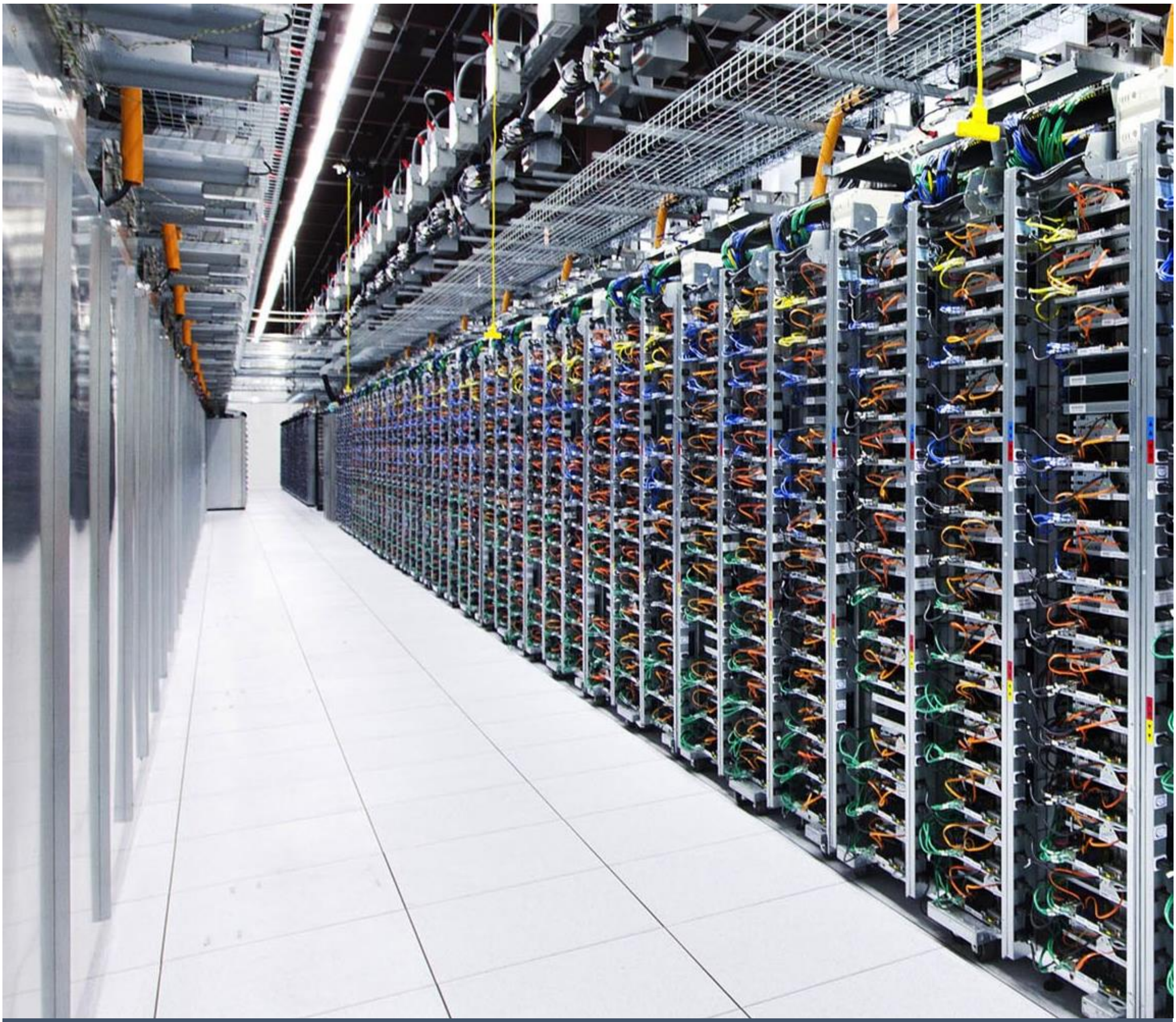


ASDN – Automated Software Defined Networking

User Manual – CA400

FILIP NIKOLIC – 14470852

20/05/2018

Supervisor: Brian Stone

Table of Contents

1. Introduction

1.1. Overview

This document contains a guide helping you adopt and understand the application as quickly as possible. This platform is a network automation system intended to increase efficiency and productivity of network engineers and system administrators, by reducing the time they spend maintaining live computer networks.

1.2. Intended audiences and reading suggestions

The most common users of this application include skilled IT professionals, with an experience in configuring and maintaining enterprise-grade computer networks. If you have no prior knowledge of these topics, the following are some reading materials that will allow you to use the application:

- A sequence of written and video Network Basics tutorials created by Juniper Networks, that will best help the novice user. This resource is located here.
- Networking device configuration guide, which covers the most basic functionality of enterprise-grade networking devices. As there are many different device vendors on the market, I will include the most popular guides by: Juniper Networks, Cisco and Extreme Networks.
- An understanding of how VPNs work and are implemented is not crucial, but will help ensure the best user experience. This is not a complete, but a condensed guide, which covers key points on the topic. A sample configuration guide for Juniper Networks devices can be found here.

2. Getting Started

2.1. Software and Hardware Requirements

This is application has a lightweight client-side web-based user interface, therefore the minimum requirements below average and are listed below:

Windows

- Windows 7, Windows 8, Windows 8.1, Windows 10 or later
- An Intel Pentium 4 processor or later that's SSE2 capable
- *Note:* Servers require Windows Server 2008 R2, Windows Server 2012, or Windows Server 2016.

Mac

- OS X Yosemite 10.10 or later

Linux

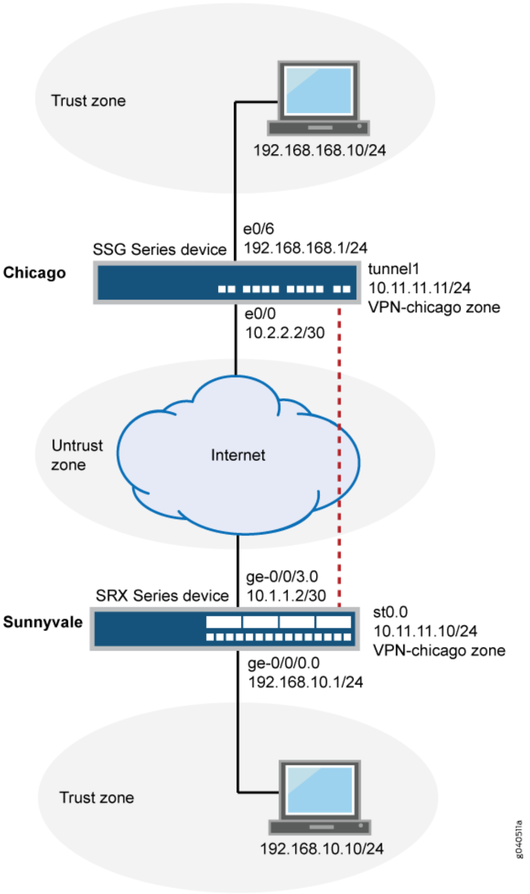
- 64-bit Ubuntu 14.04+, Debian 8+, openSUSE 13.3+, or Fedora Linux 24+
- An Intel Pentium 4 processor or later that's SSE2 capable

2.2. Network Requirements

The network requirements for this platform are extensive, however they are met by the most enterprise-level networks deployed in businesses, educational institutions and government departments. The Following is a complete list of the afore mentioned:

- At present the application can gather statistics from most network devices, however is only able to fully automate and maintain devices produced by **Juniper Networks**. Support for Extreme Networks and Cisco devices is coming soon.

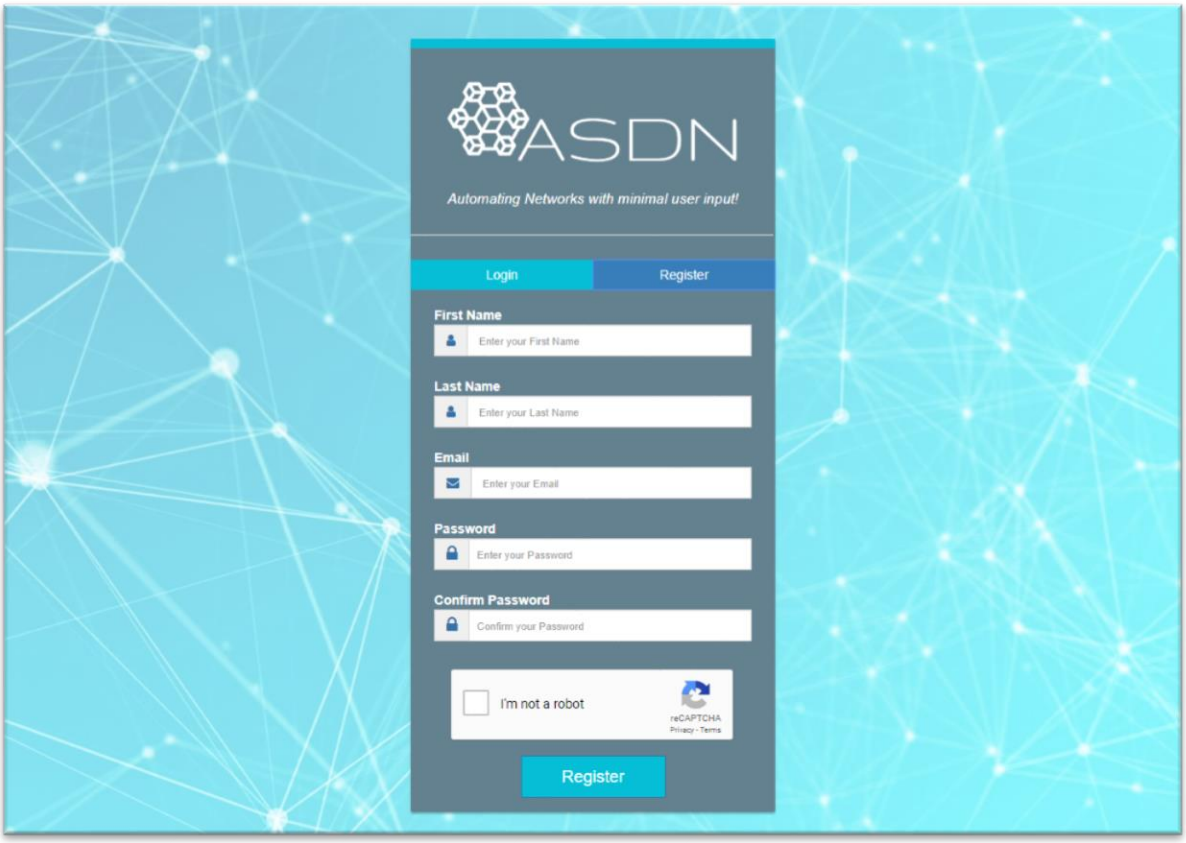
- A **public IPv4 address** that resolves on a **VPN capable device**. In most cases this will be a firewall, however may also be a computer. Whether the address is assigned directly to an interface on the device or NAT (Network Address Translation) is used is irrelevant. Below is a sample network topology that will allow the application to function correctly:



- All devices to be monitored must allow/support **SSHv2**, which is used for log in, network statistics collection and automation functionality.

- All devices must have an **account set up**, provided to the user by ASDN before more advanced functionality can work correctly.

2.3. Sign Up



- After signing up you will receive an email containing the username and encrypted email to be applied to the devices you would like to be managed.

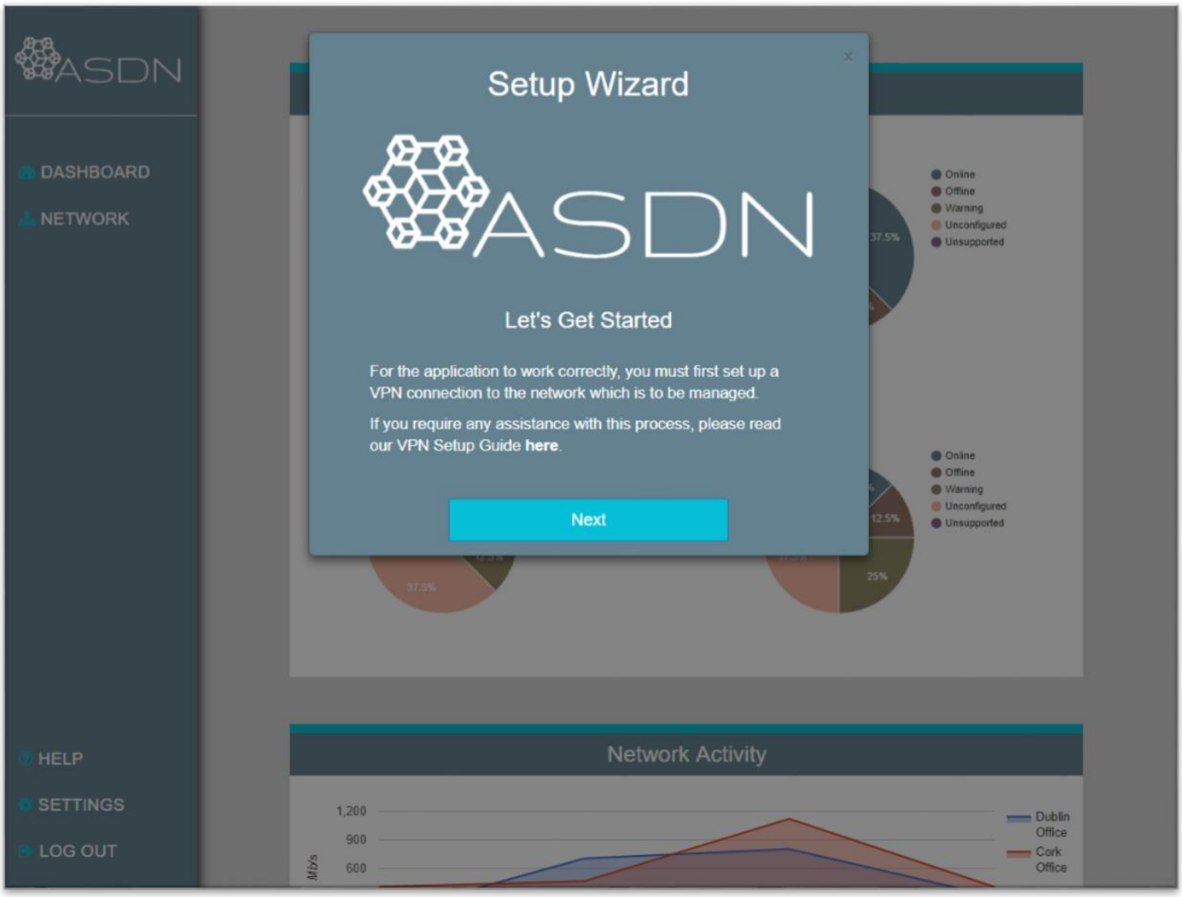
- The format of it will be:
  - user: *username*
  - encrypted-password: *$1$TXIGXY4L$LAPPbUIEXCUAJe85421oL.*

- ***Note***: This is not your website account username or password. It is to be stored securely and not to be used on any other websites as a password.

2.4. VPN Setup Wizard

This section will cover how to correctly configure the ASDN VPN, based on the parameters applied to your local VPN capable device.

2.4.1. Welcome Screen



Setup Wizard

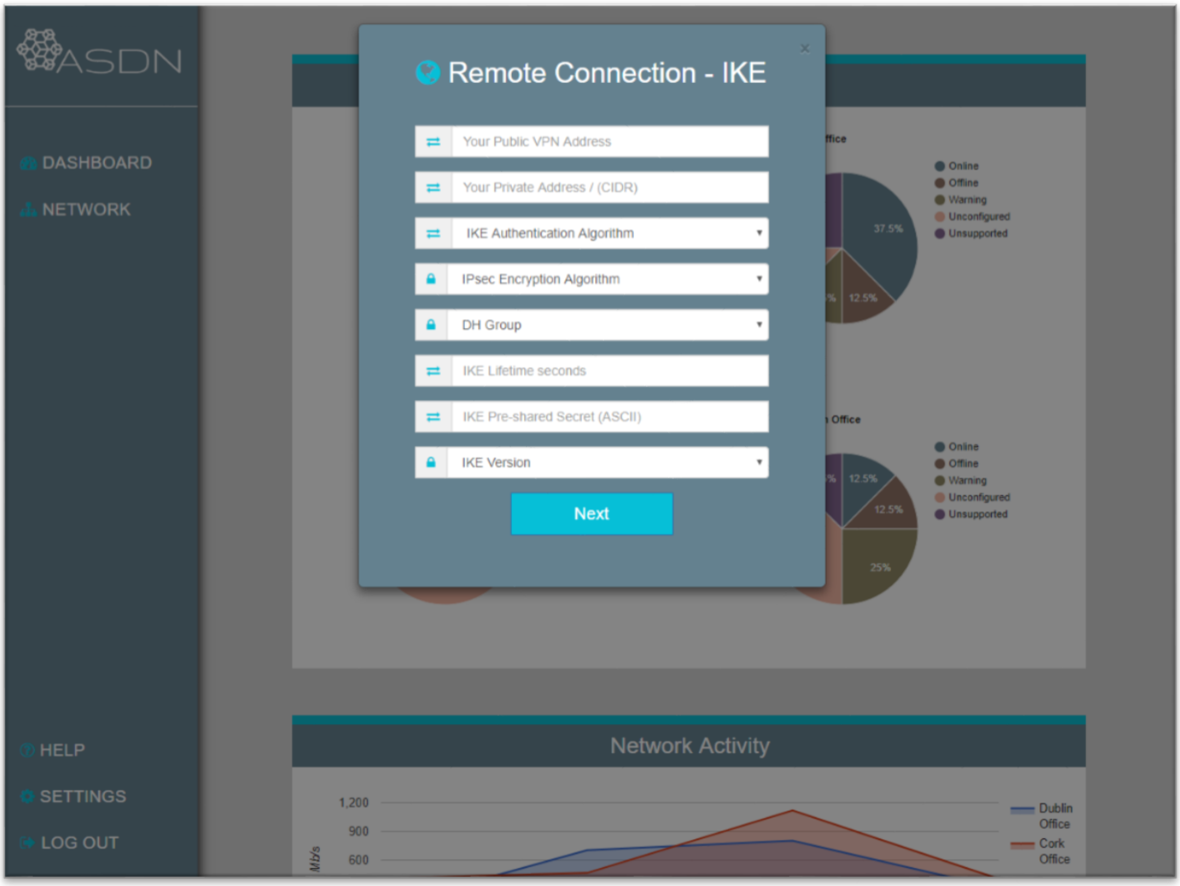
Let's Get Started

For the application to work correctly, you must first set up a VPN connection to the network which is to be managed.

If you require any assistance with this process, please read our VPN Setup Guide **here**.

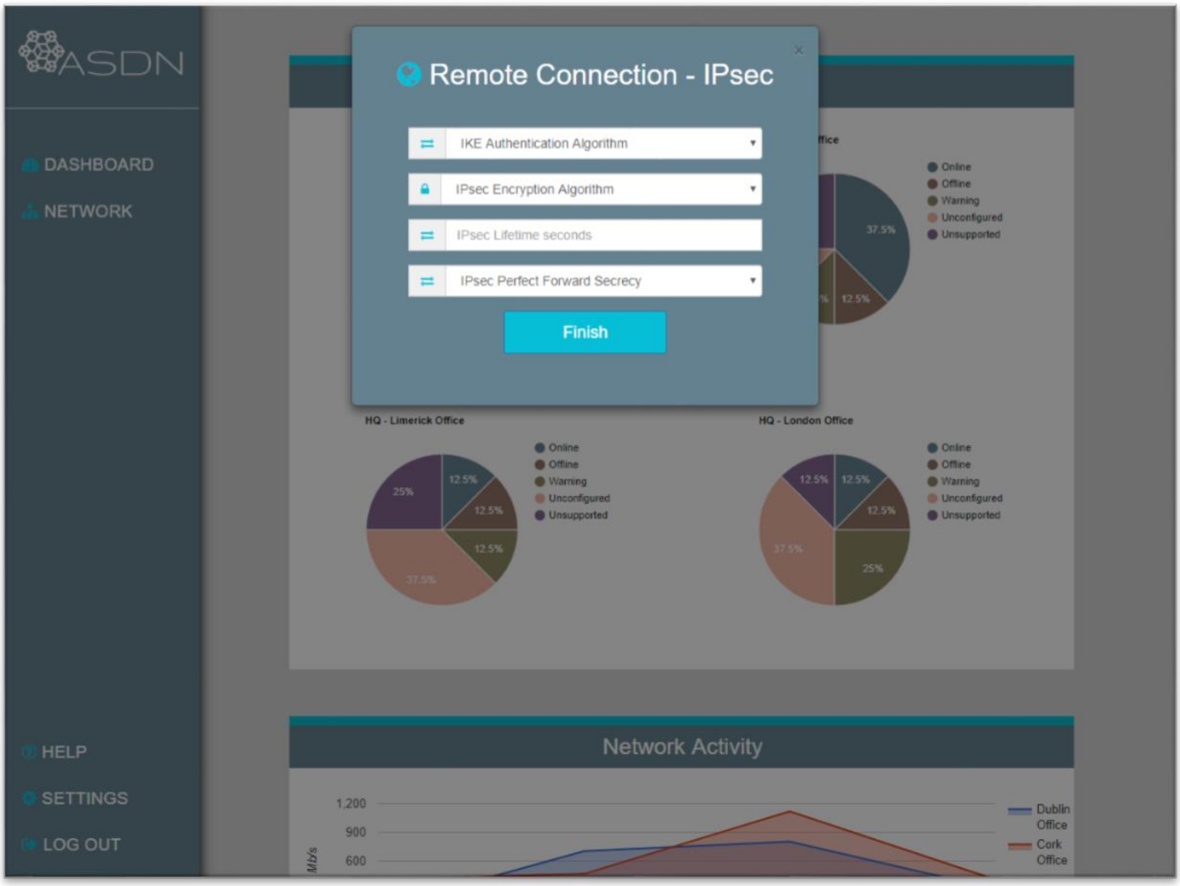
- After setting up a VPN on your public facing device/firewall and applying the account details to all your devices, proceed to the *Setup Wizard*.

2.4.2. IKE Setup



- To complete the first step, you must choose the correct IKE parameters that match the configuration set up on your VPN capable device. The required information is outlined below:
  - **Your Public VPN Address** normally assigned to you by your Internet Service Provider and can be easily determined using websites like this.
  - **Your Private Address / (CIDR)** This is the address assigned to your internal devices and can be determined using commands such as *ifconfig/ifconfig*.
  - **IKE Authentication Algorithm** – to be configured on your firewall, you can choose from the following:
    - MD5; SHA1, SHA-254, SHA-384
  - **IPsec Encryption Algorithm –** to be configured on your firewall, you can choose from the following options:
    - 3DES-cbc, AES-128-cbc, AES-192-cbc, AES-256-cbc, DES-cbc
  - **DH Group –** to be configured on your firewall, groups 1, 2, 5, 19, 20, 24 are supported.
  - **IKE Lifetime seconds –** this parameter should be set to a recommended value of 28570.
  - **IKE Pre-shared Secret (ASCII) –** this represents the passwords for establishing the VPN connection. Please ensure that the password you apply on your firewall is the same as the one in this field.
  - **IKE Version –** choose between version 1 and 2, however consider using v2 as it is much more secure.

2.4.3. IPSec Setup



Remote Connection - IPsec

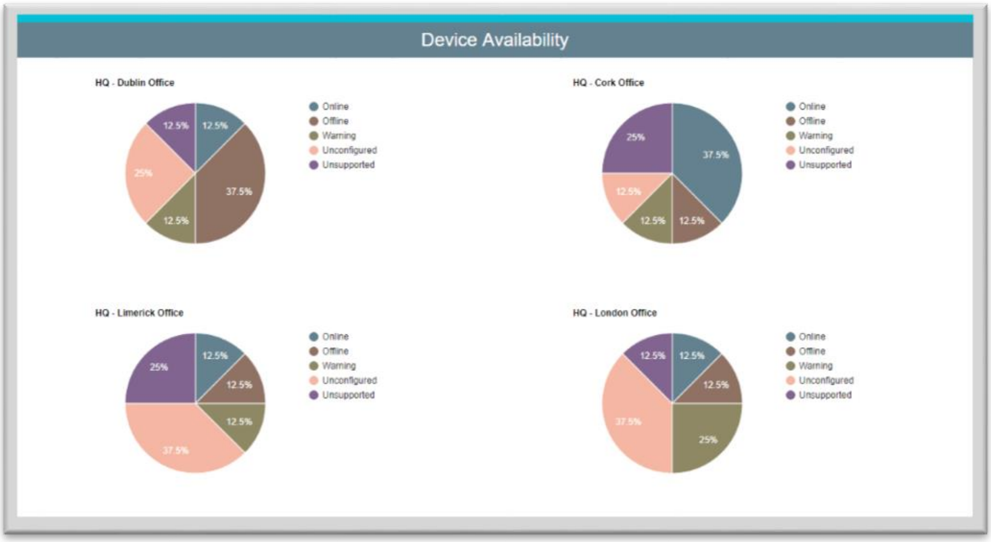
- This is the second phase of establishing a VPN connection, you must choose the correct IPSec parameters that match your configuration. The following parameters must all match precisely:
  - **Authentication Algorithm,** the system supports these options:
    - hmac-sha1-96, hmac-sha-256-128, hmac-sha-256-96, hmac-md5-96
  - **IPsec Encryption Algorithm**, the following are supported:
    - 3-DES-cbc, AES-128-cbc, AES-192-cbc, AES-256-cbc,
    - DES-cbc, AES-128-gcm, AES-192-gcm, AES-256-gcm
  - **IPsec Lifetime seconds** – the recommended value for this parameter is 3363.
  - **IPsec Perfect Forward Secrecy –** a list of groups to select, with these supported:
    - Groups 1, 2, 5, 14, 19, 20, 24

3. Continuous Use

This section will cover showcase the features you can use to monitor your network and device performance and availability.

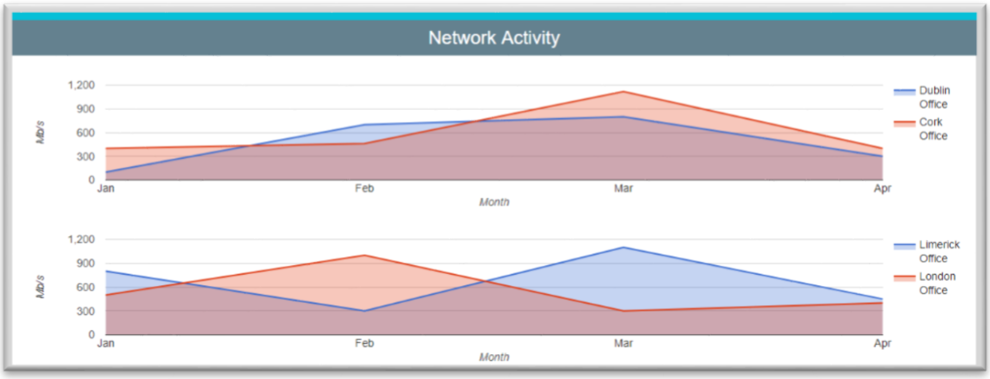
3.1. Network Monitoring

3.1.1. Device Availability



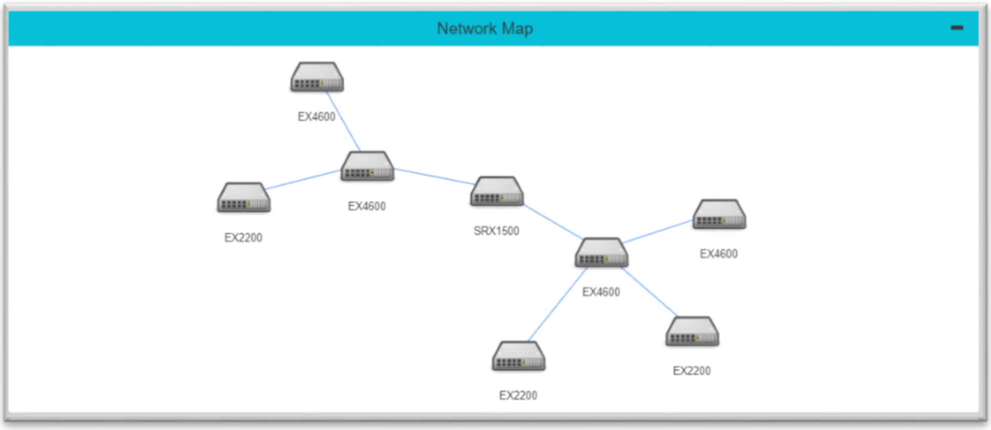
- Once the VPN connection to your desired networks is online, it will take the system a couple of minutes to gather network information. The above example shows four user networks and the state of devices on them. Each device can be in one of the following states:
  - Online – device supported by the platform and fully operational;
  - Offline – a previously operational device that went down;
  - Warning – a supported device that may have a potential issue.
  - Unconfigured – this device is supported but is not configured by the user to allow ASDN to monitor it (most likely the provided account has not been applied)
  - Unsupported – devices manufactured by unsupported vendors fall in this category.

3.1.2. Network Activity



- The above tool allows you to monitor traffic flow on the network over time and in this example, does so for four separate user networks.

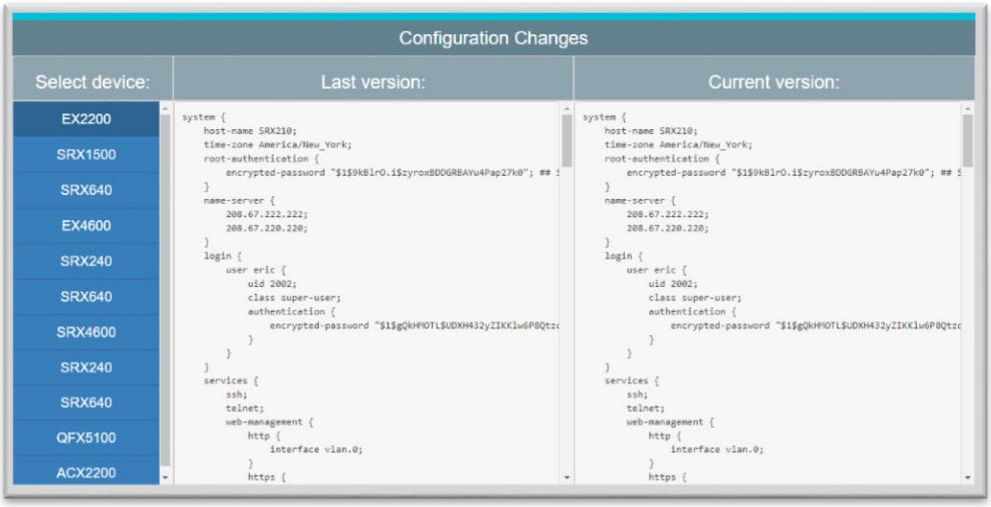
3.1.3. Network Map



- This networks map shows all devices on the network (not clients) and is useful as an additional aid for troubleshooting and monitoring.

3.2. Device Monitoring

3.2.1. Configuration Changes



Last version:

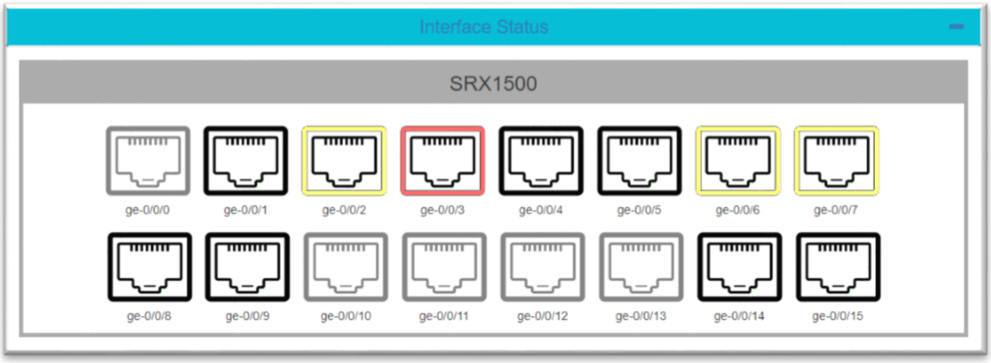
```
system {
    host-name SRX210;
    time-zone America/New_York;
    root-authentication {
        encrypted-password "$1$9kBlrO.i$zyroxBDDGRBAYu4Pap27k0"; ## S
    }
    name-server {
        208.67.222.222;
        208.67.220.220;
    }
    login {
        user eric {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$gQkHMOTL$UDXH432yZIKKlw6P8Qtz
            }
        }
    }
    services {
        ssh;
        telnet;
        web-management {
            http {
                interface vlan.0;
            }
            https {
```

Current version:

```
system {
    host-name SRX210;
    time-zone America/New_York;
    root-authentication {
        encrypted-password "$1$9kBlrO.i$zyroxBDDGRBAYu4Pap27k0"; ## S
    }
    name-server {
        208.67.222.222;
        208.67.220.220;
    }
    login {
        user eric {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$gQkHMOTL$UDXH432yZIKKlw6P8Qtz
            }
        }
    }
    services {
        ssh;
        telnet;
        web-management {
            http {
                interface vlan.0;
            }
            https {
```

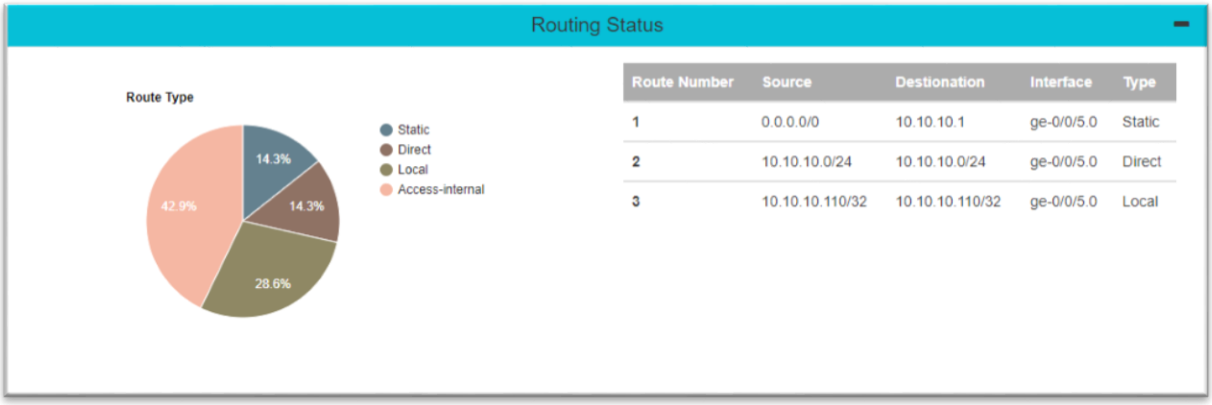
- The current and previous device configurations can be viewed in the tool above.
- Additionally, you will be able to see which changes were made by the automated system and when.

3.2.2. Interface Status



- By clicking on one of the devices listed in the network map, you will be able to see its physical ports. When you hover your cursor above each interface it will indicate the its status. The colour codes are:
    - Black – port used and working correctly
    - Grey – inactive port, noting plugged in
    - Yellow – port in use, but may have issues such as duplex mismatch.
    - Red – indicates a used port that is non-operational.

3.2.3. Routing Status

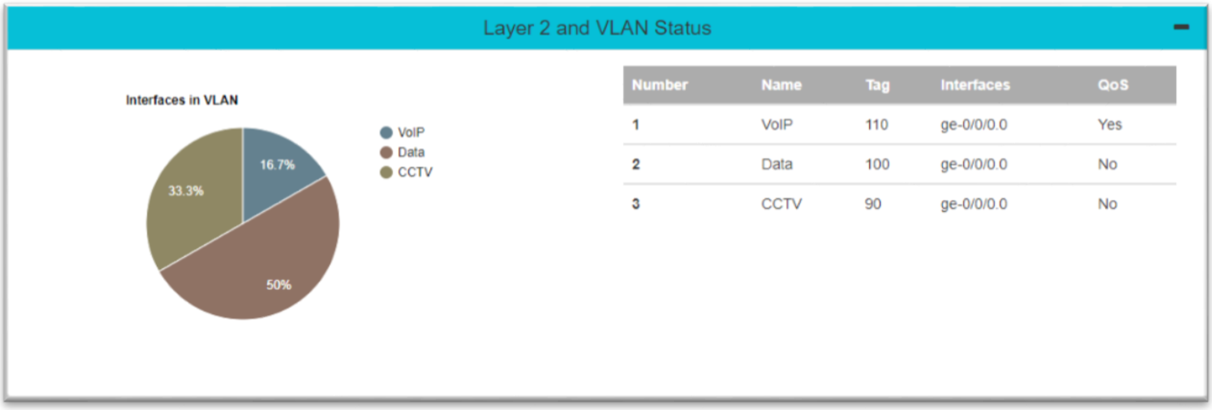


Routing Status

Route Number	Source	Destionation	Interface	Type
1	0.0.0.0/0	10.10.10.1	ge-0/0/5.0	Static
2	10.10.10.0/24	10.10.10.0/24	ge-0/0/5.0	Direct
3	10.10.10.110/32	10.10.10.110/32	ge-0/0/5.0	Local

- This interface displays the device’s rooting table, further helping you accurately monitor the network.
- The chart on the left breaks down the types of routes on the device.

3.2.4. Layer 2 and VLAN Status

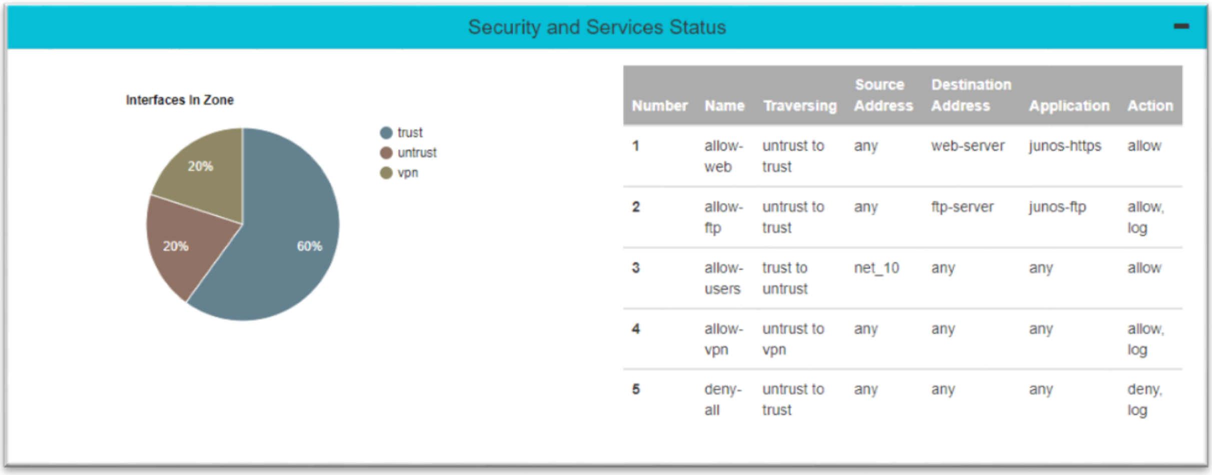


Layer 2 and VLAN Status

Number	Name	Tag	Interfaces	QoS
1	VoIP	110	ge-0/0/0.0	Yes
2	Data	100	ge-0/0/0.0	No
3	CCTV	90	ge-0/0/0.0	No

- If applicable to the selected device, the above will display VLAN information
- The pie chart gives a breakdown of the different VLANs configured on that device.

3.2.5. Security and Services Status



Security and Services Status

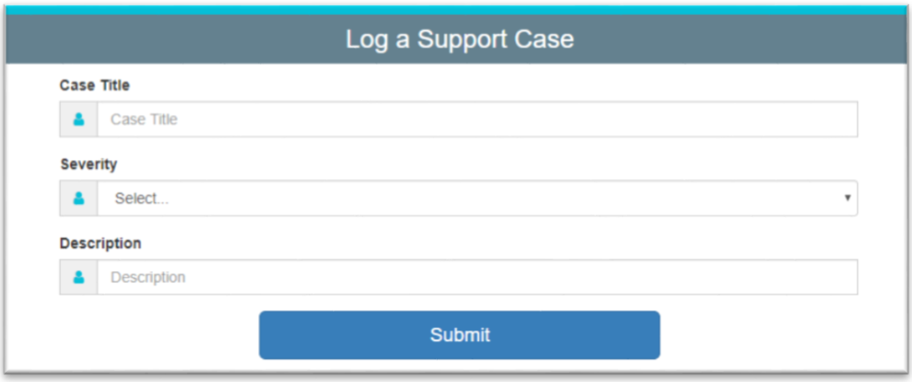
Number	Name	Traversing	Source Address	Destination Address	Application	Action
1	allow-web	untrust to trust	any	web-server	junos-https	allow
2	allow-ftp	untrust to trust	any	ftp-server	junos-ftp	allow, log
3	allow-users	trust to untrust	net_10	any	any	allow
4	allow-vpn	untrust to vpn	any	any	any	allow, log
5	deny-all	untrust to trust	any	any	any	deny, log

- For security devices such as firewalls, the above shows rules configured on that device.

4. Help and Support

If you have any issues consult the help pages of the website.

- If you cannot find relevant information that will help you solve the problem, can log a technical support ticket via the help menu, using the following form:



Log a Support Case

Case Title

Case Title

Severity

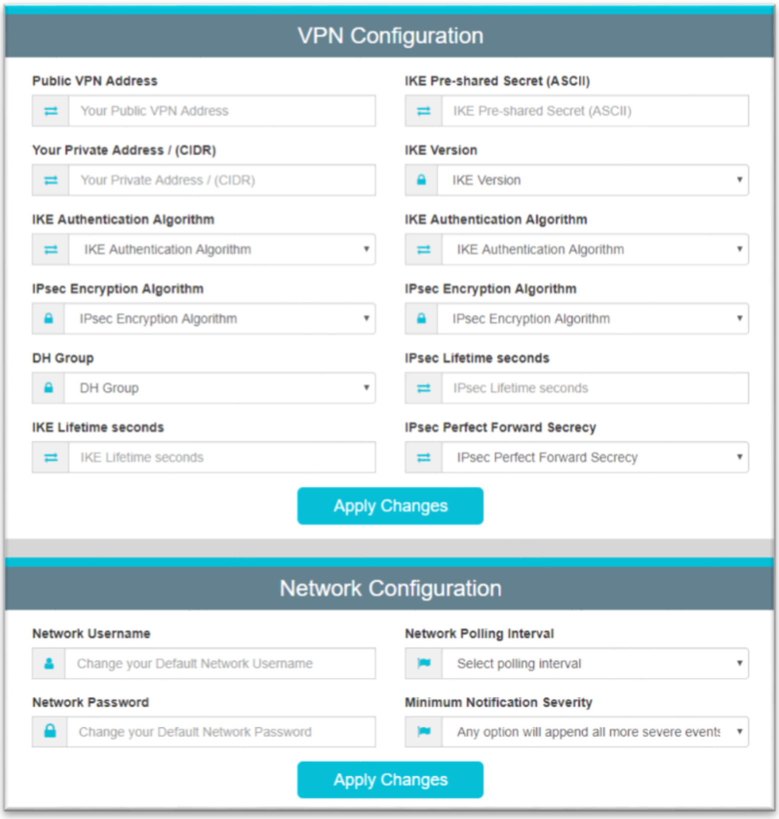
Select...

Description

Description

Submit

- Any information you entered during the setup phase of the ASDN platform on your network can be edited using the settings page:



VPN Configuration

Public VPN Address

Your Public VPN Address

IKE Pre-shared Secret (ASCII)

IKE Pre-shared Secret (ASCII)

Your Private Address / (CIDR)

Your Private Address / (CIDR)

IKE Version

IKE Version

IKE Authentication Algorithm

IKE Authentication Algorithm

IKE Authentication Algorithm

IKE Authentication Algorithm

IPsec Encryption Algorithm

IPsec Encryption Algorithm

IPsec Encryption Algorithm

IPsec Encryption Algorithm

DH Group

DH Group

IPsec Lifetime seconds

IPsec Lifetime seconds

IKE Lifetime seconds

IKE Lifetime seconds

IPsec Perfect Forward Secrecy

IPsec Perfect Forward Secrecy

Apply Changes

Network Configuration

Network Username

Change your Default Network Username

Network Polling Interval

Select polling interval

Network Password

Change your Default Network Password

Minimum Notification Severity

Any option will append all more severe events

Apply Changes