



Feasibility Evaluation of SoftEther VPN

James Hemmings

Computer Networking 2 – White Paper 2

University of Abertay Dundee

BSc (Hons) Ethical Hacking

2016

Note that Information contained in this document is for educational purposes.

1 Abstract

Virtual Private Networks (VPNs) are used extensively around the world for a variety of applications such as connecting organization networks across multiple sites, secure management access, encrypted data transit as well as privacy uses such as preventing censorship and website blacklisting.

Currently on the market there is a number of VPN solutions from companies such as Cisco, Juniper, Microsoft, Open VPN, as well as a number of open source free solutions which can match the specifications and requirements of businesses without the license fees and hardware costs, which allows for the businesses to spend money on other services and reduces the total cost of operations (TCO).

Open source solutions have an increased number of benefits in addition to pricing such as allowing in-house development teams or outside organizations to audit or further develop the VPN solution to encompass more features and functionality or to test the integrity of the code for potential backdoors, malicious code or vulnerabilities within the software itself and this provides a huge benefit to organizations.

This whitepaper will provide the comparisons between an open source solution and the rival commercial market competitor and the benefits such as usability, security and management options that SoftEther VPN provides and how this would improve a business network by providing a competitive and feasible solution.

2 Table of Contents

1	Abstract.....	2
2	Table of Contents.....	3
3	Introduction.....	4
3.1	SoftEther VPN Overview.....	5
3.2	SoftEther VPN Requirements & Limitations.....	6
3.2.1	Supported Operating Systems.....	6
3.2.2	Hardware Requirements.....	6
3.2.3	Software Limitations.....	6
4	Procedure & Results	7
4.1	SoftEther VPN Management & Reporting Functions.....	7
4.1.1	Usability.....	9
4.1.2	Security	10
4.2	Microsoft Remote Access Management & Reporting Functions.....	11
4.2.1	Usability.....	13
4.2.2	Security	13
5	Discussion.....	14
5.1	SoftEther vs Microsoft Remote Access (RRAS)	14
5.2	Future Work.....	16
6	Conclusion	16
7	References.....	17
8	Appendices.....	18
8.1	Appendix A - Installing & Configuring SoftEther VPN Server	18
8.2	Appendix B – Installing & Configuring SoftEther VPN Client	28
8.3	Appendix C - Configuring Microsoft L2TP VPN Client.....	35
8.4	Appendix D – Installing & Configuring Microsoft VPN Server	38
8.5	Appendix E – GNS3 Configuration.....	47

3 Introduction

Virtual Private Networks (VPNs) are a network technology which establishes a secure connection over public, or private networks which enables individuals, governments and business the ability to securely connect to the corporate/business network via public internet connections or from the home environment. With the ever-increasing amount of home workers and telecommuters, VPNs are becoming more of a useful tool to organizations ensuring security and privacy for business operations.

Network management solutions to date such as Virtual Private Networks can require numerous license and software fees depending on the number of users and systems connecting to the VPN solution, with some proprietary systems requiring expensive hardware equipment and further license fees and yearly software upgrade/maintenance fees. However, over the past few years a number of open source software solutions have entered the market which provide the same and if not better software features for Virtual Private Networking.

It is noted however, that previous open source software has started to become more commercialised and cost prohibitive such as Open VPN [1], which has moved more towards the enterprise and commercial level rather than completely open source. Other solutions such as Microsoft Remote Access [2] VPN require a number of remote access client licenses which can add up very quickly within small-enterprise organizations.

SoftEther VPN was selected for this project due to the open source nature of the software and the broad feature set, flexibility and easy configuration options within the server along with support for a multitude of operating systems. In addition to this, Microsoft Remote Access was selected as the market leader to compare the software with due to the extensive usage by small-enterprise organisations.

With the advent of Software-Defined-Networking (SDN) [3], small to medium size businesses now have access to VPN services without the capital expenditure and technological expertise required by on premise VPN solutions which enables organizations to utilise software based VPN solutions without the requirement to implement expensive hardware VPN solutions and the maintenance, utility bills and other fees which surround hardware based systems.

The aim of this whitepaper is to investigate the feasibility of implementing an SDN VPN using SoftEther within the business and then provide a comparison between the current market leader and SoftEther VPN.

The following objectives were identified for this whitepaper:

- Provide, and discuss a comparison between SoftEther VPN and the current market leader.
- Analyse and discuss the feasibility of SoftEther VPN within the business.
- Install and configure SoftEther VPN and provide an installation guide.
- Investigate further features and software for the business.

3.1 SoftEther VPN Overview

SoftEther VPN is multi-protocol open source VPN solution developed by the University of Tsukuba, Japan. The software supports a variety of operating systems such as Windows, Linux, Mac, FreeBSD and Solaris and was designed with flexibility and ease of use in mind and is an alternative to popular main stream VPN solutions such as Open VPN, Microsoft VPN, and Cisco VPN [4] solutions.

The VPN software has a main advantage of being able to avoid and bypass Firewall and deep packet inspection systems using Ethernet over HTTPS to hide VPN data traffic, as well as the ability to tunnel the VPN traffic over UDP DNS and ICMP [5].

SoftEther VPN is also compatible with a variety of VPN technologies and systems such as Open VPN, L2TP, IPSec, Cisco VPN, MS-SSTP, SSL VPN and EtherIP. The VPN software is also the only open source solution to implement a variety of common VPN solutions into one product, for ease of use and interoperability.

The VPN software has been performance tested and offers better network throughputs compared to market leaders such as Microsoft, Open VPN and Cisco, which has shown SoftEther has the capability to utilise up to 1Gbps network throughput performance, as demonstrated in figure two.

SoftEther VPN is very easy to use with an extensive GUI server management tool, and an array of configurable options for every aspect of the software, along with CLI configuration options for power users and server administrators which enables a variety of users, with varying technical experience to easily use the software. The VPN software also comes with full documentation on the SoftEther website to explain and demonstrate the variety of installation and configuration options and troubleshooting steps.

The software also has a variety of configurable security options such as the industry standard AES128 and AES256 encryption algorithms, in addition to this the software can prevent man in the middle attacks through the use of server certificates which uses RSA secret key and counterpart RSA public key within the X.509 SSL certificate, verification failures cause VPN session termination to ensure the integrity and confidentiality of the VPN tunnel. SoftEther also supports multiple authentication mechanisms such as password authentication, certificate authentication, NT domain authentication and RADIUS authentication with up to 4096bit PKI, which also supports smart card and USB tokens.

The software also has additional security features such as packet filters which determines the traffic that is allowed or disallowed within the VPN tunnel, in addition to this the ability to

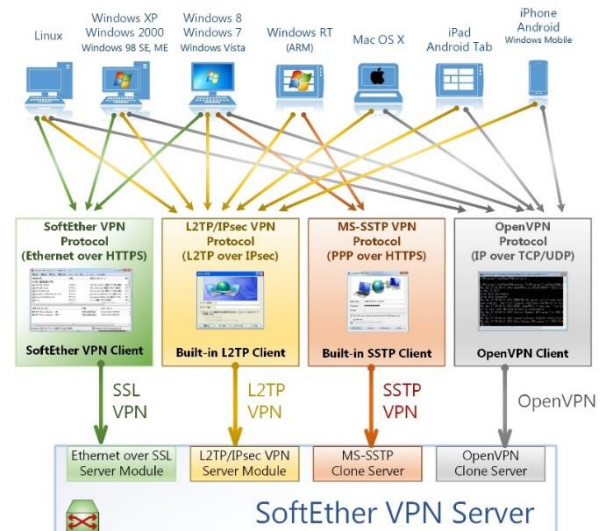


Figure 1- Supported VPN Protocols Diagram [6].

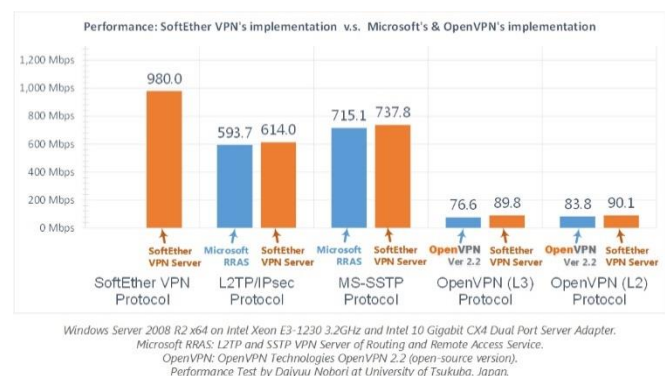


Figure 2 – VPN Throughput Comparison [7].

configure more complex rules is achievable with the security policy configuration and allows more restrictive policy to be applied such as bandwidth filtering, dropping harmful DHCP packets, preventing overlapped MAC addresses and prohibiting bridge/routing functions within the VPN [8]. Finally, the software includes the ability for packet and URL logging of security and packet logs.

3.2 SoftEther VPN Requirements & Limitations

The following section identifies the requirements and limitations of the SoftEther VPN Server & Client software.

3.2.1 Supported Operating Systems

The table below identifies the operating systems supported by SoftEther VPN.

Operating System	Version
Windows (32bit, 64bit)	Windows 98 / 98 SE / ME / NT 4.0 SP6a / 2000 SP4 / XP SP2, SP3 / Server 2003 SP2 / Vista SP1, SP2 / Server 2008 SP1, SP2 / Hyper-V Server 2008 / 7 SP1 / Server 2008 R2 SP1 / Hyper-V Server 2008 R2 / 8 / Server 2012 / Hyper-V Server 2012 / 8.1 / Server 2012 R2 / 10
Linux (32bit, 64bit)	Linux 2.4, 2.6, 3.x
Mac OS X (32bit, 64bit)	Mac OS X 10.4 Tiger / 10.5 Leopard / 10.6 Snow Leopard / 10.7 Lion / 10.8 Mountain Lion
FreeBSD (32bit, 64bit) (Server and Bridge only)	FreeBSD 5, 6, 7, 8, 9
Solaris (32bit, 64bit) (Server and Bridge only)	Solaris 8, 9, 10, 11

Figure 3 – Supported operating systems [9] [10].

3.2.2 Hardware Requirements

SoftEther VPN requires at least the following minimum RAM and disk space to operate, with the recommended option being most efficient [10].

Free RAM

VPN Server Minimum: 32Mbytes + 0.5Mbytes * (Number of Concurrent Sessions).

VPN Server Recommended: 128Mbytes + 0.5 Mbytes * (Number of Concurrent Sessions).

VPN Client Minimum: 16Mbytes.

VPN Client Recommended: 32Mbytes.

Free Disk Space

Minimum: 100Mbytes.

Recommended: 2Gbytes (Daily VPN connection logs).

3.2.3 Software Limitations

The following software limitations apply to the SoftEther VPN Server software [10].

Maximum Concurrent VPN Sessions: 4,096 sessions.

Maximum Virtual Hubs: 4,096 Virtual Hubs.

Users: 10,000

Groups: 10,000

Access List Entries: 32,768

MAC Address Table Entries: 65,536

IP Address Table Entries: 65,536

Cascade Connections: 128

4 Procedure & Results

4.1 SoftEther VPN Management & Reporting Functions

SoftEther VPN has an extensive GUI server management interface, which is easy to use and controls all aspects of the server.

As shown below, the VPN server also has the ability to list a multitude of server status information for management purposes which can be useful to managers and system administrators alike.

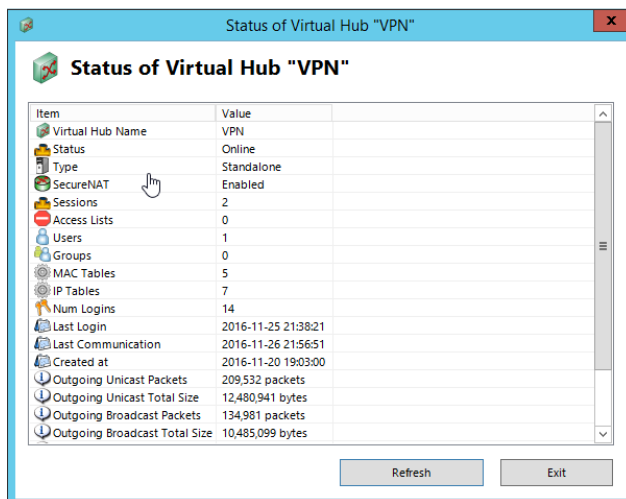


Figure 4 – VPN status view.

In addition to the server status feature, SoftEther VPN has the ability to list the connections list of all current active sessions to the server management interface (Does not include VPN sessions).

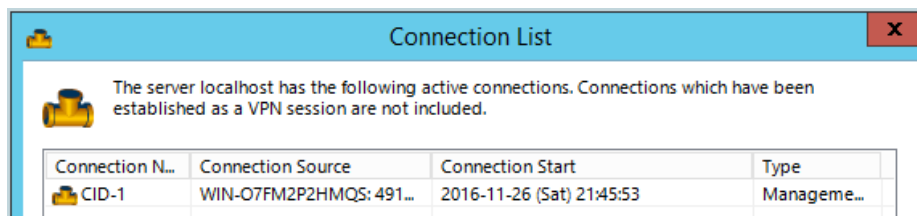
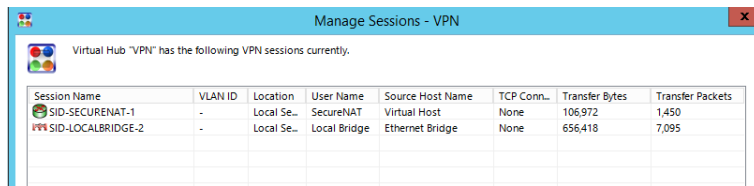


Figure 5 – VPN connections list.

The VPN server also has the capability to manage and view current VPN sessions on the server along, and displays the packet transmission information along with other information.

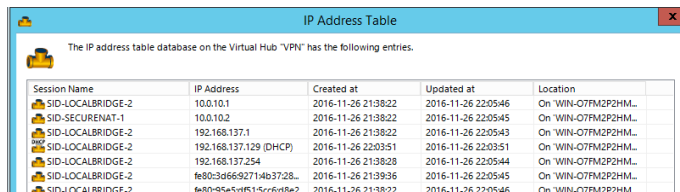


Virtual Hub "VPN" has the following VPN sessions currently:

Session Name	VLAN ID	Location	User Name	Source Host Name	TCP Conn...	Transfer Bytes	Transfer Packets
SID-SECURENAT-1	-	Local Se...	SecureNAT	Virtual Host	None	106,972	1,450
SID-LOCALBRIDGE-2	-	Local Se...	Local Bridge	Ethernet Bridge	None	656,418	7,095

Figure 6 – VPN session management.

As shown below, the VPN displays the IP address table for the virtual hub and all sessions connected to the server, which assists with server administration.

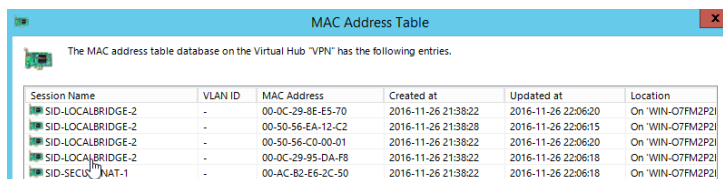


The IP address table database on the Virtual Hub "VPN" has the following entries.

Session Name	IP Address	Created at	Updated at	Location
SID-LOCALBRIDGE-2	10.0.10.1	2016-11-26 21:38:22	2016-11-26 22:05:46	On "WIN-O7FM2P2HM..."
SID-SECURENAT-1	10.0.10.2	2016-11-26 21:38:22	2016-11-26 22:05:45	On "WIN-O7FM2P2HM..."
SID-LOCALBRIDGE-2	192.168.137.1	2016-11-26 21:38:22	2016-11-26 22:05:43	On "WIN-O7FM2P2HM..."
SID-LOCALBRIDGE-2	192.168.137.129 (DHCP)	2016-11-26 22:03:51	2016-11-26 22:03:51	On "WIN-O7FM2P2HM..."
SID-LOCALBRIDGE-2	192.168.137.254	2016-11-26 21:38:28	2016-11-26 22:05:44	On "WIN-O7FM2P2HM..."
SID-LOCALBRIDGE-2	fe80:3a6692714b3728...	2016-11-26 21:39:36	2016-11-26 22:05:45	On "WIN-O7FM2P2HM..."
SID-LOCALBRIDGE-2	fe80:95e5df515cc6d8e2	2016-11-26 21:38:22	2016-11-26 22:05:46	On "WIN-O7FM2P2HM..."

Figure 7 – VPN IP address tables.

The MAC address table was displayed using the graphical view, and displays all MAC addresses which have connected to the system.

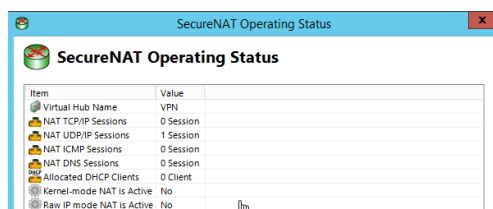


The MAC address table database on the Virtual Hub "VPN" has the following entries.

Session Name	VLAN ID	MAC Address	Created at	Updated at	Location
SID-LOCALBRIDGE-2	-	00-0C-29-8E-E5-70	2016-11-26 21:38:22	2016-11-26 22:06:20	On "WIN-O7FM2P2P2..."
SID-LOCALBRIDGE-2	-	00-50-56-EA-12-C2	2016-11-26 21:38:28	2016-11-26 22:06:15	On "WIN-O7FM2P2P2..."
SID-LOCALBRIDGE-2	-	00-50-56-C0-00-01	2016-11-26 21:38:22	2016-11-26 22:06:20	On "WIN-O7FM2P2P2..."
SID-LOCALBRIDGE-2	-	00-0C-29-95-DA-F8	2016-11-26 21:38:22	2016-11-26 22:06:18	On "WIN-O7FM2P2P2..."
SID-SECURENAT-1	-	00-AC-B2-E6-2C-50	2016-11-26 21:38:22	2016-11-26 22:06:18	On "WIN-O7FM2P2P2..."

Figure 8 – VPN MAC address table.

SecureNAT status can be displayed by using the graphical server management application which is displayed below.

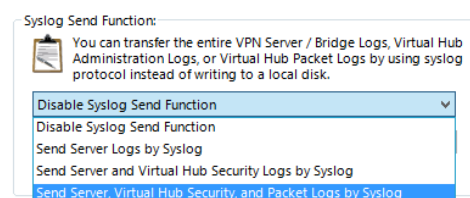


SecureNAT Operating Status

Item	Value
Virtual Hub Name	VPN
NAT TCP/IP Sessions	0 Session
NAT UDP/IP Sessions	1 Session
NAT ICMP Sessions	0 Session
NAT DNS Sessions	0 Session
Allocated DHCP Clients	0 Client
Kernel-mode NAT is Active	No
Raw IP mode NAT is Active	No

Figure 9 – SecureNAT operating status information.

SoftEther VPN also supports Syslog, which sends various logs to a remote logging server, which then could be configured to display graphical statistics and VPN status information.



Syslog Send Function:

You can transfer the entire VPN Server / Bridge Logs, Virtual Hub Administration Logs, or Virtual Hub Packet Logs by using syslog protocol instead of writing to a local disk.

Disable Syslog Send Function

Send Server Logs by Syslog

Send Server and Virtual Hub Security Logs by Syslog

Send Server, Virtual Hub Security, and Packet Logs by Syslog

Figure 10 – Syslog configuration.

In addition to the Syslog functionality, SoftEther VPN has the capability to save a variety of logs to the disk of the VPN server for further analysis by administrators or management.

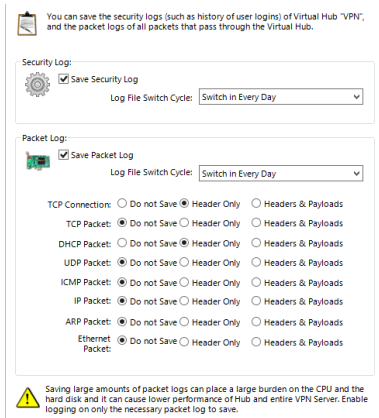


Figure 11 – Logging level configuration.

The VPN server has the ability to restrict permissions by using access control measures for administrator accounts, lower level administrators can be denied and allowed on a per permission basis, allowing for granular access control.

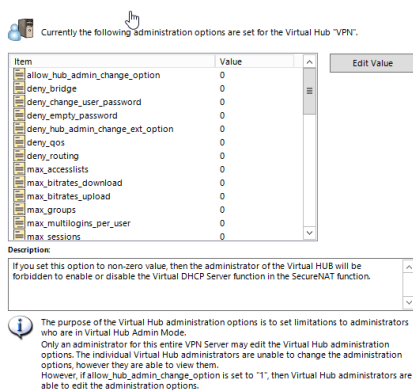


Figure 12 – Access control configuration.

4.1.1 Usability

SoftEther VPN has a simple easy to use interface with a multitude of options and menus available to fully configure the server to the requirements needed. During the installation setup process of SoftEther VPN consultation of online documentation was minimal due to the simple interface and ability to quickly deploy the VPN Solution.

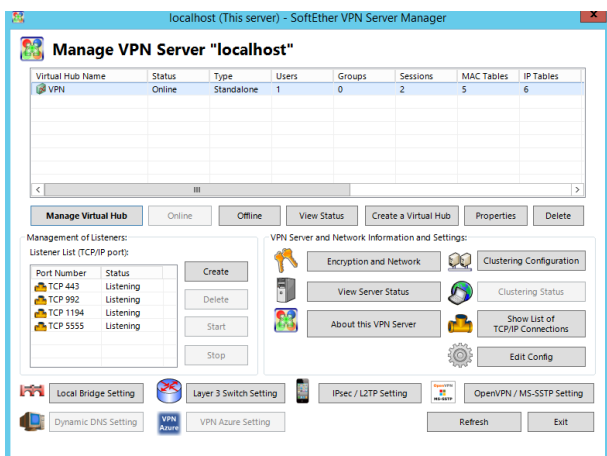


Figure 13 – VPN management overview.

SoftEther VPN supports some integration into Windows Server domains with functionality such as RADIUS/NT Domain authentication, as well as built in packet filters and access control to simulate the features that Windows Server does provide.

The screenshot shows the 'RADIUS Server Settings' window. At the top, a note states: 'To use an external RADIUS server to verify login attempts to the Virtual Hub "VPN", specify an external RADIUS server that verifies the user name and password.' The settings include:

- ☐ Use RADIUS Authentication
- RADIUS Server Host Name or IP: [text box] (use ',' or ';' to split multiple hostnames.)
- Port: [1812] (UDP Port)
- Shared Secret: [text box]
- Confirm Shared Secret: [text box]
- Retry Interval: [500] milliseconds (above 500, below 10000)

 A bottom note with an information icon states: 'The RADIUS server must accept requests from IP addresses of this VPN Server. Also, authentication by Password Authentication Protocol (PAP) must be enabled.' Below this, another note with a warning icon states: 'When using Windows NT Domain Controller or Windows Server Active Directory Controller as an external authentication server, you must setup the VPN Server computer to join the domain. To use NT Domain Authentication, there are no items to configure here.'

Figure 14 – RADIUS configuration.

4.1.2 Security

SoftEther VPN has a number of security implementations and solutions to mitigate against security threats, along with logging functionality for further analysis and detecting attacks.

Authentication -

As shown below, a multitude of authentication solutions exist for the VPN server. SoftEther VPN can integrate into a Windows domain environment using RADIUS Authentication and where needed Smart Card/USB Authentication.

- Plain Password
- RADIUS & Active Directory
- RSA Certificate – PKI 4096Bit
- Smart Card & USB Token

Encryption -

SoftEther VPN supports multiple cipher suites which are current industry best practices such as AES128/AES256 bit encryption.

- RC4 (128 bits)
- AES128 (128 bits)
- AES256 (256 bits)
- DES (56 bits)
- Triple-DES (168 bits)

Hashing -

SoftEther VPN supports HMAC algorithms (Hash-based Message Authentication Code), which are current best practices (SHA-1).

- SHA-1 (160 bits)
- MD5 (128 bits)

Features -

SoftEther VPN supports multiple security features in a variety of areas from firewall packet filtering, to logging and other defences which is shown below.

- ACL Packet Filtering
- Certificate Authentication (Anti-MITM)
- Security Policy
- Per Session Packet Monitor
- Packet Logging
- HTTP URL Logging

4.2 Microsoft Remote Access Management & Reporting Functions

Microsoft Remote Access server utilises server roles and management snap ins to control the VPN server and provide management functionality to the administrator.

As shown below, RRAS provides a management functionality to display the VPN state and the clients currently connected along with remote logging functionality and configuration.

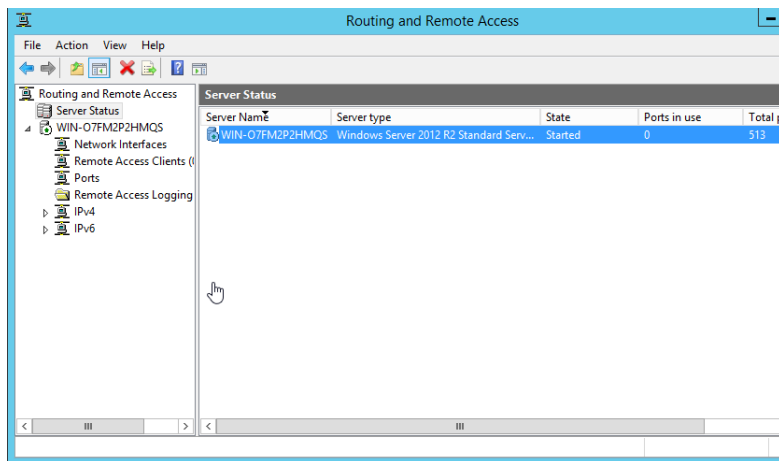


Figure 15 – Routing and Remote Access management console.

In addition to the configuration interface which was shown in figure 15, Remote Access provides a dedicated management console which displays a multitude of options such as client status, reporting and operational status.

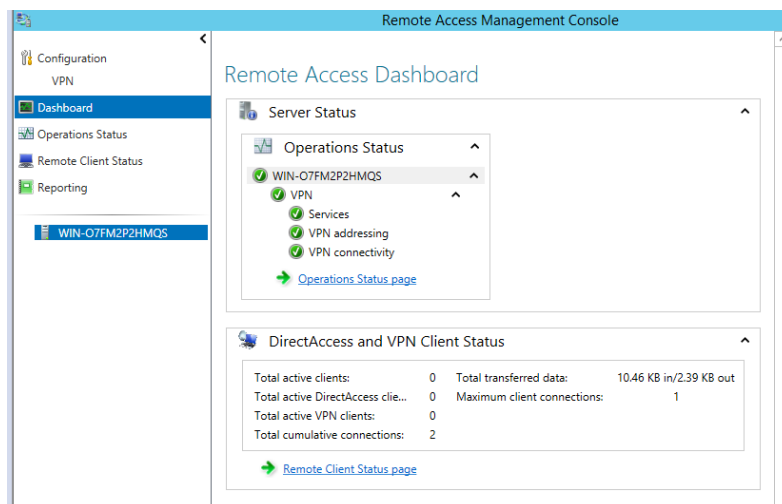


Figure 16 – Remote access dashboard.

The Microsoft RRAS server provides a dedicated “Operational Status” option which displays the current service states of the VPN and the dependences needed along with the uptime of the service and its current state.

Operations Status

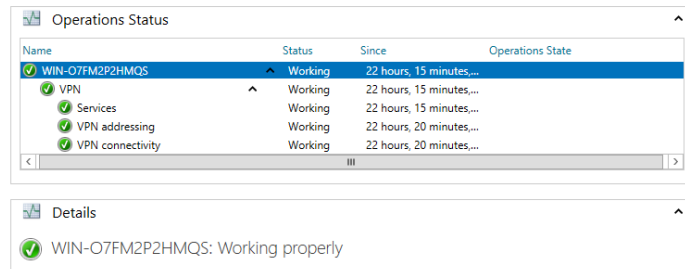


Figure 17 – Remote access management console (Operational status).

As shown below, the remote access management console displays all current connected VPN clients along with other information that can be useful to a system administrator.

Remote Access Clients Status

Connected Clients

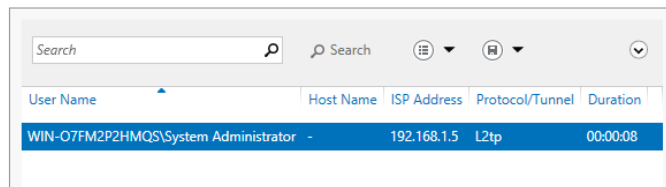


Figure 18 – Remote access client status. (VPN connections).

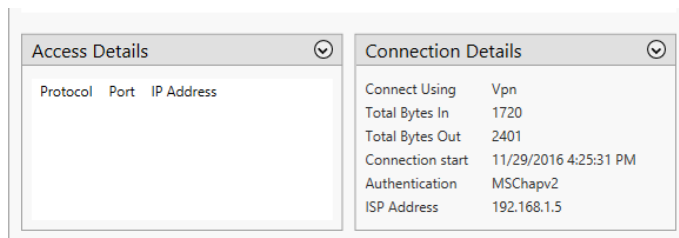


Figure 19 – Remote access client status (Connection details).

The VPN server also provides a reporting functionality which displays a log of previously connected systems and connection/address details.

Remote Access Reporting

Start date: 11/29/2016 15 End date: 11/29/2016 15 [Generate Report](#)

Usage Report

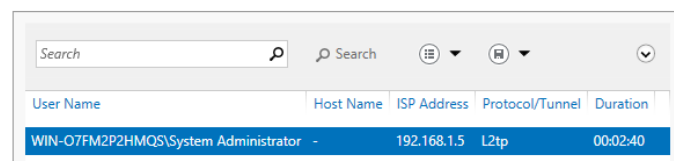


Figure 20 – Remote access reporting.

4.2.1 Usability

The Windows Remote access management console offers an easy to use GUI solution to viewing statistics and reporting from the VPN solution as well as tweaking the configuration after installation.

However, the setup process and manual configuration options needed to allow VPN connections requires more extensive knowledge of the Windows Server solution and the VPN server itself. TechNet resources were accessed to assist with the installation of this server due to the more difficult setup procedure that the solution requires.

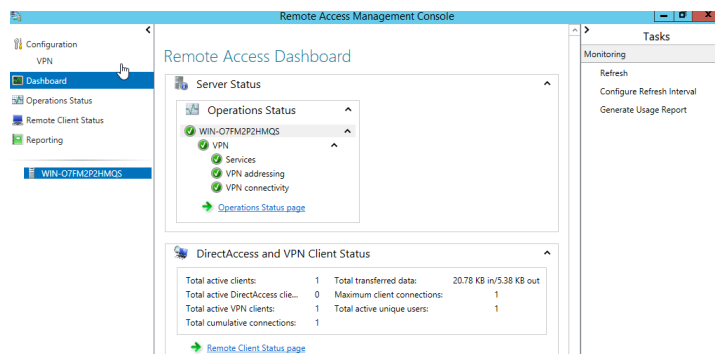


Figure 21 – Remote access management console (Dashboard).

4.2.2 Security

Microsoft Remote Access provides security functionality to ensure the VPN connection remains protected against threats, as shown below.

Authentication –

The VPN server currently supports the following authentication mechanisms

- Extensible authentication protocol (EAP)
- Microsoft encrypted authentication v2 (MS-CHAP V2)
- Encrypted authentication (CHAP)
- Unencrypted password (PAP)
- Machine certificates (IKEv2)
- Unauthenticated access

Encryption –

Microsoft Remote Access currently provides the following encryption cyphers [11].

- Data Encryption Standard (3DES)
- Diffie-Hellman Medium
- Transport Mode
- Encapsulating Security Payload (ESP)

Hashing –

- Secure Hash Algorithm (SHA-1)

Features –

The following features are currently provided by Microsoft Remote Access with some being limited to a specific client operating system [13].

- Static packet filtering
- Windows firewall
- Network access policies
- Client group policy security enforcement
- Traffic filters (Windows 10)
- LockDown VPN (Windows 10)
- Windows Information Protection (WIP) (Windows 10)
- Logging

5 Discussion

This discussion focuses on the main topic of the whitepaper which was to compare both commercial and open source solutions by analysing the feasibility of each VPN solution along with the benefits, downsides, as well as the requirements and limitations and how these solutions can improve the organisation and business operations.

The aim of this whitepaper was achieved by assessing the feasibility of the solution by configuring a test environment with GNS3 and a Windows server/client to test each solution throughout and assessing the usability and ease of use of each system. It was identified that the SoftEther VPN provides extensive VPN functionality with a variety of protocols and configuration options.

5.1 SoftEther vs Microsoft Remote Access (RRAS)

The VPN solution that has been identified for this whitepaper was compared against Microsoft Remote Access to assess the feasibility and differences between the open source software and the current paid solution.

The figure below compares the features of each VPN solution.

Features	SoftEther VPN	Microsoft Remote Access
License	GPL – Open Source	Proprietary - Paid
Platforms	Windows, Linux, FreeBSD, Mac OS X, IOS, Android	Windows, Max OS X, IOS, Android
Supported VPN Protocols	OpenVPN, L2TP/IPSec, EtherIP, Microsoft SSTP, VPN over HTTPS (SSL-VPN), VPN over DNS, VPN over ICMP	L2TP, SSTP, PPTP
Native VPN Client Support	Windows (L2TP, SSTP) Mac OS X (L2TP) IOS (L2TP) Android (L2TP)	Windows (L2TP, SSTP) Mac OS X (L2TP) IOS (L2TP) Android (L2TP)
GUI Management	X	X
CLI Management	X (Dynamic Configuration like Cisco IOS)	X (Powershell)

Dynamic DNS Function	X	
DHCP & NAT Function	X	X
Packet Filtering	X	X
Smartcards & USB Token Support	X	X
Throughput	980Mbps (SEVPN) 614Mbps (SEVPN L2TP) 738Mbps (SEVPN SSTP)	N/A 594Mbps (L2TP) 715Mbps (SSTP)
RADIUS Authentication	X	X
Certificate Authentication	X	X
VPN Server Clustering	X	X
Multi-Tenant Support	X	X
IPv6 Support	X	X
Site-to-Site VPN Support	X	X
Azure Cloud Support	X	X
Windows Group Policy Intergration		X
Price Model	Free	Paid Windows Server licenses Remote Access licenses

Figure 22 – SoftEther VPN vs Microsoft Remote Access comparison table [6] [13].

As shown in the comparison table above, SoftEther VPN provides an extensive set of features and protocols compared to the market leader Microsoft Remote Access. Although SoftEther VPN does not support features such as Direct Access and integration with Windows Server with technologies such as group policy enforcement for VPN's

Microsoft Remote Access requires a knowledge of the server management functionality which includes role management and this increases the complexity of deploying the VPN solution within an environment. Resources exist such as TechNet to provide installation documentation and other information.

In addition to the higher complexity of installation. Microsoft Remote Access only supports Windows server and does not support other operating systems for the VPN server, which can increase ease of use for server administrators with other operating system experience.

Microsoft Remote Access also does not support other server operating systems whereas SoftEther VPN can be installed on a variety of Linux operating systems which would allow for a totally open source solution without Windows Server licensing fees and remote access client license costs. In addition to this, support can be provided from the SoftEther corporation as well as from the open source community in regards to Linux operating systems.

Performance is also a key aspect of modern VPN's and SoftEther VPN when previously tested outperformed Microsoft Remote Access as well as other open source/paid solutions such as OpenVPN which shows that SoftEther VPN is a serious contender to the commercial space (See figure 21).

Reporting and logging is also more easy to access and understand within the SoftEther management console and allows for flexibility in how logging is handled with features such as syslog and disk logs with a customizable level of logging detail that can be configured and implemented.

With SoftEther providing DNS via ICMP as well as ICMP via DNS, the possibility of using SoftEther VPN on a more restricted network such as public-wifi exists where common VPN ports are usually blocked which would ensure corporate VPN clients stay protected wherever they go, and to date Microsoft Remote Access does not provide this feature to users.

SoftEtherVPN as well as Microsoft Remote Access both offer similar industry standard encryption settings which ensures communications are secure, however SoftEther VPN does provide signature verification options to prevent against man in the middle attacks which makes SoftEther VPN more robust against those sorts of attacks.

5.2 Future Work

It was identified during this whitepaper that future work and research could be investigated into a number of areas such as other open source VPN solutions such as Open VPN which offers some similar VPN functionality, as well as the included clone OpenVPN server included within the SoftEther VPN server.

Other areas of research and work include testing and deploying RADIUS/NT Domain authentication for SoftEther VPN and comparing the setup between Microsoft Remote Access and this solution.

Finally, other paid VPN solutions from commercial vendors could be compared between SoftEther VPN from vendors such as Cisco, Juniper, FortiGate and a variety of other paid vendors.

6 Conclusion

In conclusion, it has been identified during this whitepaper that SoftEther VPN provides an extensive amount of functionality and features without the implied costs and license fees of commercial and paid software. The only major differences between the two software solutions were the fact that Microsoft Remote Access has extensive integration into Windows active directory whereas SoftEther VPN does not provide that functionality. Despite this, SoftEther VPN offers RADIUS/NT domain authentication which does allow some of the same functionality's that Microsoft Remote Access can provide.

Earlier during the whitepaper in figure 2, it was identified that SoftEther VPN provides an increased level of throughput compared to market rivals both commercial and open source alike without the commercial price tag. Further to this, SotherEther VPN provides an extensive amount of security features such as packet filtering, administrator access control, and management functions which allow for system administrators to view important server information when administrating a VPN solution.

Finally, it has been demonstrated through the research and software investigation during this white paper that that the objectives have been achieved by deploying two rival VPN solutions (Commercial vs open source) and then comparing the features. During the deployment, the

configuration and installation of each solution was documented (Appendix – Section 8) to later assess the usability and ease of use for each solution. It was identified that future research into other VPN solutions is possible.

7 References

- [1] OpenVPN (2016). *OpenVPN – Open Source VPN*. [Online]. Available at: <https://openvpn.net/> [Accessed 18th November 2016].
- [2] S. Jha (2014). *What Is Routing and Remote Access?*. [Online]. Available at: [https://technet.microsoft.com/en-us/library/cc771052\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771052(v=ws.10).aspx) [Accessed 18th November 2016].
- [3] ONF (N.d). *Software-Defined Networking (SDN) Definition*. [Online]. Available at: <https://www.opennetworking.org/sdn-resources/sdn-definition> [Accessed 19th November 2016].
- [4] Cisco (2007). *Introduction to Cisco IPSec Technology*. [Online]. Available at: https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html [Accessed 21st November 2016].
- [5] SoftEther VPN (N.d). *Ultimate Powerful VPN Connectivity*. [Online] https://www.softether.org/1-features/1_Ultimate_Powerful_VPN_Connectivity [Accessed 21st November 2016].
- [6] SoftEther VPN (N.d). *SoftEther VPN Open Source*. [Online]. Available at: <https://www.softether.org/> [Accessed 22nd November 2016].
- [7] D. Nobori (2013). *Design and Implementation of SoftEther VPN*. [Online]. Available at: www.softether.org/4-docs/9-research/Design_and_Implementation_of_SoftEther_VPN [Accessed 24th November 2016].
- [8] SoftEther VPN (N.d). *Security and Reliability*. [Online]. Available at: www.softether.org/1-features/3_Security_and_Reliability [Accessed 24th November 2016].
- [9] SoftEther VPN (N.d). *Operating System Requirements*. [Online]. Available at: https://www.softether.org/4-docs/1-manual/3_SoftEther_VPN_Server_Manual/3.1_Operating_System_Requirements [Accessed 26th November 2016].
- [10] SoftEther VPN (N.d). *Specification – Basic Capabilities of SoftEther VPN Server*. [Online]. Available at: www.softether.org/3-spec [Accessed 26th November 2016].
- [11] Microsoft (N.d). *Default Encryption Settings for the Microsoft L2TP/IPSec Virtual Private Network Client*. [Online]. Available at: <https://support.microsoft.com/en-us/kb/325158> [Accessed 29th November 2016].
- [12] Microsoft (N.d). *VPN Tunnelling Protocols*. [Online]. Available at: [https://technet.microsoft.com/en-us/library/cc771298\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx) [Accessed 29th November 2016].

[13] Microsoft (N.d). *What's New in Routing and Remote Access*. [Online]. Available at: [https://technet.microsoft.com/en-us/library/cc753256\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc753256(v=ws.10).aspx) [Accessed 29th November 2016].

8 Appendices

8.1 Appendix A - Installing & Configuring SoftEther VPN Server

The first step was to download the VPN Server software from the SoftEther VPN website, and then select the Windows Server Manager for Windows, as shown in the figures below.



Figure 23 – SoftEther VPN download.

For the installation process, the “Next” button should be selected unless directed otherwise.

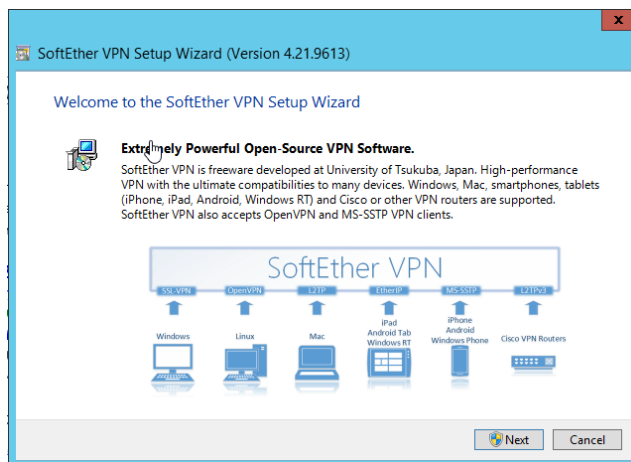


Figure 24 – VPN setup wizard.

Once the software components selection window appears, the next step was to select “SoftEther VPN Server” and then click next. This installs both the Server Manager and VPN Server.

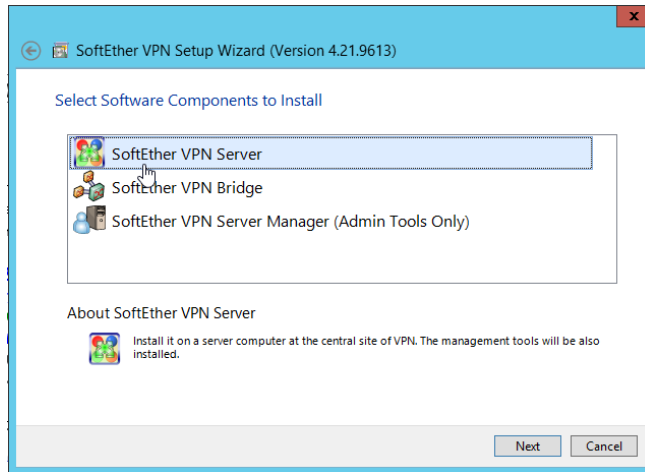


Figure 25 – VPN setup wizard (Components selection).

After reviewing the terms of the end user license agreement, the next button was pressed to continue with the installation.

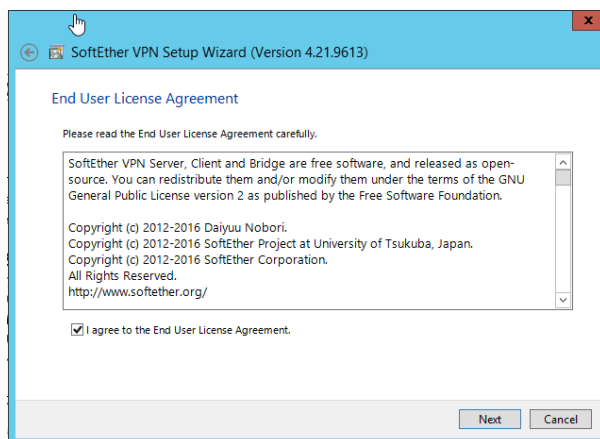


Figure 26 – VPN setup wizard (EULA agreement).

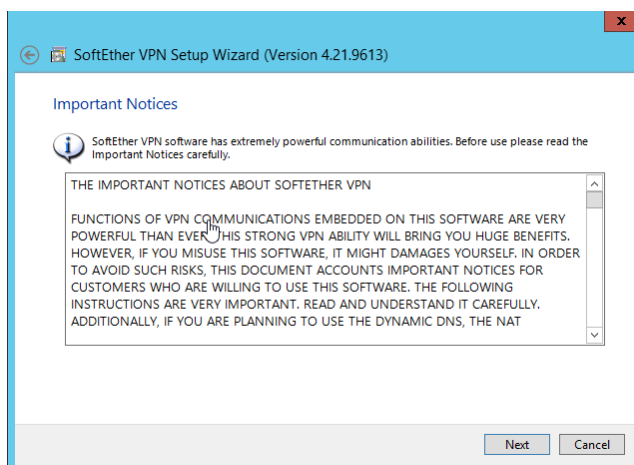


Figure 27 – VPN setup wizard (Important notices).

The default installation directory was kept as default along with ticking advanced options and install on the computer entirely.

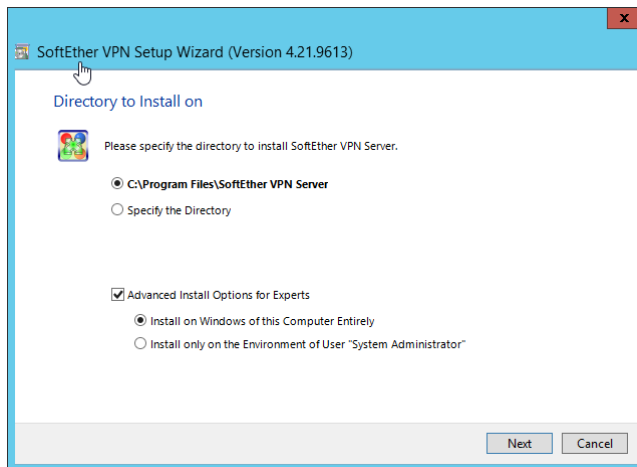


Figure 28 – VPN setup wizard (Directory setup).

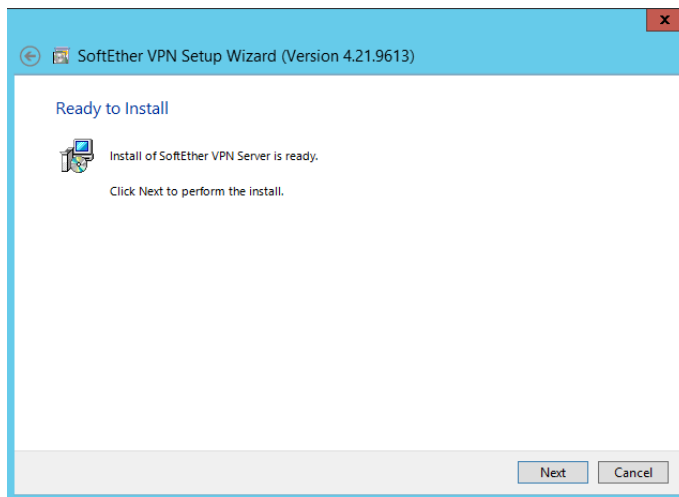


Figure 29 – VPN setup wizard (Installation confirmation).

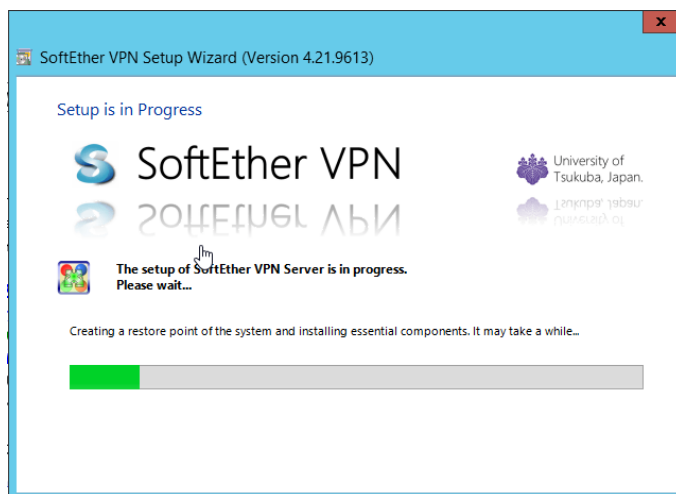


Figure 30 – VPN setup wizard (Installation progress).

During the setup process, a popup appeared to install the VPN device driver onto Windows, the install option was selected along with always trusting the software from SoftEther Corporation and then finally the VPN server was installed as shown in the figures below.

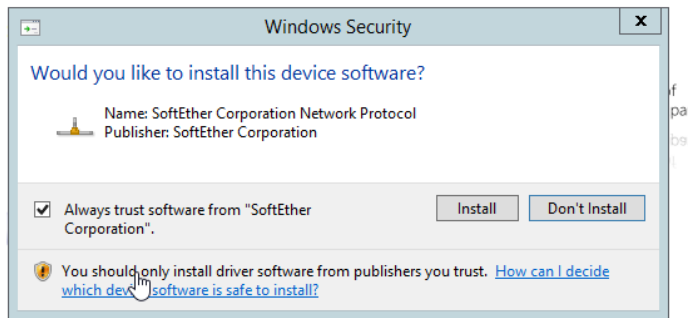


Figure 31 – VPN adapter installation.

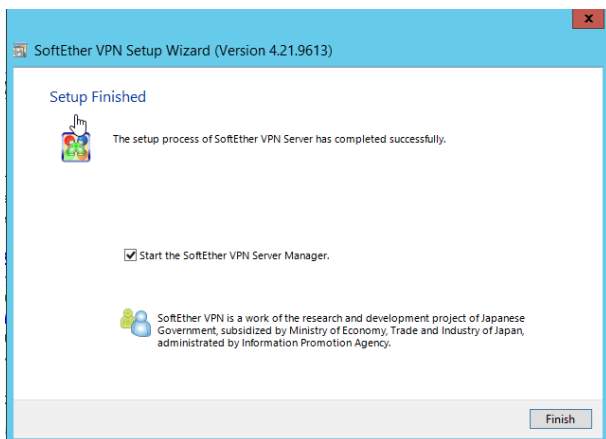


Figure 32 – VPN setup wizard (Setup complete).

The first step of configuring the VPN server was to launch the SoftEther VPN Server Manager and connect to the localhost server.



Figure 33 – VPN setup wizard (Connection settings).

Once the connection was established, a prompt appeared for setting the administration password and was set to "!vpn!server!" for this demonstration.

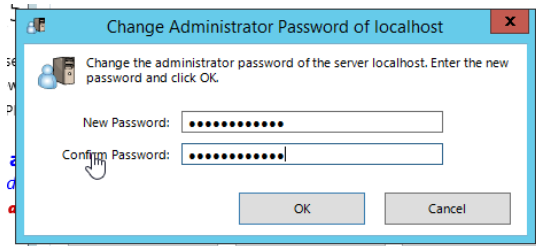


Figure 34 – VPN connection manager (Change password).

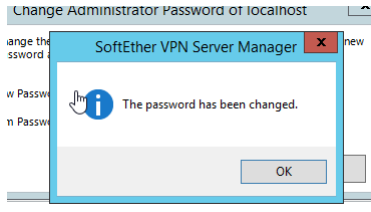


Figure 35 – Change password process (Success).

The next step was to configure the VPN server function which was as a “Remote Access VPN Server”, due to the fact that remote clients would be connecting to this system and not as a site to site VPN function.

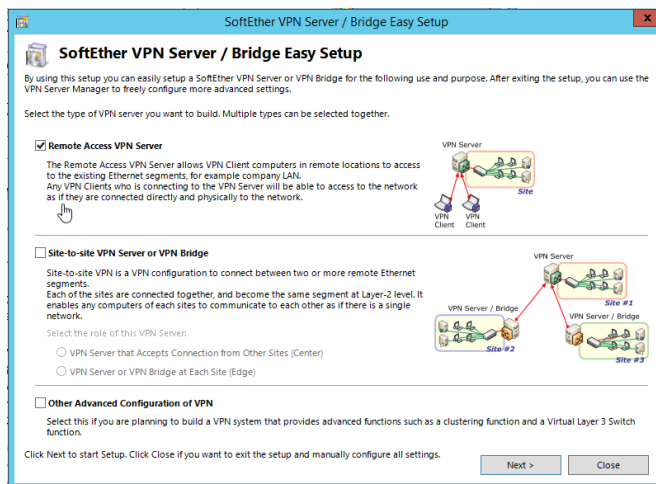


Figure 36 – VPN & bridge server setup.

The next step was to configure the VPN hub name, for the sake of the demonstration it was decided that the hub name would be “VPN”.

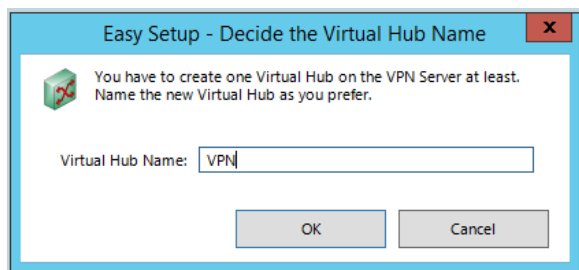


Figure 37 – Virtual hub name setup.

As the organisation is using a static IP address for this server, the following DNS settings were left unchanged.

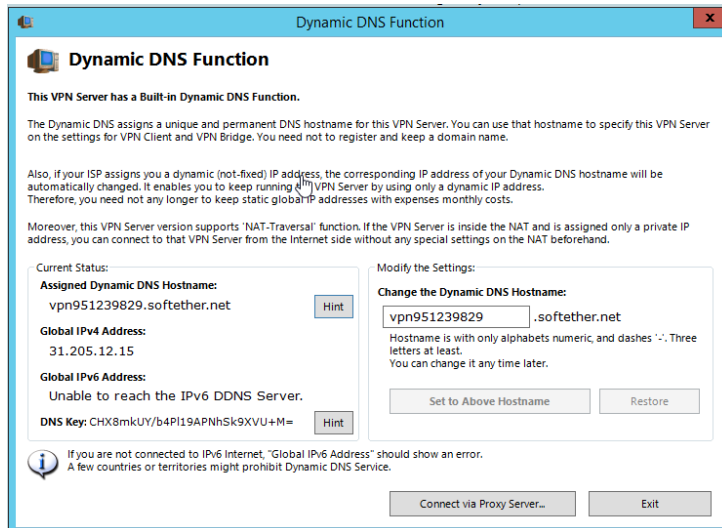


Figure 38 – Dynamic DNS setup.

The next step was to configure IPSec / L2TP VPN, so that clients can connect to the server on a variety of devices, IPSec was selected to ensure the confidentiality of data in transit and a pre-shared key was selected.

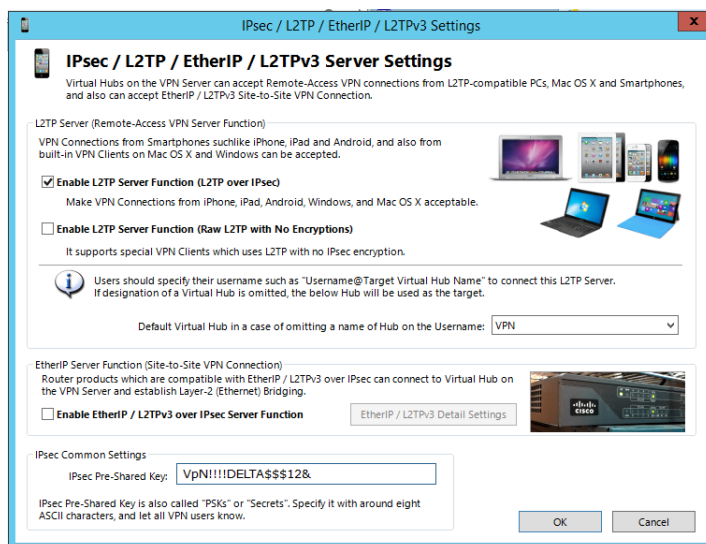


Figure 39 – L2TP VPN settings.

The VPN Azure Cloud was disabled as the demonstration network did not have a need for this service due to the server being dedicated to VPN services. Although this functionality does exist if needed.

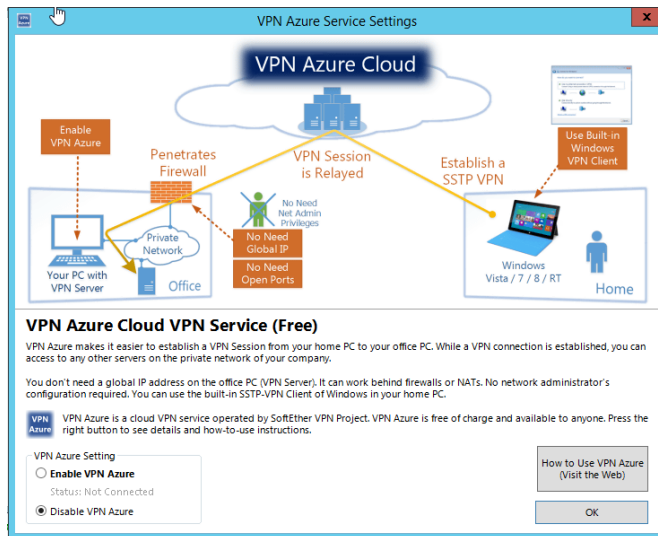


Figure 40 – VPN Azure cloud.

After disabling the VPN Cloud, the next step was to add a new normal VPN user to the server by using the GUI, for this step password authentication was selected along with the username of “testuser” and password of “testuser”.

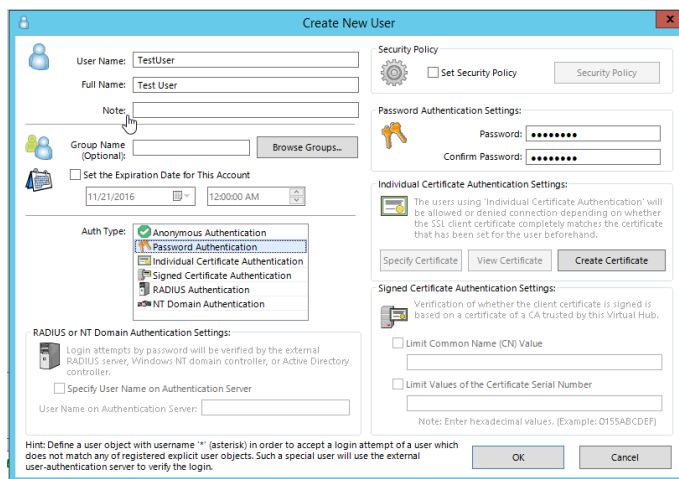


Figure 41 – User creation wizard.

The next step was to configure a local bridge via the server manager overview which ensures the local network is bridged with the VPN server.

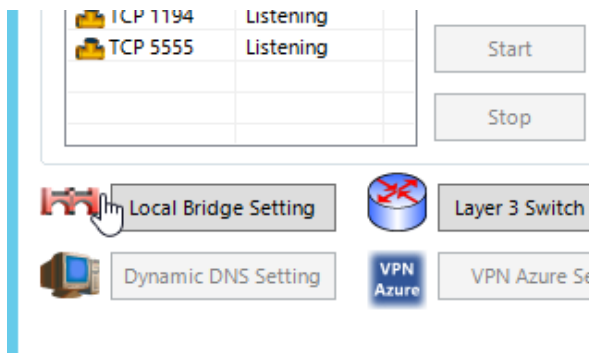


Figure 42 – VPN overview (Local bridge settings).

In the figure below, the VPN bridge is configured to Ethernet 2 which bridges the VPN server to the local business network and ensures VPN clients can communicate with the local network.

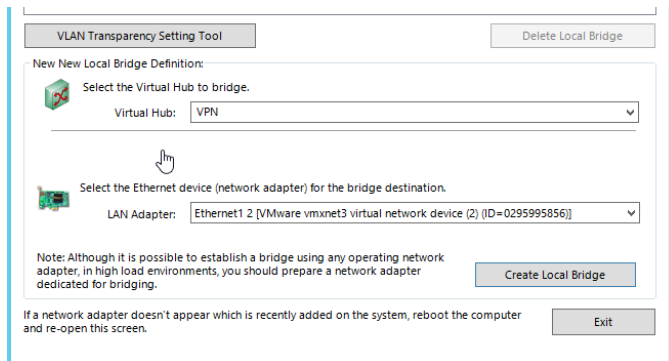


Figure 43 – Local bridge configuration.

From the main server manager window, the next step was to click “Manage Virtual Hub”, and then “Virtual NAT and Virtual DHCP Server (SecureNAT)” as shown in Figure 15 and 16.

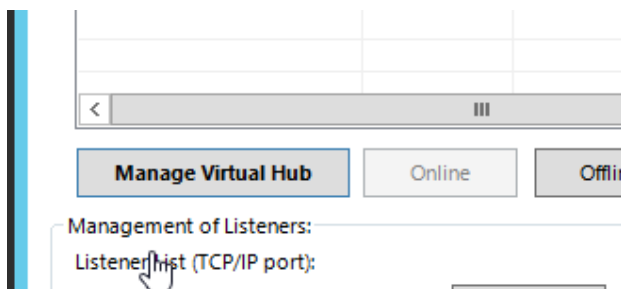


Figure 44 – VPN overview (Manage virtual hub).

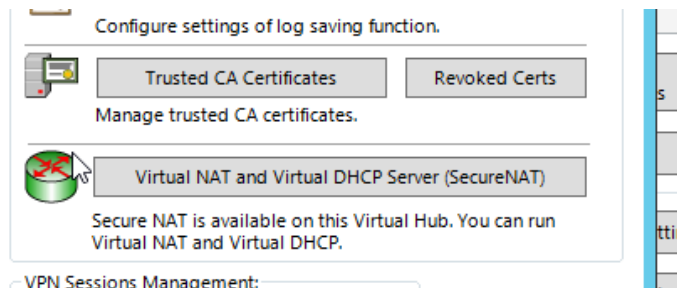


Figure 45 – SecureNAT settings.

The next step was to “Enable SecureNat”, and then edit the SecureNAT configuration, as shown below in Figure 17 and 18.

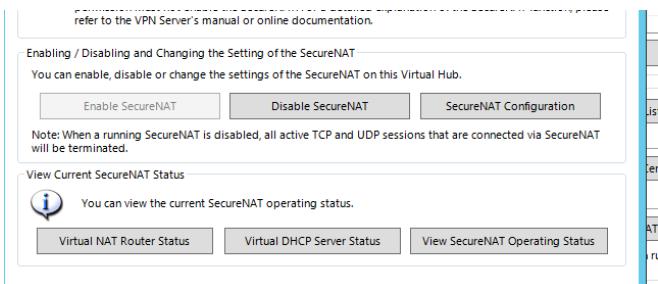
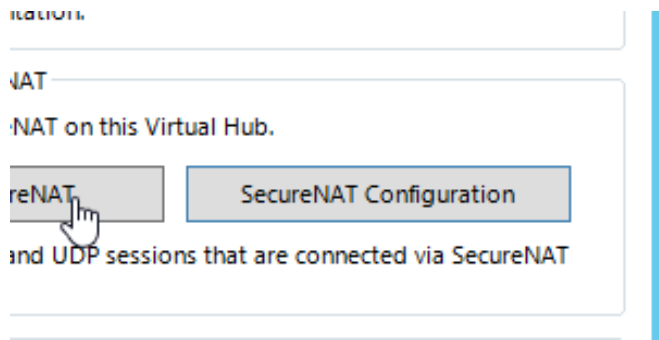
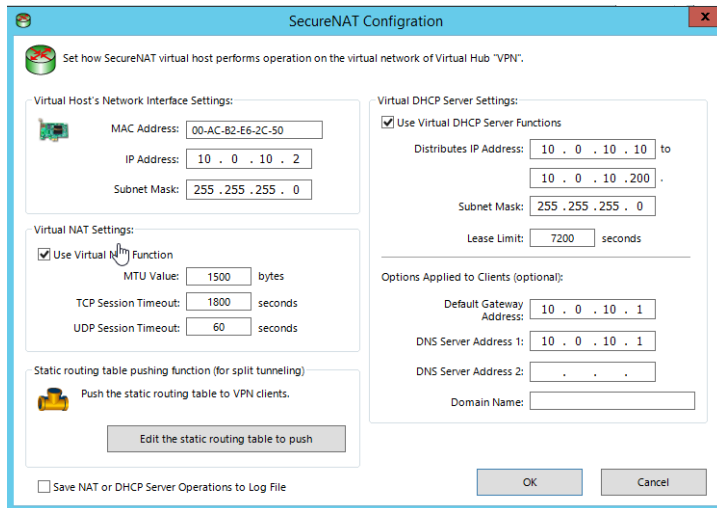
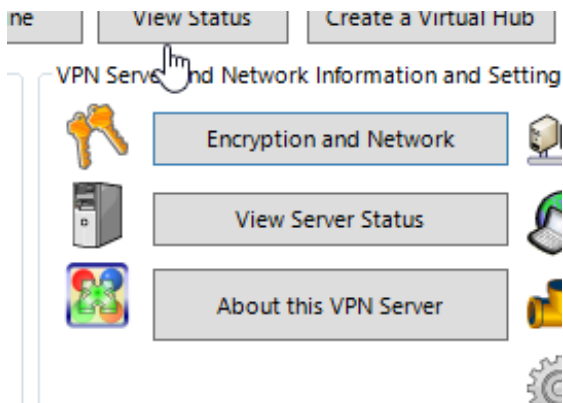


Figure 46 – SecureNAT settings.*Figure 47 – SecureNAT configuration.*

The following settings were applied to the SecureNat Configuration to ensure the VPN server provides IP addresses to VPN clients and then can communicate with local resources via the bridge connection, as shown below.

*Figure 48 – SecureNAT configuration.*

The next step was to configure the encryption cipher of the VPN tunnel traffic.

*Figure 49 – VPN encryption and network settings.*

The encryption algorithm was set to “DHE-RSA-AES256-SHA” to ensure the most secure encryption method is used for SSL VPN encryption.

You can view or change settings related to encryption, communication and security.

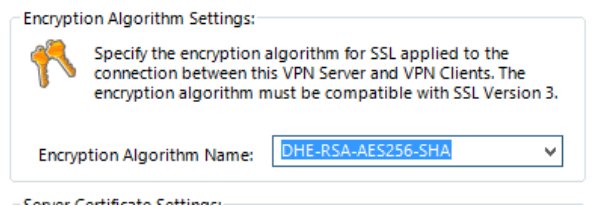


Figure 50 – VPN encryption and network settings (Ciphers).

The next step is to disable Open VPN, and enable MS-SSTP VPN protocol as our environment is based on Microsoft technologies and for this demonstration IPsec based VPNs were used.

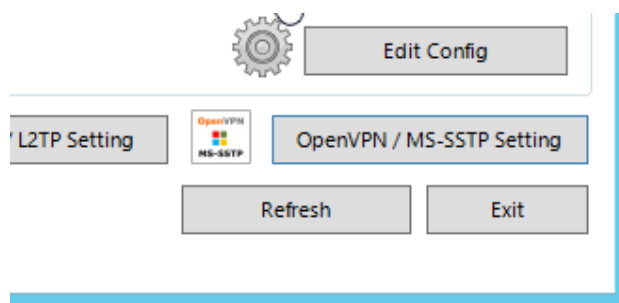


Figure 51 – OpenVPN/MS-SSTP settings.

As shown below, Open VPN was disabled and then MS-SSTP VPN enabled.

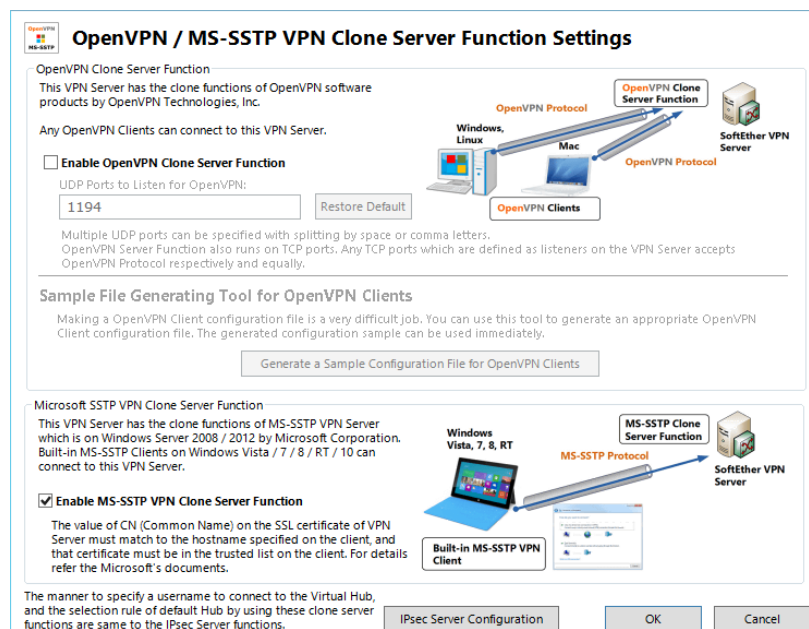


Figure 52 – OpenVPN/MS-SSTP server function settings.

The next step was to edit the VPN server properties from the main server configuration, as shown below.

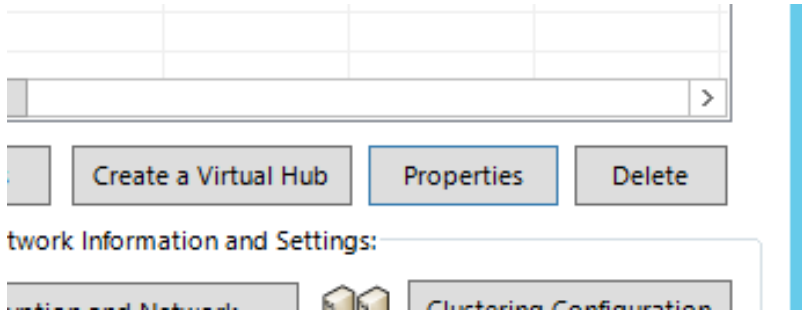


Figure 53 – VPN server properties.

In the figure below enumeration was disabled for anonymous users.

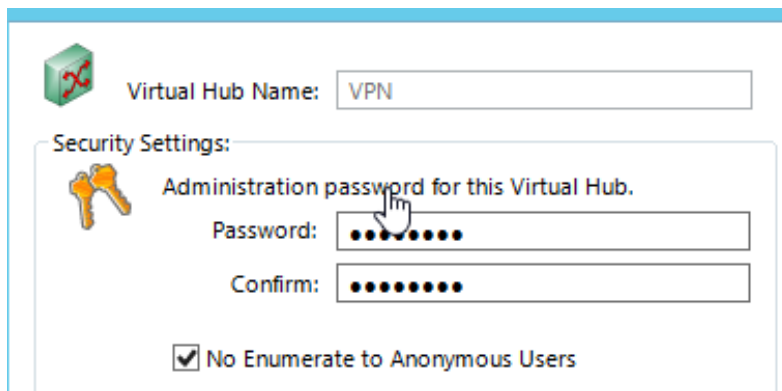


Figure 54 – VPN server properties (Administration password).

8.2 Appendix B – Installing & Configuring SoftEther VPN Client

The first step was to download the SoftEther VPN Client from the SoftEther website and then select the Windows platform and download the client.

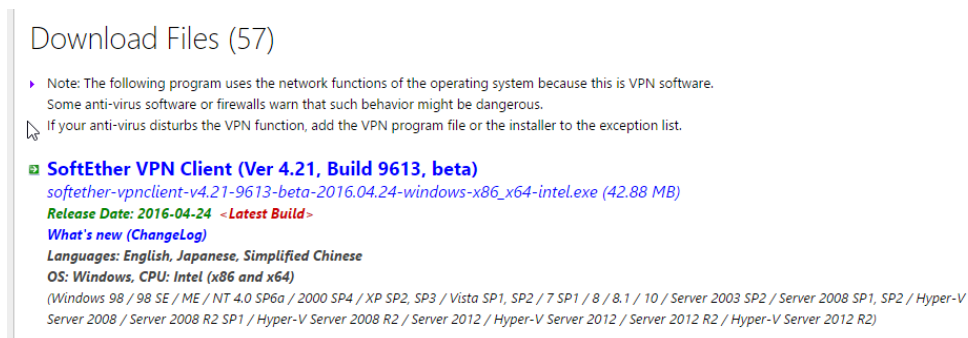


Figure 55 – VPN client downloads.



Figure 56 – VPN client setup wizard.

After continuing with the installation process, the next thing to do was to select “SoftEther VPN Client” and then next.

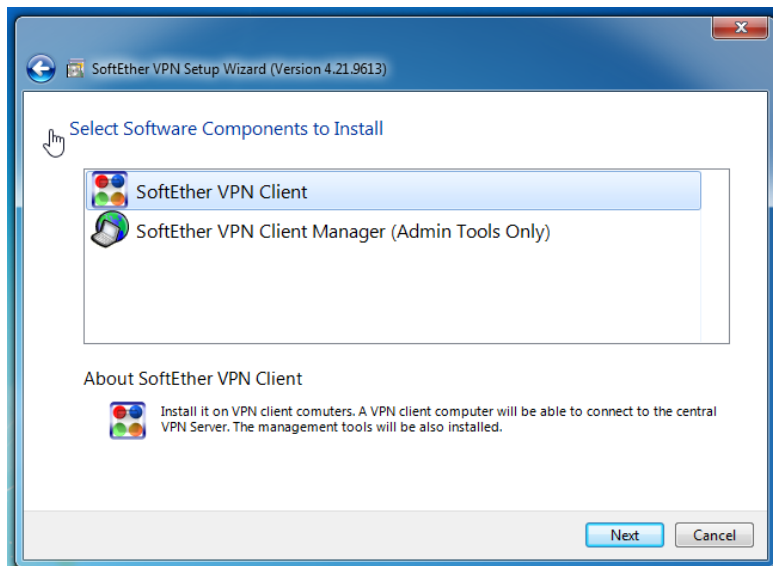


Figure 57 – VPN client setup wizard (Components selection).

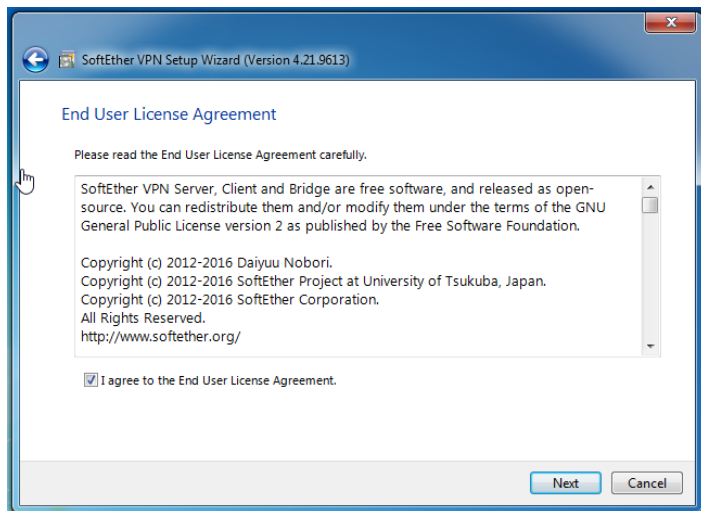


Figure 58 – VPN client setup wizard (EULA agreement).

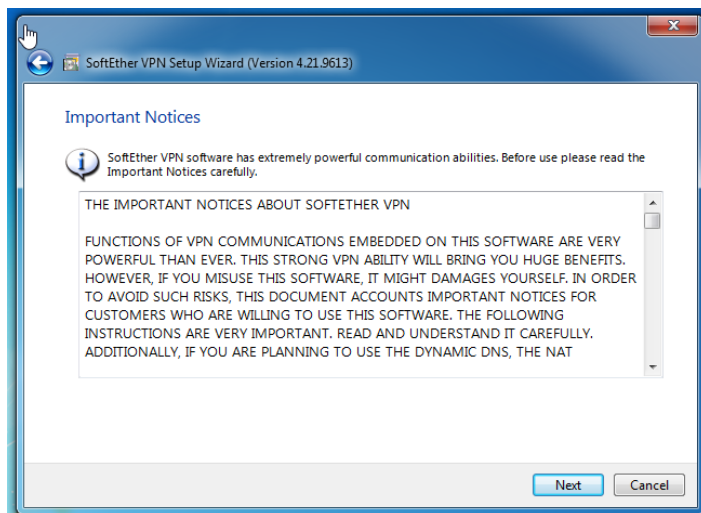


Figure 59 – VPN client setup wizard (Important notices).

The next step of the process was to tick “Advanced Install Options for Experts” and ensure the computer entirely was selected.

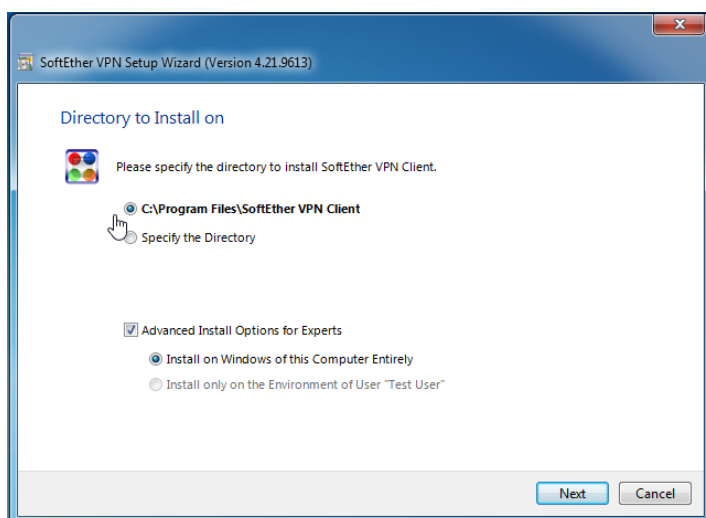


Figure 60 – VPN client setup wizard (Directory setup).

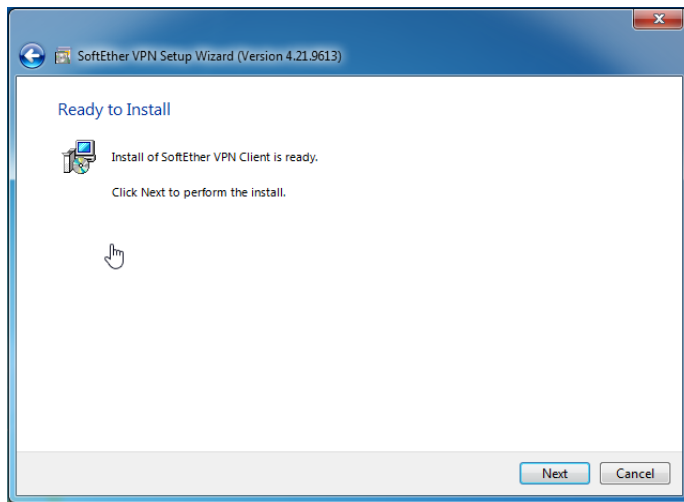


Figure 61 – VPN client setup wizard (Installation).

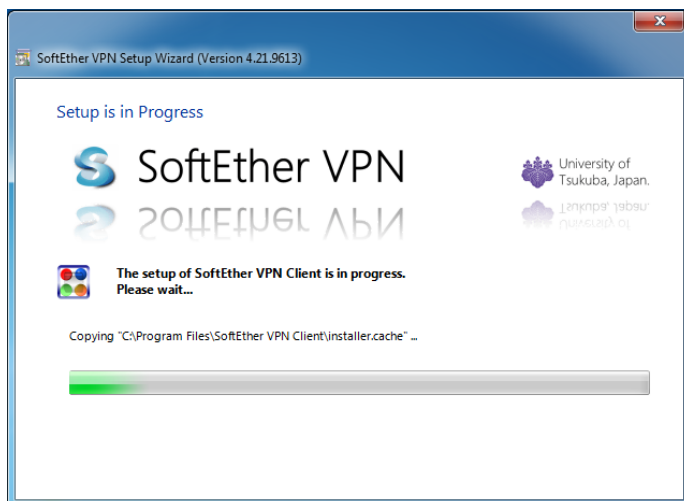


Figure 62 – VPN client setup wizard (Install progress).

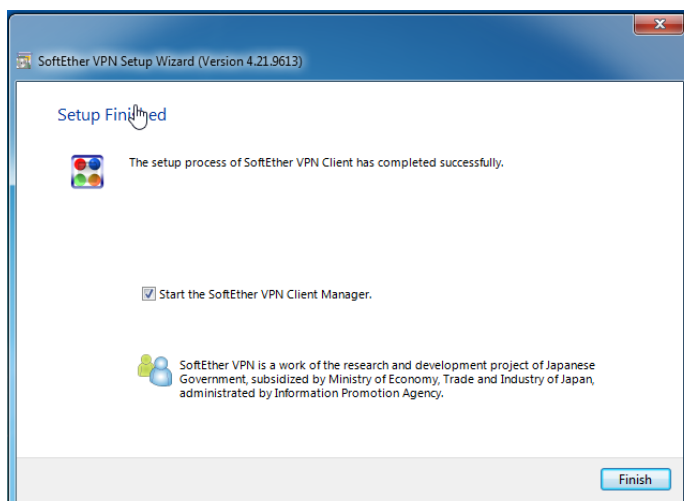


Figure 63 – VPN client setup wizard (Installed).

The next step was to configure the VPN client on the Windows 7 machine and establish a connection with the remote VPN server to demonstrate the functionality and feasibility.

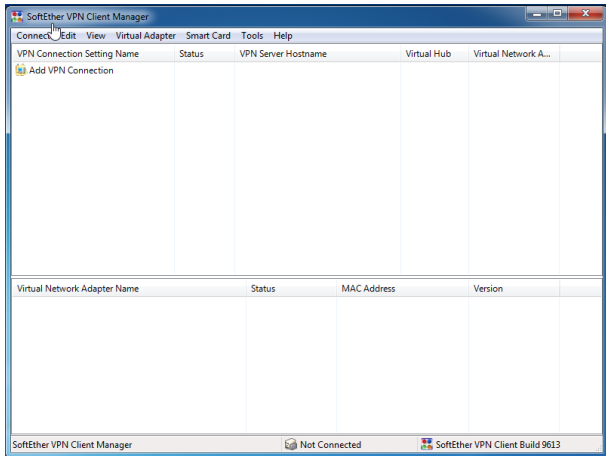


Figure 64 – VPN client manager (Overview).

The next step is to “Add a VPN Connection” and then confirm the action as shown in the figure below.

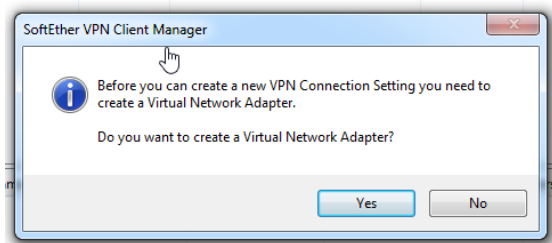


Figure 65 – VPN client manager (VPN adapter creation).

During the first step of a VPN, an adapter needs to be created for the system. For demonstration purposes the adapter name of “VPN” was used.

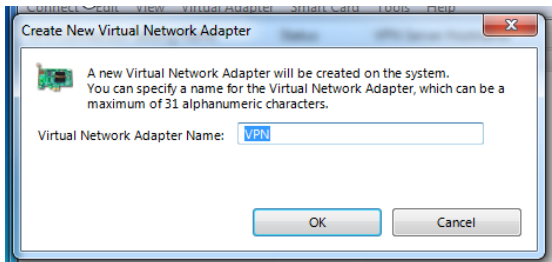


Figure 66 – VPN client manager (Adapter naming).

Once the adapter was created, the installation process started for the virtual network adapter.

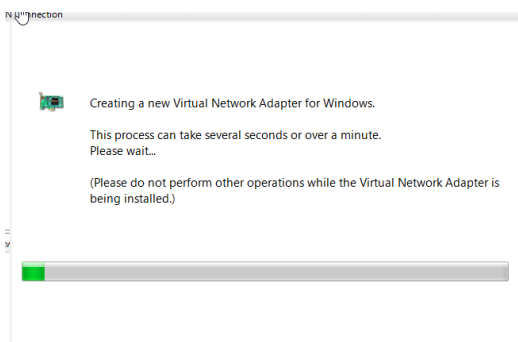


Figure 67 – VPN adapter creation progress.

The next step was to configure the VPN client connection settings, such as the username and password with standard password authentication.

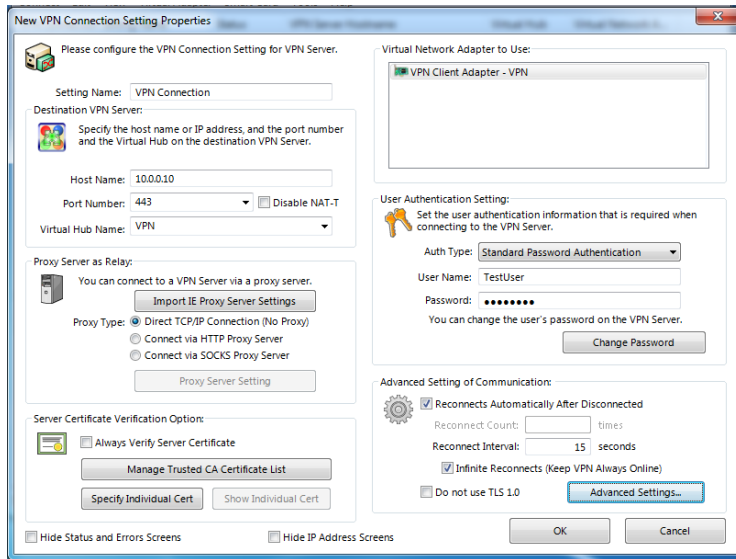


Figure 68 – VPN client connection settings.

After configuring the VPN settings, the connection was established to the VPN by double clicking the connection.

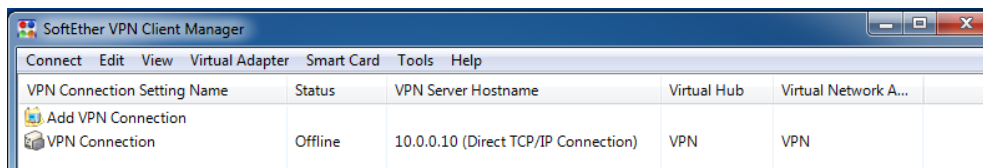


Figure 69 – VPN client manager overview.

For the demonstration, DNS has not been set for the dynamic DNS hostname however in a production environment this message would not be displayed once configured correctly. The connection was resumed, as shown below.

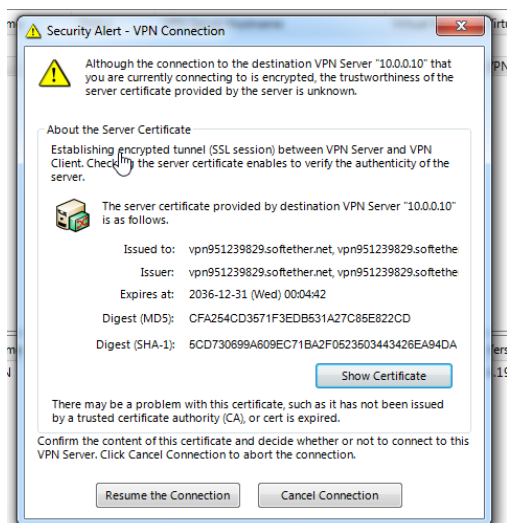


Figure 70 – Server certificate signature verification.

The VPN certificate authority was trusted in the figure shown below, to ensure VPN connects without error on the next connection.

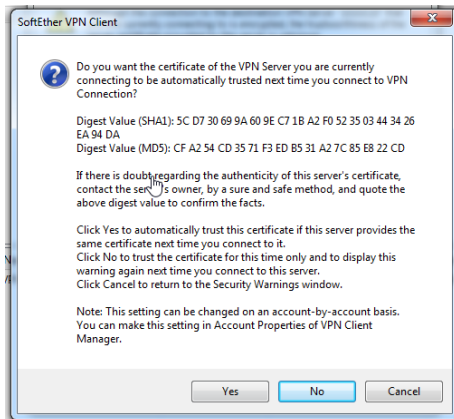


Figure 71 – Remote server digest verification.

As shown below, the VPN is successfully connected and requested a DHCP IP address from the server.

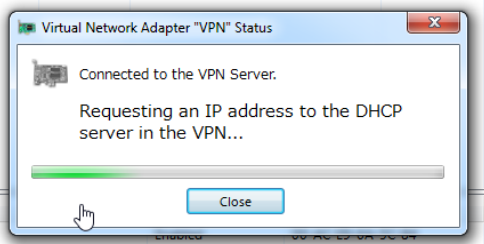


Figure 72 – VPN client connection status (DHCP).

As shown below, the VPN connection was established successfully.

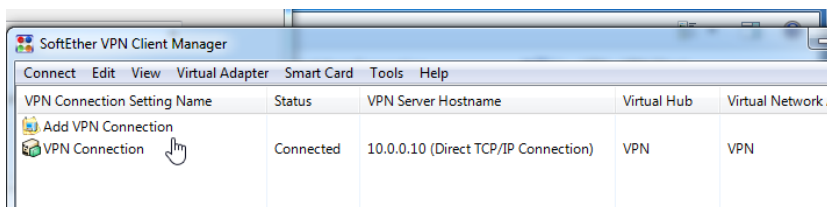


Figure 73 – VPN client manager (Connected).

The VPN server Remote Desktop protocol was previously configured to only accept connections from the 10.0.0.0/24 network range using Windows Firewall, to test the VPN functionality which was successful.

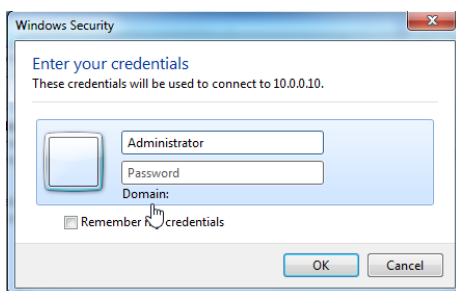


Figure 74 – Remote desktop connection.

8.3 Appendix C - Configuring Microsoft L2TP VPN Client

The next part of the process, was to test the functionality and feasibility of using the in-built Windows VPN client by using the “Set up a new connection or network” wizard.

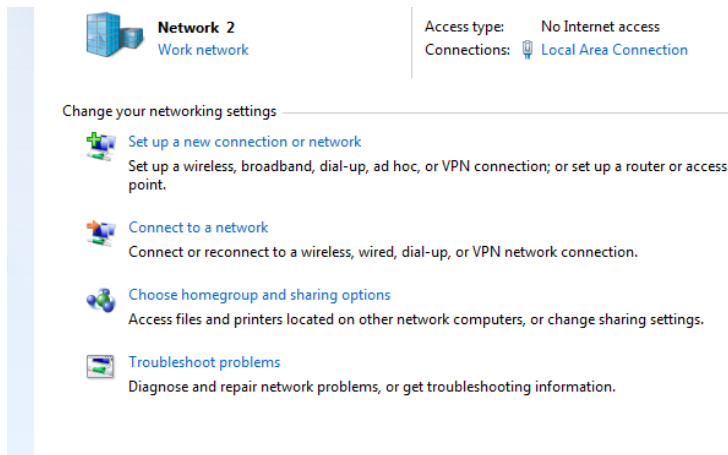


Figure 75 – Windows network connection manager.

After opening the network connection wizard, the next step was to connect to a workplace as shown below.

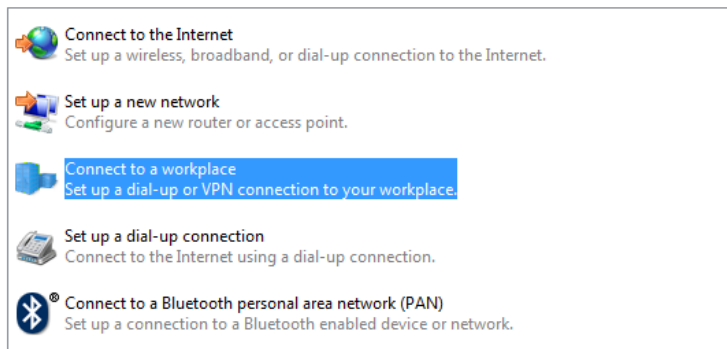


Figure 76 – Windows connection setup.

As the connection is to a VPN server, the first option was selected to connect through an internet connection using a VPN.

How do you want to connect?

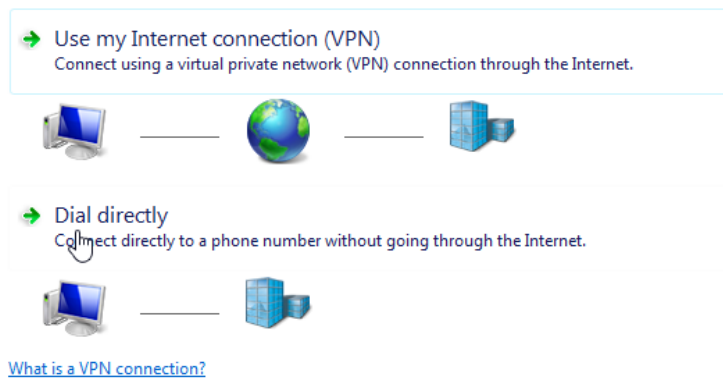


Figure 77 – Windows VPN connection setup.

The VPN server IP address and server name was entered into the setup wizard.

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Figure 78 – Windows VPN connection configuration (Server information).

The username and password was entered into the VPN configuration window, as there is not a Windows domain configured, this was left blank.

Type your user name and password

User name:

Password:

☐ Show characters

☒ Remember this password

Domain (optional):

Figure 79 – Windows VPN connection configuration (Authentication).

After configuring the VPN settings, the connection was ready to be established as shown below.

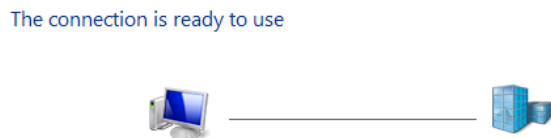


Figure 80 – VPN connection setup (Success).

The next step was to configure the VPN to connect using the L2TP protocol by clicking the properties option.

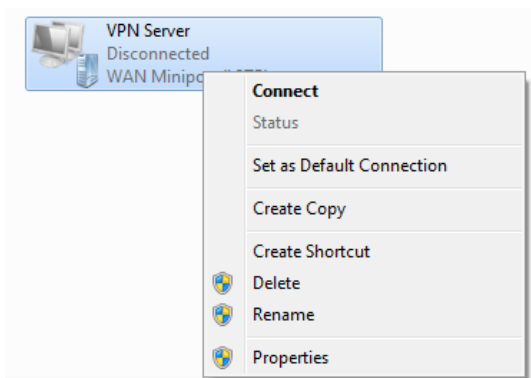


Figure 81 – VPN connection.

By clicking on the “Security” tab, the type of VPN was then changed to L2TP. This ensures the VPN uses the correct protocol for the server. After setting the protocol, “Advanced Settings” was selected.

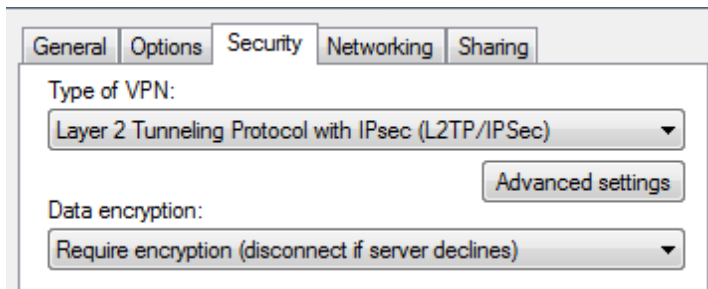


Figure 82 – L2TP security settings.

During the configuration of the VPN server, a pre-shared IPsec key was generated which clients must use for authentication, the key was entered as shown below.

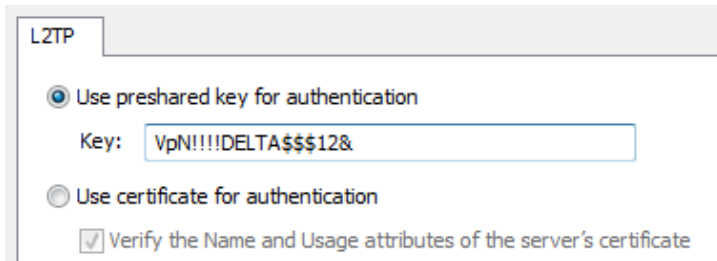


Figure 83 – L2TP IPsec PSK settings.

After configuring the VPN client, the next step was to connect to the VPN using the Windows client.



Figure 84 – Windows VPN connection window.

The VPN connection was successfully established and connected without issue, as shown in the figure displayed below.

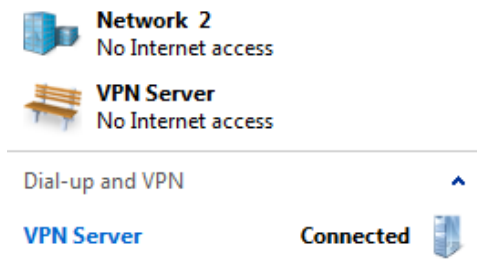


Figure 85 – VPN connection status.

8.4 Appendix D – Installing & Configuring Microsoft VPN Server

The first step of installing Windows Remote Access server was to open “Server Manager” and then click the option for “Add roles and features”.

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

Figure 86 – Server manager roles configuration.

After the “Add Roles and Features” wizard appears, the next step was to click next.

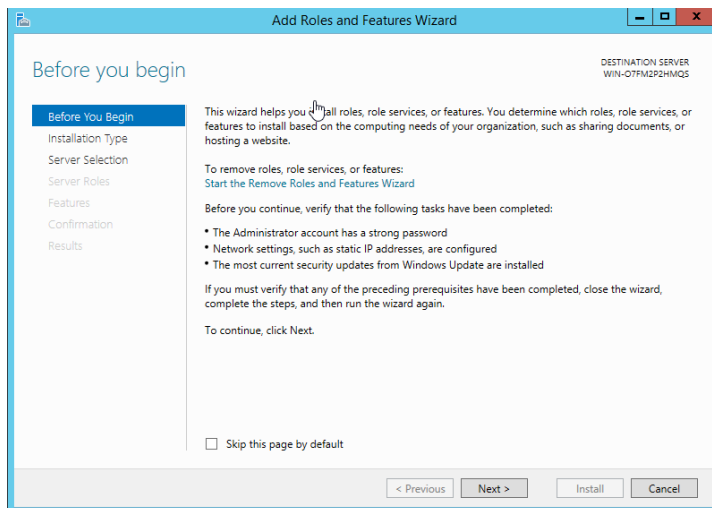


Figure 87 – Add/remove roles wizard.

The next step was to select the “Role-based or feature-based installation” option and then click next.

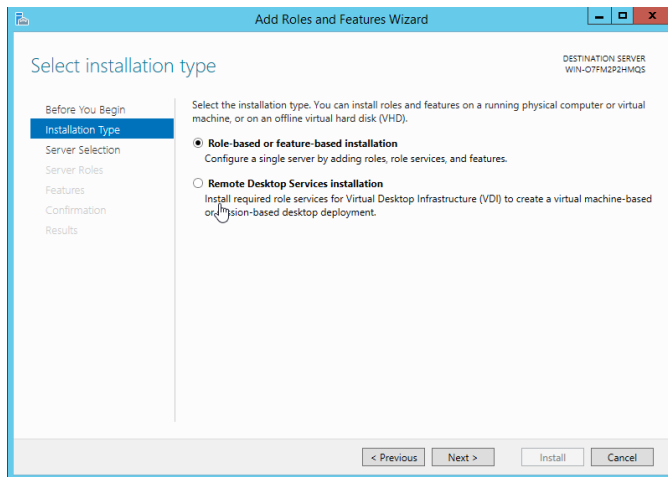


Figure 88 – Add/remove roles wizard (Installation type).

The next part of the installation process was to press “Next” and continue the installation.

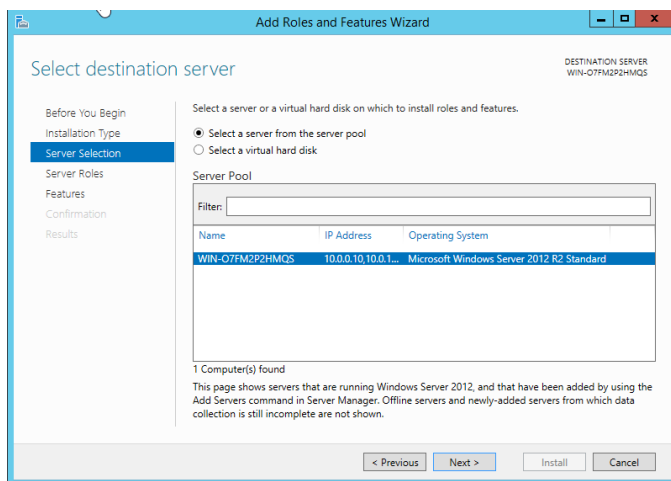


Figure 89 – Add/remove roles wizard (Destination selection).

During this part of the setup process, “Remote Access” was selected from the roles list.

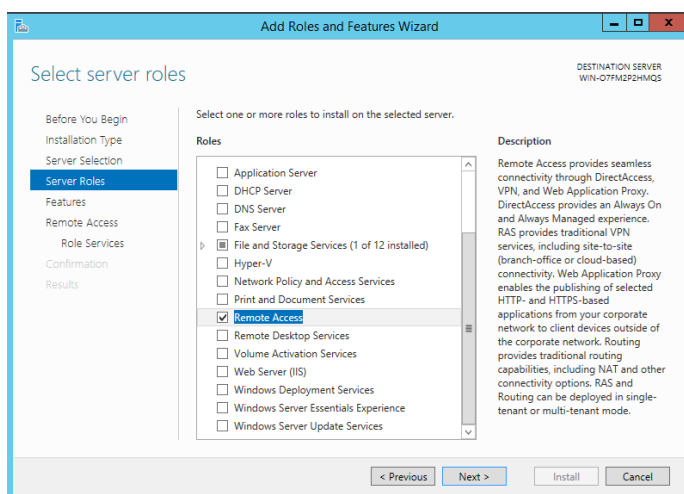


Figure 90 – Add/remove roles wizard (Server roles).

For this step the next option was selected to continue with the installation process.

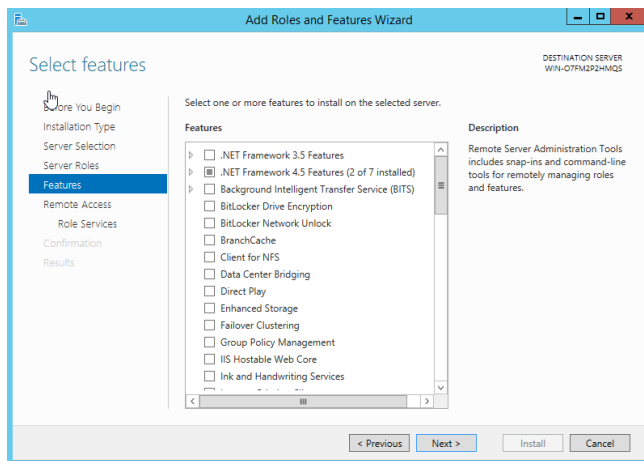


Figure 91 – Add/remove roles wizard (Features selection).

The next part of the installation process was to press next to continue with the setup.

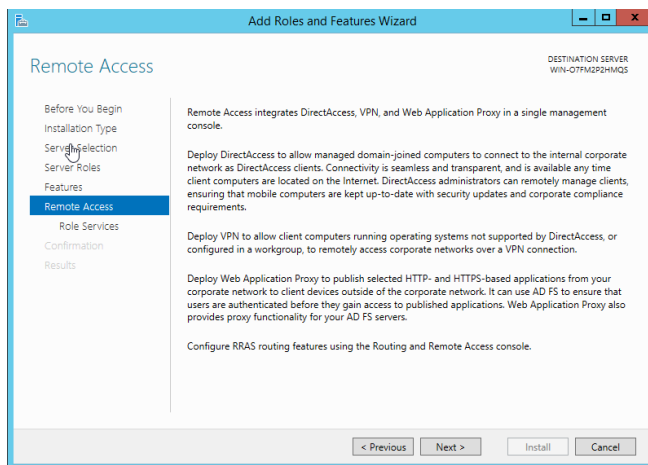


Figure 92 – Add/remove roles wizard (Remote access).

“Add Features” was pressed for this part of the installation which confirms the installation of the required extra features to the server.

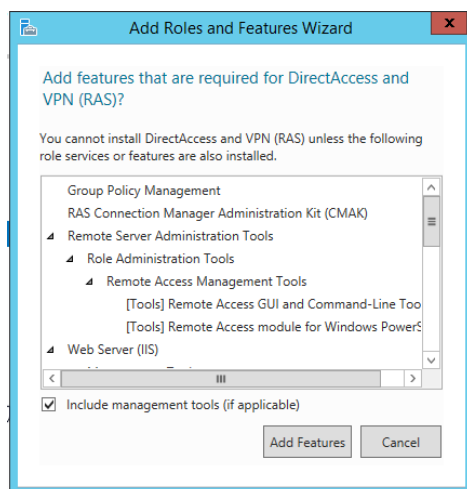


Figure 93 – Add/remove roles wizard (Required roles/features prompt).

The next step was to press next again after reviewing the IIS Role information as shown below.

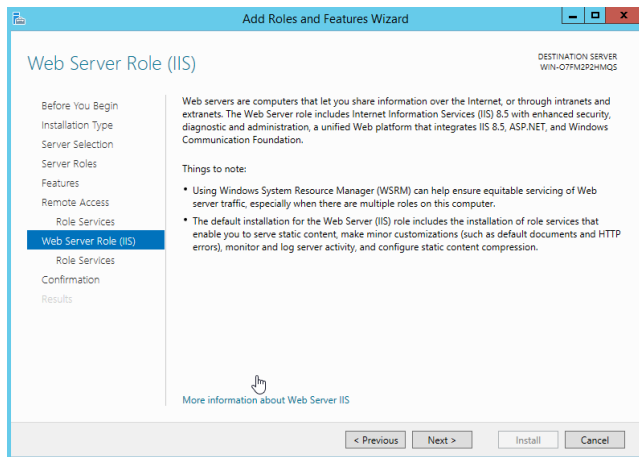


Figure 94 – Add/remove roles wizard (IIS Roles).

As the server automatically selected the required IIS roles, no changes needed to made. The next option was selected to continue the setup process.

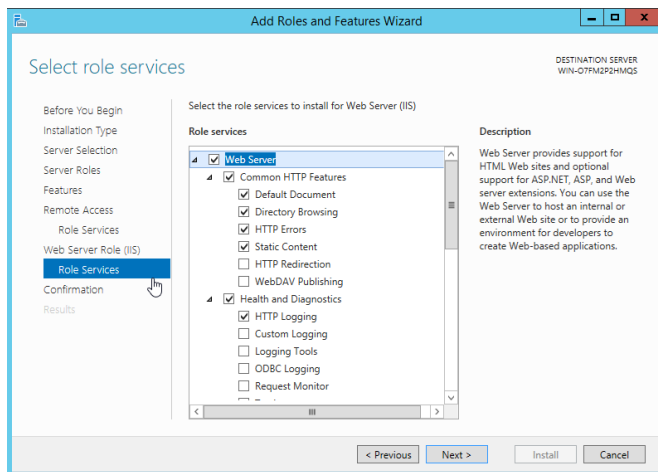


Figure 95 – Add/remove roles wizard (IIS role services).

The “Install” option was selected which installs the previous selections of roles and features.

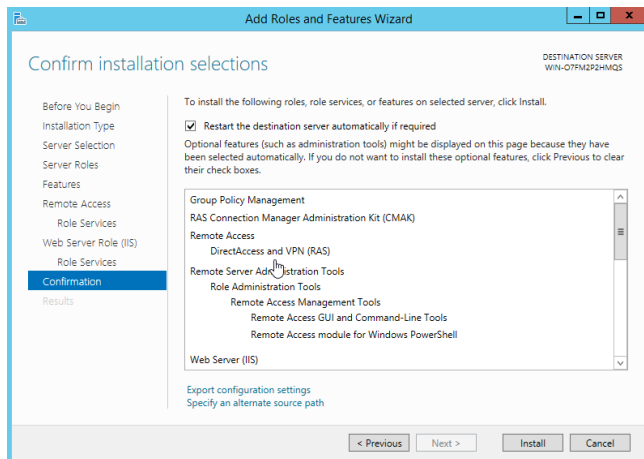


Figure 96 – Add/remove roles wizard (Confirm selections).

After the installation process, has finished, the window can be closed and another setup window should appear to configure Remote Access.

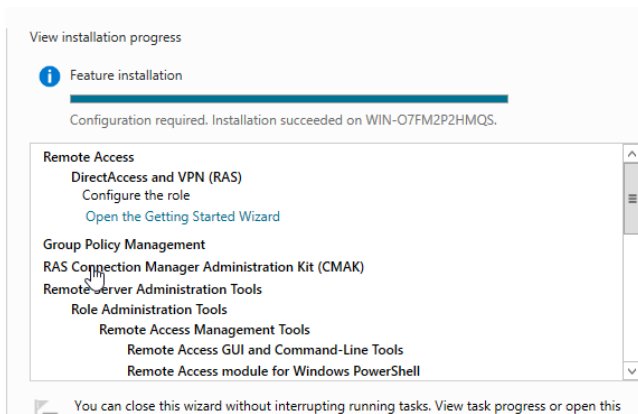


Figure 97 – Add/remove roles wizard (Installation completion).

For the next part of the configuration process “Deploy VPN only” was selected, as only VPN functionality is being compared and trailed at this point.

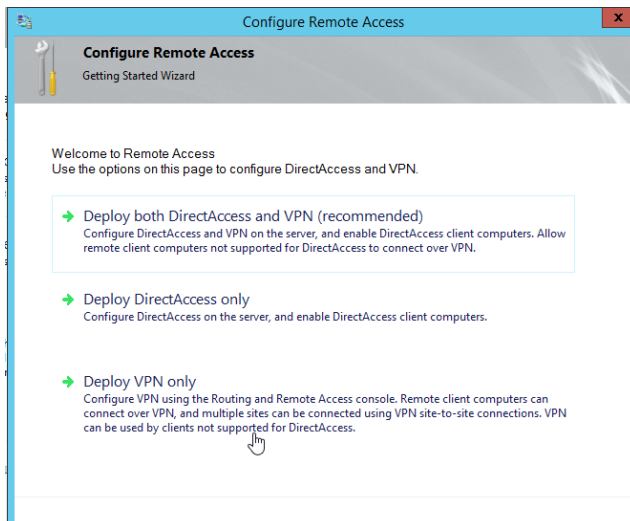


Figure 98 – Remote access configuration.

Once the VPN Only option was selected, the next step was to configure and enable Routing and Remote Access.

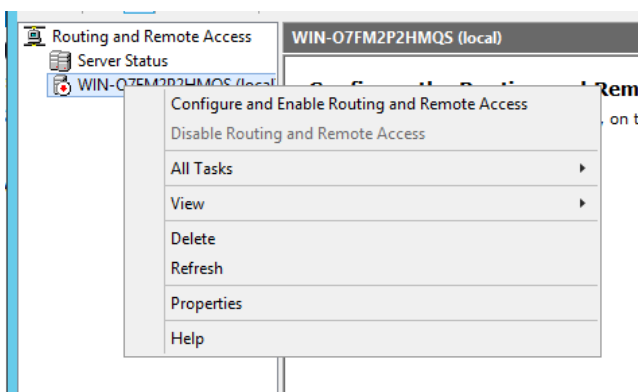


Figure 99 – Remote access management console.

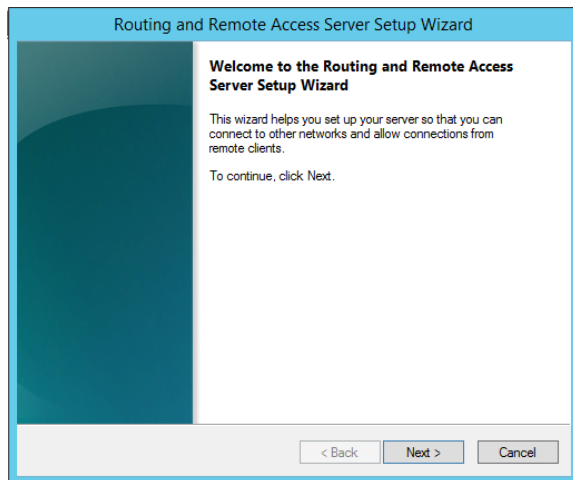


Figure 100 – Routing and remote access setup wizard.

The next step would be to select “VPN” so that the connections are allowed to the server.

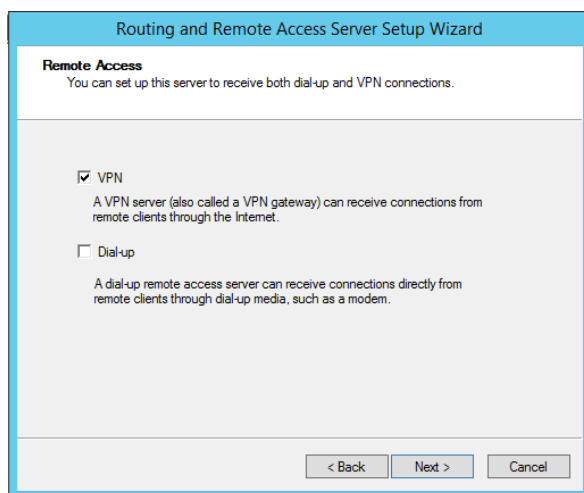


Figure 101 Routing and remote access setup wizard (Connection selection).

The main interface needs to be selected which for this case was “Ethernet 0 2” and then “Enable security on the selected interface by setting up static packet filters”.

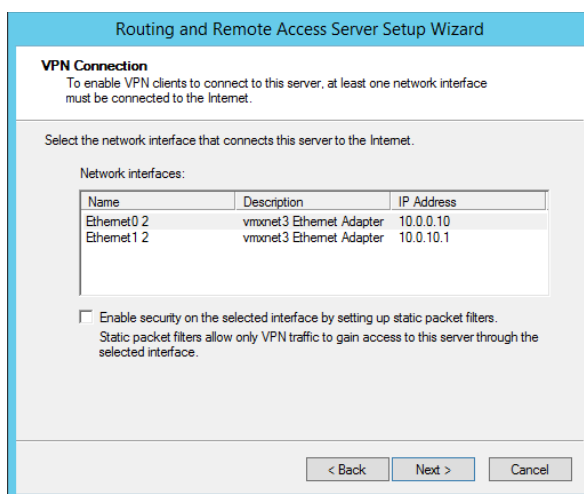


Figure 102 – Routing and remote access setup wizard (Network interfaces).

The next step was to select “Add” and then the following IPv4 Address Range.

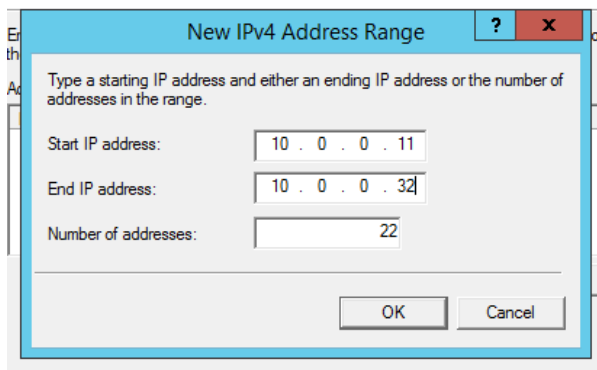


Figure 103 – Routing and remote access setup wizard (IP range selection).

As RADIUS is not used within a small test environment setup, the default setting of “No” was selected.

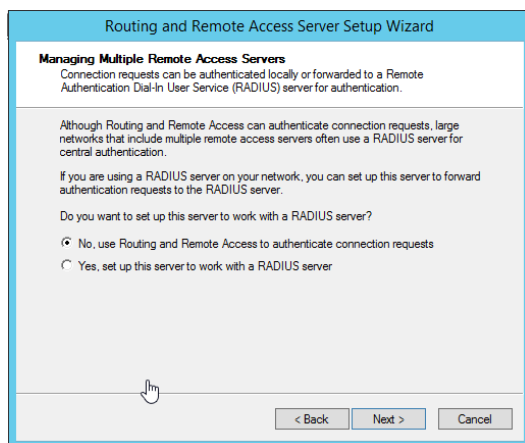


Figure 104 – Routing and remote access setup wizard (Authentication selection).

The next step was to verify the configuration summary and then press next.

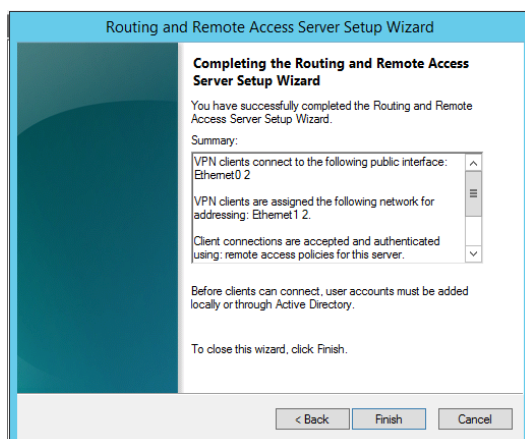


Figure 105 – Routing and remote access setup wizard (Setup summary).

As static IP addressing by the VPN server was configured, this message was ignored and then the next button selected.

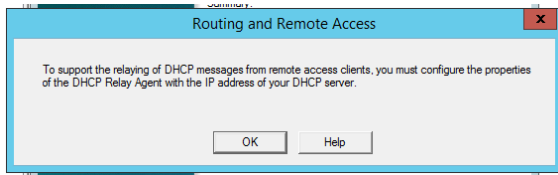


Figure 106 – Routing and remote access setup wizard (DHCP relay warning).

The next step was to right click the “WIN-O7FM2P2HMQS (local)” and then select “Properties”.

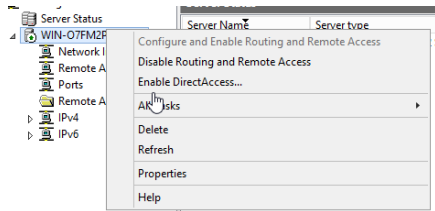


Figure 107 – Routing and remote access management.

After opening the VPN server properties window, the next step was to click the “Security” tab and then check the “Allow custom IPsec policy for L2TP/IKEv2 connection” and entering the pre-shared key which will then be entered onto the client device and then pressing “OK” on the next window as shown below.

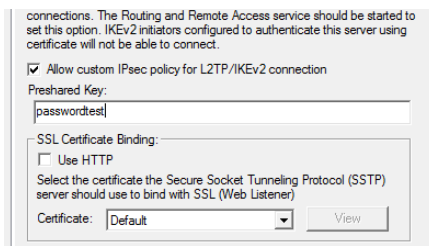


Figure 108 – Routing and remote access (Security settings).

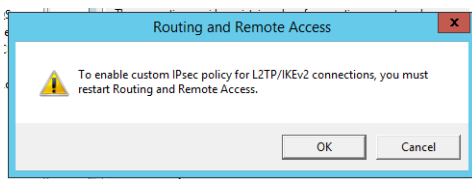


Figure 109 – Routing and remote access (IPSec warning).

After configuring L2TP/IKEv2, the next step was to right click the VPN server and then go to “All Tasks” and “Restart” which enables IPsec functionality.

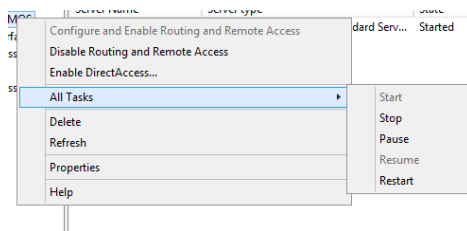


Figure 110 – Routing and remote access (Restart task).

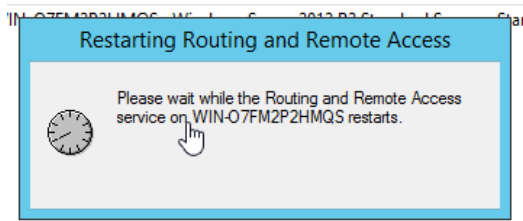


Figure 111 – Routing and remote access (Service restart).

After configuring the VPN server, the firewall ports needed to be opened by searching for and opening “Windows Advanced Firewall Management” and clicking “Inbound Rules” and enabling all Routing and Remote Access firewall rules, as shown in the below figures.

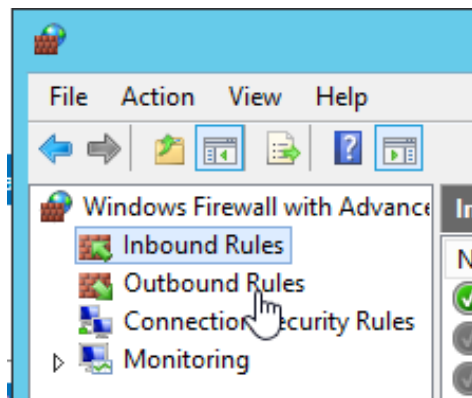


Figure 112 – Advanced windows firewall management.



Figure 113 – Advanced windows firewall management (Rules).

The next step was to right click on “Remote Access Policies and Logging” and then “Launch NPS.”

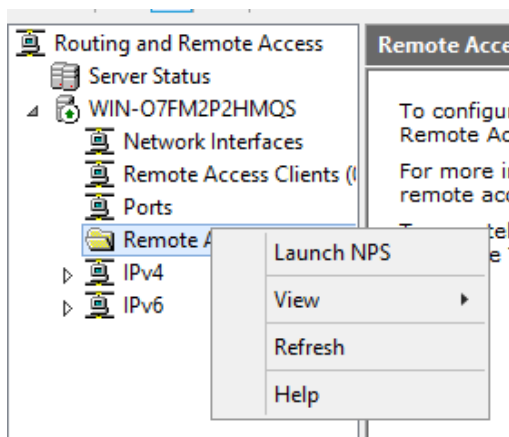


Figure 114 – Routing and remote access (Network policy server).

After launching NPS, the next step was to modify the NPS policy for “Connections to Microsoft Routing and Remote Access server”.

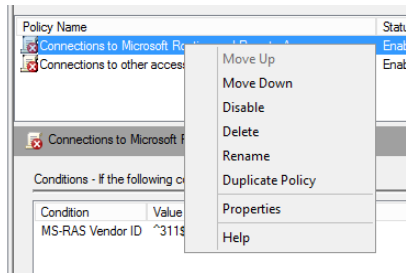


Figure 115 – Network policy server (Policies).

Once the policy was opened the next step was to change the access permission to “Grant access” which enables remote VPN connections to the server.

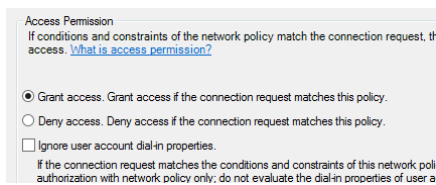


Figure 116 – Network policy server (Remote access policy).

8.5 Appendix E – GNS3 Configuration

The VPN freeware solution was tested in a virtual environment using a client and a server on two different networks and separated by a Cisco C7200 virtual router to ensure correct VPN functionality. The network diagram is shown below.

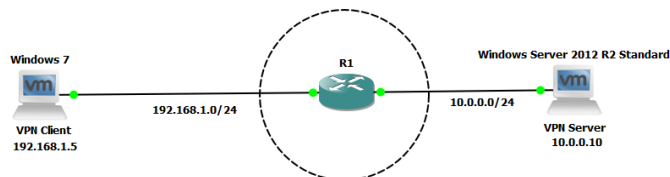


Figure 117 – GNS3 topology diagram.

The following Cisco commands were executed on R1 to enable the two networks (10.0.0.0/24 and 192.168.1.0/24) to communicate and to establish networking on the testing environment.

```
R1(config)#int gigabit1/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Figure 118 – Router 1 interface 1/0 configuration.

```
R1(config)#int gigabit0/0
R1(config-if)#ip add 10.0.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Figure 119 – Router 1 interface 0/0 configuration.