ NAT OpenVPN Traffic

Site URL:

The default configuration for Untangle OpenVPN is to push local DNS so that your system, once connected, get the benefits of any locally added DNS entries and it also defaults to a NON full tunnel setting. This means that only traffic destined for your local network behind the firewall (in this case 192.168.1.1/24) will be routed over the VPN, all other traffic will be sent out your normal internet connection. The other setting is "Full Tunnel" which will route 100% of your traffic over your VPN and out your firewall. To change this configuration, click on the "Groups" tab and change the "Full Tunnel" from "False" to "True" under the "Default Group" setting.

Next, to add a remote client and configure the settings, click on the "Add" icon directly under the "Remote Clients" tab. Give your Client a name and make sure the "Enabled" checkbox is selected and then click "Done" at the bottom.



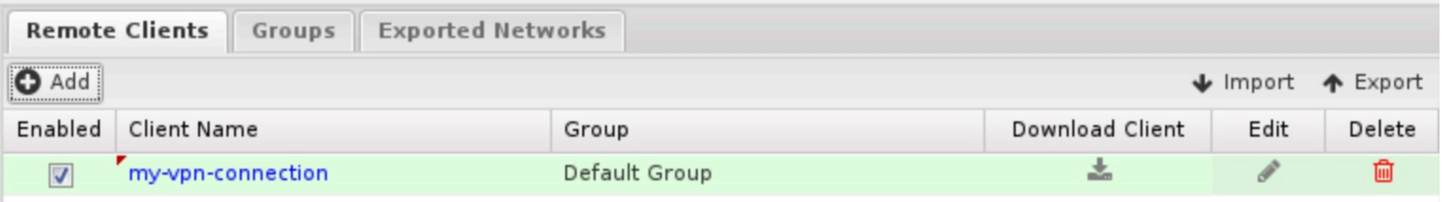
Enabled: ☑

Client Name: my-vpn-connection

Group: Default Group

Type: Individual Client

You should now be at the screen where you can enable or disable the client or delete the client as well as download the client files:



Enabled	Client Name	Group	Download Client	Edit	Delete
☑	my-vpn-connection	Default Group			

Before downloading the client, you must click the "Save" option at the bottom right side of the screen. Select "Download Client" and Untangle will start building the various clients for you to download. Select the download that is correct for your platform.

If you are using windows, it a comes as a .exe that installs the OpenVPN software as well as the config and key files for your VPN connection. This is all done as part of the software setup.

For OSX, Linux, iPads, etc you will want to select the second options (apple/linux/etc). For Apple, you will want to download and install TunnelBlick which is the OpenVPN client for OSX. You can find it here:

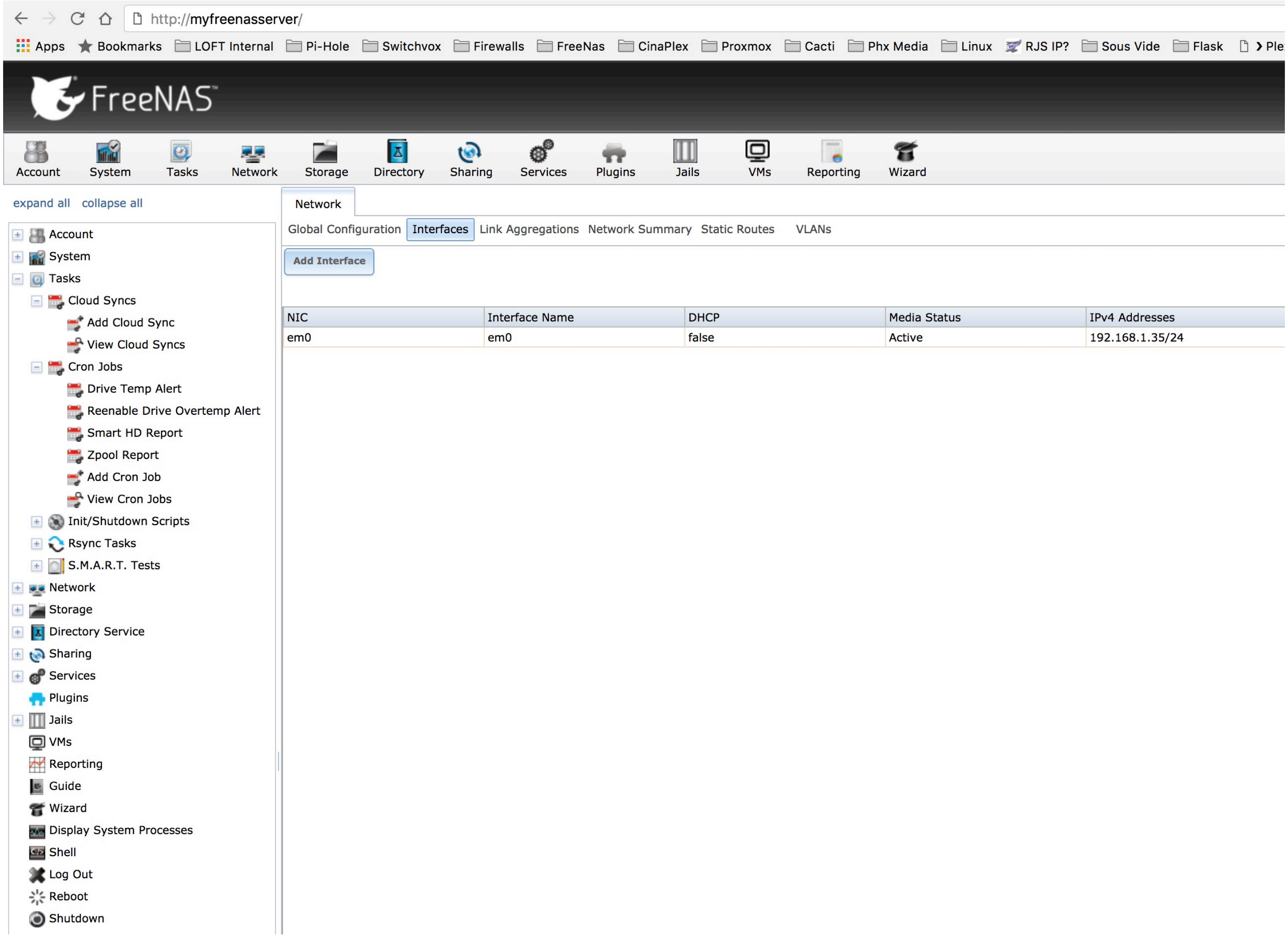
https://tunnelblick.net/

Once you have downloaded and installed the TunnelBlick client, open the client and double click on the "opvn" config file. OSX will ask you if you want to install the VPN for you or everyone. Select the appropriate response for your particular configuration and click finish.

As a side note, you can also install OpenVPN on your iPad and access your internal network from your ipad.

To make life easy, there is one more setting that we can use to make getting to our FreeNAS server easier. At the top of the Untangle screen, select the "Config" option, then "Network" then "DNS Server". Here click the "Add" icon and add a static entry for your FreeNAS server. Click "Save" at the lower right hand corner and now once connected via your VPN, you can use http://myfreenasserver to get to your web interface on your server.

To test your new VPN, you will need to be on a different network than the one where your firewall resides. This could be your local Starbucks, your neighbors wi-fi, a hot-spot from your phone, anything that will give your test machine a separate live internet connection. Once you have that, activate your VPN and open your web browser and point to your FreeNAS server IP:



NIC	Interface Name	DHCP	Media Status	IPv4 Addresses
em0	em0	false	Active	192.168.1.35/24

Congratulations, you now have free, secure, remote access to your internal network from pretty much anywhere in the world!