Thesis
Implementation of secure network solutions for Project Area

By: Dennis Elgström | dem09001
School of Innovation, Design and Engineering
Mälardalen University Västerås

Supervisor, Ventyx – ABB: Peter Dahlberg
Technical advisor, Ventyx – ABB: Anders Berggren
Advisor, Mälardalen University: Stefan Löfgren
Examiner, Mälardalen University: Mats Björkman

Abstract

Ventyx in Västerås has a project area where ongoing projects for customers are located; however the network for the project area is somewhat insecure. Customers often come with a higher security standard regarding the project area network which leads to temporary solutions to meet their security requirements.

The purpose of this thesis is, amongst other, to implement a better security standard with the help of authentication, authorization and accounting from a RADIUS server, and the VPN session established between the customers’ and Ventyx networks.
Acknowledgements

I would like to thank all of my colleagues at Ventyx; Big thanks to Peter Dahlberg for accepting and giving me the opportunity to do my thesis at Ventyx, and Anders Berggren for the technical advice and pushing me in the right directions. I would also like to express my gratitude to Pirkko, Arne and Henry at the office for being supportive throughout the thesis process and giving me advice and support when I needed it the most.

I would like to thank my advisor at Mälardalen University, Stefan Löfgren for the help and the network equipment you provided.

Finally, I want to thank my family for their support and unconditional love.
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>ABB</td>
<td>Asea Brown Boveri</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>ASA</td>
<td>Adaptive Security Appliances</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application-Specific Integrated Circuit</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>GNS3</td>
<td>Graphical Network Simulator</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>ISO</td>
<td>Internetwork Operating System</td>
</tr>
<tr>
<td>ISR</td>
<td>Integrated Service Router</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NPE</td>
<td>Network Processing Engine</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PIX</td>
<td>Private Internet Exchange</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Services</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Server</td>
</tr>
<tr>
<td>RTS</td>
<td>Request To Send</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual PC Simulator</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Routing and Forwarding</td>
</tr>
</tbody>
</table>
Contents

1 Introduction ................................................................. 6
  1.1 Background.................................................................... 6
  1.2 Purpose........................................................................... 7
  1.3 Problem formulation .................................................. 7
  1.4 Requirements ............................................................. 8
2 Theory ........................................................................... 9
  2.1 Virtualization .............................................................. 9
    2.1.1 GNS3...................................................................... 10
    2.1.2 VPC....................................................................... 11
  2.2 Security ....................................................................... 12
    2.2.1 VRF....................................................................... 12
    2.2.2 Firewall ................................................................... 13
    2.2.3 VPN ....................................................................... 15
    2.2.4 RADIUS ............................................................... 16
3 Method ........................................................................... 19
  3.1 Network Topology ......................................................... 20
  3.2 Configuration ............................................................... 21
    3.2.1 Project Area Network ........................................... 21
    3.2.2 Office Network ..................................................... 27
    3.2.3 Customer Network ................................................ 27
4 Results ........................................................................... 28
  4.1 Requirements ............................................................... 28
  4.2 Future work ................................................................. 29
5 Conclusion ...................................................................... 30
6 Bibliography .................................................................... 31
7. Appendix A .................................................................... 35
   Pre-study ........................................................................ 35
   7.1 Introduction ............................................................... 37
     7.1.1 Purpose ............................................................... 37
     7.1.2 Background ........................................................ 37
     7.1.3 Problems and Needs ............................................ 37
     7.1.4 Solution proposal ................................................ 38
   7.2 Analysis ..................................................................... 39
     7.2.1 VPN ................................................................... 39
   7.3 Bibliography ............................................................... 41
8. Appendix B .................................................................... 42
   Project Formulation ........................................................ 42
9. Appendix C .................................................................... 44
   Guide: How-to RADIUS server ...................................... 44
   9.1 Cisco Configuration ................................................... 45
   9.2 Windows Server 2008 NPS ........................................... 46
Chapter 1

Introduction

Following thesis was conducted at Ventyx, an ABB company, as part to complete a Bachelors Degree in Network Engineering at Mälardalen University. This introduction chapter will describe, amongst other, the background and purpose of the thesis.

1.1 Background

"Ventyx, an ABB company, is the world’s leading supplier of enterprise software and services for asset intensive industries – such as energy, mining, public infrastructure and transportation – that help keep our world running."[1]

This thesis took place at Ventyx office in Västerås, an office with approximately 160 employees.¹ The thesis has been ongoing during a ten week period with the supervision and guidance from Peter Dahlberg and Anders Berggren.

Ventyx internal network is divided in two sub networks, an office network and a network for the project area. Pre-thesis it was relative poor security between the two networks; with some knowledge all employees could access the project area network and vice versa. How to make it secure but still let chosen employees access the project area network from the office network, is one of many questions that has to be answered.

When a customer chooses Ventyx as partner, a project is started in the project area network. A VPN tunnel is established from the project area network to the customers’ network, that way the customer can monitor the project process without having personnel on site at Ventyx Västerås office, and the Ventyx personnel can access and manage devices located at the customer. By letting the customer have access to the project area network some kind of authentication would be useful, if there is a rogue user on the customers network authentication would stop, or at least give the attacker and additional obstacle, to interfere with Ventyx network.

¹ Peter Dahlberg, 2013-04-12
1.1 BACKGROUND

As previously mentioned people on the project area network can access the office network; meaning customers, or rogue users, can access the office network. This is a security issue that has to be solved.

Upon completion of thesis the expected end result is to enhance the security between the two internal networks and for external users connecting to the project area network, by authentication and putting them under appropriate restrictions.

1.2 Purpose

The purpose of this thesis is to secure the network communication between the office and project area network, only authorized users are allowed in to the project area network from the office network. The network communication between Ventyx project area network and the customers' network needs to be secured as well; this should be done by an automated VPN session between the two locations. Come up with a solution to automatically establish a VPN session between Ventyx project area network and the customers' network. Customers accessing the project area should be authenticated and put under appropriate restriction.

1.3 Problem formulation

![Network Diagram](image)

Figure 1.1: Network topology pre-thesis

As of pre-thesis, the left hand side edge router (Illustrated in Figure 1.1) uses WebVPN, Network Address Translation (NAT) and Virtual Routing
1.3 PROBLEM FORMULATION  

and Forwarding (VRF) Lite for security. All projects are separated in to VRFs with no possibility to reach each other (no routing between the VRFs). Looking at the NAT configuration, the office network is set to outside and project area to inside; different key components from each project have static NATs to allow access from the office network. With the help of WebVPN it is possible to connect to the desired component in the project area network by pointing towards its static NAT address. Meaning, all employees on the office network can connect to that desired component if they know the translated IP, since there are neither authentication nor authorization of the users connecting - which is a problem.

Looking on the right hand side edge router, a VRF-aware IPsec tunnel is setup to the customer allowing them access to the VRF where their project is ongoing. Customers connected to a device on the project area network can access the office network if that device is accessible from the office by static NAT; this is of course a big security flaw. You should not be able to reach anything outside the project area network if you are not authorized for that.

1.4 Requirements

Requirements that have to be met are as follow:

1. Only authorized employees are allowed to access the project area network from the office network.
2. Authenticate and restrict customers when connecting to their corresponding VRF in the project area network.
3. Users from the project area should not be able to reach the office network or any other project located in the project area.
4. RADIUS server should authenticate employees from their current Active Directory (AD) with the help of certificate (if possible) when connecting to project area from office network.
5. An EasyVPN tunnel should be automatically established from the customer to their corresponding VRF when connecting the pre-configured ASA to their internal network.
Chapter 2

Theory

If unfamiliar with the different techniques or technologies used in this project it can be cumbersome to exactly understand why some choices were made. This chapter will give a brief theoretical background on the different techniques and technologies.

2.1 Virtualization

"Virtualization is a term that refers to the various techniques, methods or approaches of creating a virtual (rather than actual) version of something, such as hardware platform, operating system or network resources."[2]

When all hardware necessary is not available, or you simply want to try out a new technology, virtualization can be the best solution. With the help of your existing hardware, and correct software, it is possible to virtualize the wished hardware that is missing; a computer, router or other equipment.

In the beginning of this thesis all hardware needed, to complete the project, was not available. As a solution to this the network simulator GNS3 was used to create a virtual test environment of the desired network. With the help of Virtual PC Simulator (VPC); computers were simulated that were used to check availability of the network. You can find more in-depth information about GNS3 and VPC in section 2.1.1 GNS3 and 2.1.2 VPN.

Although virtualization is good, it has its flaws; if the server that is hosting the virtual machines crashes, all the virtual machines will of course crash as well. This can be solved by having one or more redundant servers with fail-over, but it can be an expensive solution. Another flaw is that it is not possible to virtualize everything; GNS3 cannot virtualize Cisco Catalyst switches due to the impossibility to emulate ASIC processors that are used in those devices, and the available EtherSwitch card has very limited features [6].
2.1 VIRTUALIZATION

2.1.1 GNS3

Graphical Network Simulator (GNS3) is an open source, graphic front-end that is used to emulate network equipment. It works great together with other emulation programs, especially Qemu, Pemu and VirtualBox. These programs are used to emulate Cisco ASA and PIX firewalls, Cisco IPS, Juniper routers and hosts/servers. Qemu, Pemu and VirtualBox are all part of the GNS3 emulation suit, together it is possible to simulate complex virtual networks with routers, hosts, server and more. [5] The possibilities feel endless. Figure 2.1 shows and example of the graphical user interface of GNS3.

Example; with the help of a server that is emulated from VirtualBox, network equipment from GNS3 and a firewall from Pemu it is possible, with appropriate configuration, to simulate a complete network solution of an office, with an AD and some users.

GNS3 offers a wide range of network equipment and tools for simulating different scenarios, as previously mentioned, but GNS3 is used above all to emulate chosen number of Cisco routers.

The software used to emulate a Cisco IOS is called Dynamips. The purpose of Dynamips is to provide a training platform that uses real world software, allowing configuring and experimenting with different Cisco IOS features, making it easier to become familiar with Cisco devices. Note that the emulator cannot replace a real router since the available performance is about 1000 packets per second, compared to the 100 000 packets per second delivered by a NPE-100 (the oldest NPE model). [10] Unfortunately Dynamips is no longer officially maintained, but there are some contributors that maintain an unofficial version of Dynamips called dynamips-community [11]. An important note when using Dynamips is to let GNS3 calculate an Idle-PC value, otherwise Dynamips will use 100% CPU all the time.

Something that is important to distinguish is that GNS3 is emulating routers and not simulating them; meaning the routers is using real Cisco IOS with all its commands - unlike a simulator like Packet Tracer that has a very limited range of command. An important note is that GNS3 cannot emulate Cisco Catalyst switches since it is, according to the creators of GNS3, impossible to emulate the ASIC processors that are used in the Catalyst switches [3]. But it is still possible to configure normal switching features with the help of an EtherSwitch card in a router, or if that is not enough it is possible to connect a physical Catalyst switch to the virtual network [6].
2.1.2 VPC

The Virtual PC Simulator (VPC) is a freeware that can be used in both Windows and Linux. As the name reveals VPC it is a program that simulates up to nine PCs with limited functionality. The VPC can only perform a few network commands, such as ping and traceroute, but if there is no need for more functionality from a host then VPC is ideal; very low memory and CPU usage, while allowing availability checks in the network with ping and traceroute. [4] Only one PC can be used at the time from a console window, much like the command line in Windows or a Cisco CLI.

A default startup script runs when starting VPC, loading up the clients with pre-configured IPs and doing a simple test of the connection with various pings. To modify this script with your own IPs and tests can save you a lot of time; otherwise you will have to do this every time you start the program.

---

http://www.gns3.net/screenshots/
2.1.2 VPC

Listing 2.1: VPC startup script

```
# The startup file of VPC
# VPC1: ipv4, static, Project Area - vlan10
# VPC2: ipv4, static, Project Area - vlan20
# VPC3: ipv4, static, Office Network

1 ip 10.100.10.10 10.100.10.1 24
2
3 ip 10.100.20.10 10.100.20.1 24
4
5 ip 172.5.1.10 172.5.1.1 24
6
7 # Test connection
8 # VPC1: ping to gateway (10.100.10.1)
9 # VPC2: ping to gateway (10.100.20.1)
10 # VPC3: ping to gateway (172.5.1.1)
11
12 ping 10.100.10.1
13 1
14 ping 10.100.20.1
15 2
16 ping 172.5.1.1
17 3
18
19
20
21
22
23
```

This script (shown above in Listing 2.1) assigns IP 10.100.10.10 with the
gateway of 10.100.10.1 on the /24 subnet to client one. Client two get
assigned to IP 10.100.20.10, gateway 10.100.20.1 on the /24 subnet. And
client three get assigned with IP 172.5.1.10, gateway 172.5.1.1, on /24
subnet.

After the clients have got assigned to a network, a simple test of the
connection is made by a ping to corresponding gateway.

2.2 Security

2.2.1 VRF

Virtual Routing and Forwarding, often associated with MPLS VPN and
usually used by Service Providers to give services in a MPLS cloud with
several customers. VRF make it possible to create multiple routing tables
on a router, meaning that it doesn’t matter if customers use same internal
IP addresses since they are separated within the different VRFs. In short,
VRF creates a virtual router with its own routing table on a physical router
(illustrated in Figure 2.2); it employs essentially the same concept as
VLANs and trunking, but at layer three. VRF is not only deployed
together with MPLS, it is just that the two components have really good
synergy. In Cisco terminology, implementation of VRF without MPLS is
called VRF Lite. [7][8]
2.2.1 VRF

VRF Lite
In a VRF Lite implementation, each router within the network participates in the virtual routing environment in a peer-based fashion.

VRF Lite is the simplest form of VRF; it is relatively easy to implement, suited for small to medium businesses and data centers, but does not scale good enough to be used by global corporation due to the need to implement every single VRF instance on all of the affected routers. As previously mentioned, VRF Lite is the usage of VRF without MPLS. [9]

In this thesis, VRF Lite is used to separate the different customers’ sub-networks in the Project Area Network. The different VRFs get accessible from the Ventyx office network with help of NAT, and customers get a VRF-aware EasyVPN tunnel over TCP to their corresponding VRF.

![Illustration of a router with two VRPs, using same physical interfaces](image)

Figure 2.2: Illustration of a router with two VRPs, using same physical interfaces\(^3\)

2.2.2 Firewall

A firewall is a security system for the network with the main task of controlling incoming and outgoing traffic and determines if the traffic should be allowed to pass through or not. A firewall helps to set up a barrier between a trusted, secure network (e.g., your internal network) and a network seen as not trusted and/or insecure (e.g., the internet).

Just as anything else here in life, the firewall comes in many different shapes and sizes. There are software- and hardware-based firewalls, routers with firewall components and firewalls with routing functions. During the process of this thesis, two hardware-based firewalls were used - both manufactured by Cisco, Cisco ASA5505 and Cisco ASA5510.

“Hardware-based firewalls protect all the computers on your network. A hardware-based firewall is easier to maintain and administer than individual software firewalls.” [12]

---

\(^3\) [http://www.cisco.com/..../products_configuration_example.shtml](http://www.cisco.com/..../products_configuration_example.shtml)
2.2.2 FIREWALL

The main focus of the firewall in this thesis was not to analyze data packets and determine whether or not they should be allowed through, the main focus was having the firewall act as an EasyVPN client.

2.2.2.1 ASA
Adaptive Security Appliance (ASA) was introduced by Cisco in 2005; it combines the functionality of its precursor Cisco PIX, VPN 3000 series and IPS product line. [13]

As previously mentioned, hardware-based Cisco ASA 5505 and 5510 firewalls were used during this thesis. For starters the ASA 5510 were used, but there was an obvious issue with it – it could not be configured as an EasyVPN client, only EasyVPN server is possible. Due to this fact ASA 5505 was used instead since it has capabilities for both EasyVPN client and server. Figure 2.3 shows the front and backside of a Cisco ASA 5505.

The ASA 5505 was configured to automatically establish a VRF-aware EasyVPN tunnel over TCP from the customers' network (where the ASA is placed) to a VRF dedicated to the customer inside Ventyx Project Area Network.

Figure 2.3: Front- and backside of a Cisco ASA 5505

---

2.2.2.2 NAT
With the help of Network Address Translation it is, amongst other, possible to have several components to share one public IP address. This NAT technique is called PAT (Public Address Translation), and is probably the most well-known type of NAT due to the fact that almost everyone uses this technique in their home networks to be able to connect several PCs to the internet. This is possible due to use of port addresses that is used to separate and make all components unique even though they use the same public IP address.

The type of NAT that has been used in this thesis is Static NAT - which is often also called one-to-one NAT [14]. The purpose of Static NAT is to assign a specific public IP address to a specific internal IP address; this is useful for devices that you want to be able to reach from the outside of the internal network, example servers. This technique is not very common in smaller networks and is often found within large corporation complex network.

Dynamic NAT is another NAT technique and just like static NAT is also most common in larger complex networks. Dynamic NAT is very similar to static NAT, but instead of the one-to-one mapping of IP addresses static NAT provides dynamic NAT use a group of available public IP addresses [15].

2.2.3 VPN
With the help of a Virtual Private Network it is possible to extend a private internal network across a public network, such as the internet. This feature is particularly useful for business with offices in different geographical locations, traveling employees that need access to files or computers on the business's network. Or as in the case of this thesis, setting up a secure link between devices placed in the customers' network and Ventyx Project Area Network, thus allowing secure communication between to both locations. If by any means someone would intercept the traffic while traveling from one location to another, packet encryption ensures that no sensitive data will be visible. [16]

"A VPN's purpose is providing a secure and reliable private connection between computer networks over an existing public network, typically the Internet." [17]
2.2.3 VPN

A well-designed VPN should provide several improvements to the business network, such as:

- Improved security – with the help of encryption to make sure that the eventual attacker only would see encrypted data. Hashes are used to make sure that no packets are tampered with along the way from point A to B, giving message integrity. [18]
- Scalability – as previously mentioned VPN services helps to handle the growth of a business by securely interconnecting the two, or more, sites internal networks. This will also increase productivity for remote users.
- Reliability – giving employees and remote offices the freedom to connect to the network without any problems at any time, unless specified otherwise.

Important to note is that there are different types of VPNs – IPsec, SSL, PPTP and more. The VPN type that has been used in this thesis is IPsec.

2.2.3.1 IPsec

IPsec is a protocol suite that provides security features at the network layer (Layer 3) of the OSI model. Saying it is a protocol suite means that it is a framework of different protocols for encryption and authentication, customizable to suit the users' needs. IPsec is mostly used for network-to-network deployments, rather than remote-access.

A few features worth highlighting with IPsec VPN are the fact that it is security at the network layer. This means that no modification of TCP/IP applications is required to secure them, unlike SSL VPN. It is very versatile due to the various security mechanisms available such as data authentication, encryption, integrity check and replay protection. Most operating systems have support for IPsec since it is an industry-recognized IETF-standard; this improves the scalability since it can be implemented on almost any device and is usable over any IP-capable network. [19]

However there are some disadvantages as well; the devices with the task to encrypt, decrypt and authenticate traffic may experience heavy CPU load which may hurt the performance. The vast configuration options don’t only provide great flexibility, but also making it very complex.
2.2.4 RADIUS

RADIUS is a networking protocol intended to help with security, it provides a centralized solution for Authentication, Authorization and Accounting (AAA) management for computers and users throughout the network.

When a user or computer wants to access a certain network resource they send a request with its user credentials to a Remote Access Server (RAS). A Remote Access Server is a device that routes the RADIUS packets towards the RADIUS Server; in this thesis the RAS was a Cisco 3725 router. Upon receiving the message containing access credentials, typically in form of a username and password or a certificate, the RAS sends a RADIUS Access Request message to the RADIUS server requesting authorization to grant access via the RADIUS protocol [20]. With help from one of the authentication schemes PAP, CHAP or EAP the RADIUS server either responds with an Access Reject, Access Accept or Access Challenge message, allowing, rejecting or demanding more information to determine the fate of the user or computer. This process is illustrated in Figure 2.4.

- **Access Accept** – As it sounds, the user is granted access. Even though the user is allowed to use one network service doesn't mean that he is allowed to use all network services. The RADIUS server will check to see if the user is authorized to use the network service requested.
- **Access Reject** – The user is denied any access to the network service requested.
- **Access Challenge** – RADIUS server requests additional information to make its decision, this additional information can be in form of a secondary password or a PIN.

![Figure 2.4: RADIUS Authentication and Authorization Flow](http://en.wikipedia.org/wiki/File:Drawing_RADIUS_1812.svg)
In addition to one of the three RADIUS responses it may also include a message stating the reason of the eventual rejection, the prompt for the challenge or a welcome message if accepted.

[21] If accepted the RADIUS server can include authorization attributes in the Access Accept-message. Example of authorization attributes are as follows:

- A IP address to be assigned by the user, either a specific address or one to be chosen from a address pool
- Quality of Service parameters
- VLAN parameters
- Maximum length the user may remain connected
Chapter 3

Method

This thesis was divided into following four phases:

1 Pre-study
   During the first week at Ventyx the time was spent making a Pre-study; with help from employees the problems were identified and ideas of how to solve them were presented. Investigations were made to determine if there were other possible solutions, which then were compared to each other to determine the best suited solution. Lost and unknown knowledge about various network techniques and features were renewed by reading about them on the internet and get lectures by employees.

   The pre-study can be found in Appendix A.

2 Network Topology
   Due to lack of available hardware the network was re-created virtually in the network simulator GNS3, it proved to be an arbitrary emergency solution but had a few drawbacks such as limited support for switches as well as a constantly crashing ASA.

3 Configuration
   The configuration itself was divided in to four phases, one for each sub-part of the network. The first phase is to configure the basics of the main focus of this thesis; the Project Area Network. Second, configure the Office Network to establish desired connection between the two networks (Office and Project Area). Third, establish a VRF-aware EasyVPN tunnel over TCP from the Customer Network to allow them to access their project inside the Project Area Network. Last phase - forth, a RADIUS server were configured to authenticate users connecting to the Project Area Network from either the Office or Customer Network.

4 Verification
   To verify that everything is working as intended a series of tests were conducted. Tests that either failed or did not give a satisfied result were complemented till the satisfied result(s) were met. The tests were made in both the virtual GNS3 environment as well as a physical environment with real equipment.
3.1 Network Topology

As previously mentioned – due to lack of available hardware a simplified version of Ventyx network was re-created in the network simulator GNS3. As a result of this, a bit more time than expected had to be spent with basic things such as get a grasp of GNS3, find appropriate GNS3 capable Cisco IOSes and so forth.

The network was created to be a simplified replica of Ventyx internal network. With the help of employees the new virtual network topology was created containing all essential parts of the real network – the office network, project area network and the customers' network, see Figure 3.1. Since the virtual network had to be made from scratch, a new IP table had to be made as well. The IP addresses chosen for the virtual network are not related to the real network, see table 3.1.

![Network Topology Diagram]

Figure 3.1: Network topology shown in GNS3
### 3.1 NETWORK TOPOLOGY

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mask</th>
<th>Connected to</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/0</td>
<td>-</td>
<td>-</td>
<td>SW1 – Port 1</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.10</td>
<td>10.100.1.10</td>
<td>255.255.255.0</td>
<td>SW1 – Port 1</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.20</td>
<td>10.100.2.10</td>
<td>255.255.255.0</td>
<td>SW1 – Port 1</td>
</tr>
<tr>
<td></td>
<td>Fa0/1</td>
<td>192.168.100.1</td>
<td>255.255.255.0</td>
<td>R4 – Fa0/0</td>
</tr>
<tr>
<td>R2</td>
<td>Fa0/0</td>
<td>-</td>
<td>-</td>
<td>SW1 – Port 2</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.10</td>
<td>10.100.1.10</td>
<td>255.255.255.0</td>
<td>SW1 – Port 2</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.20</td>
<td>10.100.2.10</td>
<td>255.255.255.0</td>
<td>SW1 – Port 2</td>
</tr>
<tr>
<td></td>
<td>Fa0/1</td>
<td>192.168.200.1</td>
<td>255.255.255.252</td>
<td>R3 – Fa0/0</td>
</tr>
<tr>
<td>R3</td>
<td>Fa0/0</td>
<td>192.168.200.1</td>
<td>255.255.255.252</td>
<td>R2 – Fa0/1</td>
</tr>
<tr>
<td></td>
<td>Fa0/1</td>
<td>192.168.250.1</td>
<td>255.255.255.0</td>
<td>ASA – e0/0</td>
</tr>
<tr>
<td>R4</td>
<td>Fa0/0</td>
<td>192.168.100.1</td>
<td>255.255.255.0</td>
<td>R1 – Fa0/1</td>
</tr>
<tr>
<td></td>
<td>Fa0/1</td>
<td>172.30.1.1</td>
<td>255.255.255.0</td>
<td>SW2 – Port 1</td>
</tr>
<tr>
<td>ASA5510</td>
<td>E0/0</td>
<td>192.168.250.2</td>
<td>255.255.255.0</td>
<td>R3 – Fa0/1</td>
</tr>
<tr>
<td></td>
<td>E0/1</td>
<td>172.30.1.1</td>
<td>255.255.255.0</td>
<td>Phys. Laptop</td>
</tr>
</tbody>
</table>

Table 3.1: IP Table

### 3.2 Configuration

#### 3.2.1 Project Area Network

The project area network is considered as the inside core network of this thesis. It is divided in several sub-networks with the help of VRFs, simulating different projects. From the project area network a VRF-aware EasyVPN tunnel over TCP allows customers to gain access to their project. Employees from the office network are able to remotely access authorized projects via WebVPN and/or through the VPN tunnel. With the help of a RADIUS server AAA is implemented on both edge routers to only allow authorized personnel.

#### 3.2.1.1 VLAN

The project area network is configured in the 10.100.VLAN.0 /24 network; VLAN meaning the number of the VLAN. To make it as simple as possible only two VLANs are implemented, VLAN 10 and 20, these VLANs are supposed to simulate two projects located in the project area network. A VPC is put in both VLANs, with the IP 10.100.VLAN.10 and a gateway of 10.100.VLAN.1 (on router one, R1), to help verifying availability and configurations.

#### 3.2.1.2 VRF

Each VLAN is put in separate VRFs, VLAN 10 in a VRF named lan10 and VLAN 20 in VRF named lan20. As mentioned in the theory part 2.2.1 VRF, a virtual router is created with its own routing table, to allow access between these virtual routers either static routes or routes from a routing protocol is needed. In this case there is no routing between the VRFs in the project area network; this is a security precaution making it impossible for the VPC to reach each other.
3.2.1 PROJECT AREA NETWORK

3.2.1.3 Static Route
No routing protocols are used within the Ventyx internal networks, only static routes. Static routes are set to allow access between office, project area and ISP. First I saw this as a flaw, and questioned - how could this ever scale well? But when I started configuring I understood that it was a necessity and easier due to the translated addresses from NAT and VRFs. Important to note is that there are three separate routing tables because of the VRFs, when adding a route to two or more routing tables the static route command has to be entered for every routing table you want to apply it to. Following commands are applied to add a static route to the office network (172.5.1.0 /24) from respectively VRF.

<table>
<thead>
<tr>
<th>Listing 3.1: Static routes for VRFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>(config)# ip route vrf lan10 172.5.1.0 255.255.255.0 192.168.100.1 global</td>
</tr>
<tr>
<td>(config)# ip route vrf lan20 172.5.1.0 255.255.255.0 192.168.100.1 global</td>
</tr>
</tbody>
</table>

Initially there were some problems with the routing, TCP RTS packets were spammed and when pinging to the router in question replies were spammed in the hundreds indicating some type of loop. Upon further review of this issue it all came down to simulated hardware in GNS3, the router I was using. Cisco 7200 was not optimized for use in GNS3 and could cause switching loops, which was the problem I had. Instead of using this model I changed to a Cisco 3725 and everything worked just fine.

3.2.1.4 NAT
Due to the requirement (see 1.4 Requirements) to allow authorized employees from the office network to connect to the project area network, NAT is implemented to translate the address(es) of desired component(s) in the project area network; the desired components in this case are the VPCs. With static NAT the VPCs addresses are translated to look like they are part of the link network between the project area edge router R1 and office edge router R4, and thus become available from the office network with the help of static routes. Static NAT is used instead of dynamic due to the need of knowing what IP address a component is translated to.

As the requirement states to allow only authorized employees, this is considered a security flaw; with the current configuration all employees can access the VPCs on the project area network, this will be solved later on with RADIUS AAA.
3.2.1.4 NAT

Listing 3.2: NAT configuration

(config)# ip nat inside source static 10.100.10.10 192.168.100.100 vrf lan10 extendable
(config)# ip nat inside source static 10.100.20.10 192.168.100.200 vrf lan20 extendable

3.2.1.5 VPN

A requirement from Ventyx regarding the VPN solution was to use Ciscos EasyVPN feature. The end goal was the have a VRF-aware EasyVPN tunnel over TCP in NEM-mode to be automatically established between the customers' network and Ventyx Project Area Network. This task proved to be the most difficult and time consuming part of the thesis due to a lot of unexpected errors. Some of the errors include problems with a specific virtualized router model, non-supported operating systems, pings timing out even though the tunnel was up, and having the tunnel crash when using a mix of virtualized and physical hardware. In the end it all came down to a more customized/unique solution rather than a traditional one.

Following are some of the problems I encountered along with their solution.

**Problem** Lack of support on the Cisco ASA 5510; it cannot be configured as an EasyVPN client, only EasyVPN server. This is a problem since the ASA, placed in the customers' network, is going to be configured as EasyVPN client to establish connection with the EasyVPN server located on the edge of the Project Area Network.

**Solution** Since this issue could not be solved with an IOS upgrade the only available solution was to replace the ASA 5510 to a model with support for EasyVPN client. The replacement model is a Cisco ASA 5505 which was used throughout the whole thesis process.

**Problem** When using Ciscos’ Anyconnect from a remote PC trying to connect to the EasyVPN server, the session is established and tunnel goes up but no traffic travels through the tunnel.

**Solution** Trying to ping from the inside of the project area network to the remote PC gave me the output that packets were encapsulated and sent through the tunnel, but they did never return and did not get decapsulated:

```
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

This would indicate that there is a problem with the split-ACL, NAT being incorrect or routes are missing. Making sure that the split-ACL was correct and since no NAT was being used here it quickly narrowed it down to missing routes.
Looking at the statistics in Anyconnect (shown above) on the remote PC show that no packets are encrypted or decrypted, indicating that the problem should be on this device.

Upon reviewing the remote PCs routing table it is proven that no route is added to redirect traffic through the tunnel going towards the project area network. This route should be added automatically when the tunnel is established; making me to believe there might be a compatibility issue between Anyconnect and Windows 8. When testing the same scenario with Windows 7 installed on the remote PC the outcome was different, the missing route was now there and traffic could flow through the tunnel.

**Problem** Tunnel crashed when trying to connect to ASDM through the tunnel, from a PC on the inside of the Project Area Network to the ASA located at the customers' network.

**Solution** As the routers in the Project Area Network are simulated in GNS3 this creates a huge bottleneck, since GNS3 only allows 1000 packets per second to be processed. Upon trying to establish an ASDM session through the virtual router it proved to be too much traffic for GNS3 to handle making the tunnel to crash. Using physical hardware and doing the same test, accessing ASDM through the tunnel, worked without any problem. When watching how many packets per second that actually was needed it proved to be around 5000 packets per second during the first seconds when initializing the ASDM session.
Problem  Tunnel is established between EasyVPN Server (Cisco 3725 Router) and EasyVPN Client (Cisco ASA 5505), the split-ACL attributes are correctly transferred to the ASA, all traffic are encapsulated and decapsulated on both sides but ping times out when trying to reach anything beyond any of the end points.

Solution  This proved to be the most difficult and time consuming issue to solve. Trying to ping while the tunnel is not established worked without any problems. One might think ICMP is not allowed through the tunnel, but allowing it through with the help of an ACL did not do any difference at all. The solution to this became rather unique and maybe more of a workaround since I was not able to fully identify the source of the problem. Instead of using an EasyVPN-only solution, as I had planned, I did a mix of dynamic VRF-aware IPsec and EasyVPN that proved to be a solution/workaround the the problem.

Important to note is that a normal VRF-aware IPsec solution is not possible due to the requirements set by Ventyx.

In a normal EasyVPN-only solution the configuration consist of an isakmp client configuration group, an isakmp profile, an IPsec profile and a virtual-template to bind the tunnel to an interface. Here is an example of a normal EasyVPN-only configuration:

```plaintext
crypto isakmp client configuration group EZVPN-GRP10
    key Vasteras0
    pool EZVPN-POOL
    acl EZVPN-SPLIT-ACL
    netmask 255.255.255.0

crypto isakmp profile CUST10-IKE-PROF
    match identity group EZVPN-GRP10
    client authentication list AUTH-EZVPN
    isakmp authorization list AUTHOR-EZVPN
    client configuration address respond
    client configuration group EZVPN-GRP10

virtual-template 10

crypto IPsec profile CUST10-IPSEC-PROF
    set transform-set EZVPN-TS
    set isakmp-profile CUST10-IKE-PROF

interface Virtual-Template10 type tunnel
    ip vrf forwarding lan10
    ip unnumbered FastEthernet0/1
    tunnel mode IPsec ipv4
    tunnel protection IPsec profile CUST10-IPSEC-PROF
```

As previously mentioned this code did not work as intended and an alternate implementation had to be made.
The mix, and solution to the problem, between dynamic VRF-aware IPsec and EasyVPN consist of an isakmp client configuration group, an isakmp profile, a crypto map placed on the outside interface to help bind the tunnel to an interface, and a dynamic-map. Following is the code used to solve the problem:

crypto isakmp client configuration group EZVPN-GRP10
  key Vasteras0
  acl EZVPN-SPLIT-ACL

! crypto isakmp profile CUST10-IKE-PROF
  vrf lan10
  match identity group EZVPN-GRP10
  client authentication list AUTH-EZVPN
  isakmp authorization list AUTHOR-EZVPN
  client configuration address respond
  client configuration group EZVPN-GRP10

! crypto dynamic-map EZVPN-DMAP 10
  set transform-set EZVPN-TS
  set isakmp-profile CUST10-IKE-PROF

! crypto map EZVPN-CMAP 20 IPsec-isakmp dynamic EZVPN-DMAP

! interface FastEthernet0/1
  crypto map EZVPN-CMAP

You can see the similarities of the two different configurations, and it might seem that this mixed code needs more unique lines of code per VRF than the previous EasyVPN-only code. But the truth is that this mix does only need thirteen lines of unique code per VRF, rather than the eighteen lines needed by the EasyVPN-only configuration.

3.2.1.6 RADIUS Server

With the help from a Dell ESXi server – a RADIUS server is implemented and used for authentication and authorization of VPN sessions coming from the outside, customer network. Each VPN session has a user connected to it on the RADIUS server, allowing access only to their specific VRF in the project area network and from users with a source of the customers’ internal IP. For fun and a better learning experience RADIUS authentication and authorization were also used when logging in to the virtual routers used during the thesis process. To prevent getting locked out from the routers local usernames were also implemented, incase the RADIUS server would go down or lose connection. Listing 3.3 display the commands needed for RADIUS authentication and authorization on the routers.
3.2.1.6 RADIUS SERVER

<table>
<thead>
<tr>
<th>Listing 3.3: RADIUS configuration on Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>(config)# username &lt;username&gt; privilege 15 password &lt;password&gt;</td>
</tr>
<tr>
<td>(config)# aaa new-model</td>
</tr>
<tr>
<td>(config)# aaa authentication login &lt;group name&gt; group radius local</td>
</tr>
<tr>
<td>(config)# aaa authorization exec &lt;group name&gt; group radius local</td>
</tr>
<tr>
<td>(config)# ip radius source-interface &lt;interface&gt;</td>
</tr>
<tr>
<td>(config)# radius-server host &lt;ip address&gt; key &lt;password&gt;</td>
</tr>
</tbody>
</table>

A request made by Ventyx was to have a how-to guide of how to setup a RADIUS server; this guide can be found in Appendix C.

3.2.2 Office Network

The office network has very basic configuration and is only used for testing availability from authorized and unauthorized users to the project area network. Authorized users are employees working on a certain project; they are only allowed to access their project LAN and no other projects LAN. Unauthorized users on the other hand will be denied all access to the project area network.

To start with availability was tested from a VPC, using ping and traceroutes. In a later stage, when RADIUS was implemented, the VPC was changed to a real computer making it possible to test WebVPN and remote desktop.

3.2.3 Customer Network

When a project is started Ventyx sends a pre-configured ASA to the customer automatically establishing a VRF-aware EasyVPN tunnel over TCP to the LAN where their project will develop. In this thesis an imaginary customer is called customer10 is used and, as you can imagine, have their project in VLAN 10 in the project area network.

Due to lack of hardware the first approach was to have everything virtualized in GNS3, including the ASA in the customers’ network in the early stages of the thesis process. Having an ASA virtualized proved to be much more complex than expected. After testing six different IOS versions and all of them crashing when trying to start ASDM or establish an IPsec connection, the approach was changed to use a physical Cisco ASA 5505 which proved to be the better approach.

As mentioned, from the Cisco ASA 5505 a VRF-aware EasyVPN tunnel over TCP was configured pointing towards project area network VLAN 10, customers are now able to monitor their project.
Chapter 4

Results

4.1 Requirements

1. Only authorized employees are allowed to access the project area network from the office network.
   With help from NAT chosen devices in the projects are accessible from the office network. Users trying to connect to a device gets authenticated and authorized against a RADIUS server, only allowing access to authorized employees.

2. Authenticate and restrict customers when connecting to their corresponding VRF in the project area network.
   When the customer connects the preconfigured ASA to their internal network, a VPN tunnel is automatically set up between the customer network and their corresponding VRF in the project area network. This VPN session is authenticated against a RADIUS server, restricting all access to only their VRF.

3. Users from the project area should not be able to reach the office network or any other project located in the project area.
   No routing is enabled between the VRFs, thus limiting users connected to one project from reaching another projects VRF. RADIUS server authenticates users trying to connect to the office network, denying unauthorized users.

4. RADIUS server should authenticate employees from their current AD with the help of certificate (if possible) when connecting to project area from office network.
   This requirement was not met due to not being allowed to touch Ventyx current AD.

5. An EasyVPN tunnel should be automatically established from the customer to their corresponding VRF when connecting the pre-configured ASA to their internal network.
   When the customer connects the pre-configured ASA to their network a VRF-aware EasyVPN tunnel in Network Extension Mode over TCP is established towards Ventyx project area network. The VPN session is authenticated against a RADIUS server giving them access to their corresponding VRF.
4.2 Future work

When a VPN tunnel is established and the ASA is located behind a NAT device, the IP address shown when issuing “show crypto isakmp sa” command will be the IP address of the NAT device and not the IP address of the ASA. If the ASA have a dynamic outside IP address from a DHCP pool it difficult to remotely access the ASA, since you have no idea what IP you should connect to and the Cisco ASA does not allow management sessions to their inside interface. A solution, or maybe I should call it a workaround, to this problem would be to use an ISR (Integrated Service Router) instead of an ASA. The ISR do allow management sessions on the inside interface, the price is about the same and the ISR have the features needed to setup a VRF-aware EasyVPN tunnel in NEM-mode over TCP.

In order to better this project it would be recommended to change from using private shared keys to certificates, this would greatly increase the security of the VPN sessions.
Chapter 6

Conclusion

Corporation networks aren’t always as secure as one can imagine. In some cases the security can be very poor and people with knowledge in networking can gain access rather easily, which can have catastrophic consequences. Luckily, this was not the case with Ventyx network. Their security was neither bad nor good, there were some holes that needed to be shut; which proved to be both resource and time consuming. This has provided me with the insight that even though you have the knowledge of issues or upgrades that needs to be done in a certain matter; it’s not always possible to execute them in the corporate world. Mainly because of the time and resources needed to be invested to solve the requests. In the end, it all comes down to money.

The final product that I left behind upon completion of this thesis was not perfect. There are several ways to improve the solution, probably many more than what I have found. One of the obvious would be to implement certificates for authentication of the VPN sessions rather than using private shared keys. The final product has neither been implemented, to my knowledge, in Ventyx network – if the problem regarding remote management and changing private shared keys to certificates is implemented there are good possibilities that it will be implemented.

The requirements set by Ventyx were met to the extent possible. All requirements beside one, where I were tasked to use Ventyx internal AD and use certificate for authentication of VPN sessions from the Office- to the Project Area Network, were met. This requirement could not be met since I was not given the authority to manage their servers, which is understandable. Although, I did provide Ventyx with a HOW-TO guide to help them solve this request themselves (which can be found in Appendix C), as well as setting it up in my virtual GNS3 environment.

All in all I am very happy to have been given the great opportunity to make this thesis at Ventyx. It has been a very educational and fun way to end my studies at Mälardalen University Västerås, thank you.
Chapter 7

Bibliography

[1] Ventyx.com; Company Overview
   Last accessed: April 10th, 2013

   http://en.wikipedia.org/wiki/Virtualization
   Last accessed: April 17th, 2013

[3] GNS3.net; Hardware emulated by GNS3
   http://www.gns3.net/hardware-emulated/
   Last accessed: April 17th, 2013

[4] Virtual PC Simulator Wiki; Documentation
   Last accessed: April 22nd, 2013

[5] GNS3.net; Home
   http://www.gns3.net/
   Last accessed: April 22nd, 2013

[6] GNS3.net; Switching
   http://www.gns3.net/switching/
   Last accessed: April 22nd, 2013

[7] PacketLife.net; Intro to VRF Lite
   http://packetlife.net/blog/2009/apr/30/intro-vrf-lite/
   Last accessed: April 22nd, 2013

[8] Cisco Dreamer; VRF Basics
   http://ciscodreamer.blogspot.se/2009/06/vrf-basics.html
   Last accessed: April 22nd, 2013

   http://en.wikipedia.org/wiki/Virtual_Routing_and_Forwarding
   Last accessed: April 22nd, 2013
[10] IPflow.utc.fr; Cisco 7200 Simulator
   http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator
   Last accessed: April 24th, 2013

   http://www.gns3.net/dynamips/
   Last accessed: April 24th, 2013

[12] Cisco.com; Software Firewalls vs. Hardware Firewalls
   http://cisco.com/../../../small_business_firewall_software/index.html
   Last accessed: August 3rd, 2013

[13] Wikipedia; Cisco PIX
   https://en.wikipedia.org/wiki/Cisco_PIX#ASA
   Last accessed: August 3rd, 2013

[14] Wikipedia; Network Address Translation
   https://en.wikipedia.org/wiki/Network_address_translation
   Last accessed: August 7th, 2013

   https://en.wikipedia.org/../../../#Dynamic_network_address_translation
   Last accessed: August 7th, 2013

[16] Howstuffworks; How VPNs Work
   http://www.howstuffworks.com/vpn.htm
   Last accessed: August 10th, 2013

[17] Howstuffworks; What Makes a VPN?
   http://computer.howstuffworks.com/vpn2.htm
   Last accessed: August 10th, 2013

   Last accessed: August 10th, 2013

[19] Network Computing; Picking The Right VPN
   http://www.networkcomputing.com/../../../picking-the-right-vpn/
   Last accessed: August 11th, 2013

[20] Wikipedia; RADIUS
   http://en.wikipedia.org/wiki/RADIUS
   Last accessed: August 11th, 2013

[21] Cyberoam; Configure Windows Server 2008 as a RADIUS Server
   http://kb.cyberoam.com/default.asp?id=2407
   Last accessed: August 11th, 2013
[22] GNS3.net; Documentation
   http://www.gns3.net/documentation/
   Last accessed: April 25th, 2013

[23] CBTnuggets.com; Free video about GNS3
   http://www.cbt nuggets.com/..../freevideo/cisco_642_902_02.mp4
   Last accessed: April 25th, 2013

[24] GNS3.net; Adding host to your Topologies
   Last accessed: April 25th, 2013

[25] Howstuffworks; Network Address Translation
   http://www.howstuffworks.com/nat.htm
   Last accessed: April 25th, 2013

[26] Cisco; Match-in-VRF Support for NAT
   http://www.cisco.com/..../iadnat-match-vrf.html
   Last accessed: April 27th, 2013

[27] Youtube; Setting up ASA and ASDM in GNS3
   http://www.youtube.com/watch?v=bPIZwtt7ZYE
   Last accessed: April 27th, 2013

[28] XeruNetworks; Cisco ASA 8.4 on GNS3
   http://www.xerunetworks.com/2012/02/cisco-asa-84-on-gns3/
   Last accessed: May 17th, 2013

[29] Firewall.cx; Basic ASA 5505 configuration
   http://www.firewall.cx/..../basic-asa-5505-configuration.html
   Last accessed: May 20th, 2013

[30] Cisco; ASA to IOS Router LAN-to-LAN IPsec Tunnel
   http://www.cisco.com/..../products_configuration_example.shtml
   Last accessed: May 20th, 2013

[31] Cisco; Configuring Remote Access VPNs
   http://www.cisco.com/..../configuration/guide/vpnremote.html
   Last accessed: May 20th, 2013

[32] Moonie.com; Certificate Server in GNS3
   https://www.m00nie.com/..../cisco-ios-certificate-server/
   Last accessed: June 15th, 2013

[33] Cisco; VRF-aware IPsec cheat sheet
   https://supportforums.cisco.com/docs/DOC-13524
   Last accessed: April 29th, 2013
[34] Networking Nut; RADIUS Server on Window 2008 R2
   http://www.networkingnut.net/radius-server-on-windows-2008/
   Last accessed: May 22\textsuperscript{th}, 2013

[35] Trainsignal; Installing Cisco Configuration Professional
   http://www.trainsignal.com/blog/configuration-professional
   Last accessed: May 22\textsuperscript{th}, 2013
Appendix A

Pre-study

By: Dennis Elgström | dem09001
School of Innovation, Design and Engineering
Mälardalen University Västerås

Supervisor, Ventyx – ABB: Peter Dahlberg
Technical advisor, Ventyx – ABB: Anders Berggren
Advisor, Mälardalen University: Stefan Löfgren
Examiner, Mälardalen University: Mats Björkman

# Contents

7.1 Introduction ................................................................. 37  
7.1.1 Purpose ................................................................. 37  
7.1.2 Background ............................................................. 37  
7.1.3 Problems and Needs .................................................. 37  
7.1.4 Solution proposal ...................................................... 38  
7.2 Analysis ........................................................................... 39  
7.2.1 VPN ........................................................................... 39  
7.3 Bibliography ................................................................. 41
7.1 Introduction

7.1.1 Purpose
The purpose of this pre-study is to identify and determine the best possible solution to the different security problems faced in the thesis. By comparison and a list of pros and cons the best solution is determined.

7.1.2 Background
Ventyx internal network is divided into two sub networks, an office part and a project area part. All ongoing projects are carried out in the project area network, to have them separated from the office network and only allowing access to employees involved in the project.

The project area network itself is divided in to sub networks, with the help of VRF Lite, to separate different project from each other and provide some security. Note that VRF Lite does not support routing between the VRFs making the networks separated like VLANs, but at level three.

Employees from the office network can connect to the project area network with the help of WebVPN and remote desktop; this is sometime considered a security problem, from the customers’ point of view, because there is no authentication of users.

When a project is started Ventyx sends a pre-configured ASA to the customer allowing them to connect, with the help of an EasyVPN tunnel, to project area network and their corresponding VRF where their project is located. Neither here are the users authenticated when entering the project area network which is also considered a security problem.

7.1.3 Problems and Needs
Following problems and needs have been discussed and identified.

7.1.3.1 Needs
- From the office network, employees working in a project should only be able to connect to the project they are part of, in the project area network.
- Customers should only be able to connect to their project located in the project area network.
- Users from the project area network should not be able to enter the office network.
- Authentication of employees connecting to the project area network.
- Authentication of customers connecting to the project area network.
- Authentication, Authorization and Accounting via RADIUS server should preferably (if possible) be done with certificate.
7.1.3.2 Problems
- Hardware needed is not available.
- Virtualization solution might not support all features needed.
- Authentication, unknown if possible to use employees current AD or if new AD is needed.
- Single Point of Failure - unable to access the project area network if the authentication server crashes.

7.1.4 Solution proposal

As of pre-thesis, the left hand side edge router uses WebVPN, NAT and VRF Lite for security. All projects are separated in to VRFs with no possibility to reach each other (no routing between the VRFs). Looking at the NAT configuration, the office network is set to outside and project area to inside; different key components from each project have static NATs to allow access from the office network. With the help of WebVPN it is possible to connect desired component in the project area network by pointing towards its static NAT address. Meaning, all employees on the office network can connect to that desired component if they know the translated IP.

Looking on the right hand side edge router, an IPsec tunnel is setup to the customer allowing them access to the VRF where their project is ongoing. Customers connected to a device on the project area network can access the
office network if that device is accessible from the office by static NAT; this is of course a big security flaw.

The topology illustrates first and foremost how the project area and office network are separated (note: the office and project area are also physically separated on two locations), but more importantly where the security need to be implemented.

- RADIUS servers will be used for Authentication, Authorization and Accounting (AAA) on the edge routers of the project area network to put limitations on users.
- Is it possible to use Vertyx current AD together with RADIUS, or is a new AD required?
- If possible, users should be authenticated with certificate. If not, pre-shared key should be used.
- The IPsec tunnel used between customer and project area network, is that the best solution? Take a look at other solutions.

7.2 Analysis

7.2.1 VPN
To start with we have to ask the question, what do the remote users (customers in this case) do when connected to the project area network? Do they use web applications, file sharing, printers or other applications? Questions like these are important to answer in order to choose the best suited VPN.

To help with the decision of choosing a suitable VPN, some research is required. Internet Protocol Secure (IPsec) VPNs and Secure Sockets Layer (SSL) VPNs are the two major types of internet-based VPNs. Each has its own significant advantages and disadvantages in a corporate network environment.

7.2.1.1 IPsec
IPsec is a complete encryption framework of open standards for IP networks that in particular provides network-to-network security with the help of a variety of protocols and encryption techniques.

IPsec consist of two sub-protocols: Encapsulated Security Payload (ESP) and Authentication Header (AH). ESP provides encryption using various cryptography algorithms like AES or 3DES. AH provides protection for the IP packet header and prevents spoofing by computing a checksum and performing hashing on the header field. [1]

An advantage with IPsec is the integrity and confidentiality it offers through ESP and AH. As previously mentioned AH computes a checksum and performs a hash on the header field, this assures that no one has
modified your packet(s) – integrity. ESP encrypts the packets with the desired cryptography algorithm, thus providing confidentiality. [2]

It is possible to configure IPsec in one of two different modes, either Transport or Tunnel mode. Transport mode is used to encrypt traffic between two hosts and only encrypts the packet payload. Tunnel mode however encrypts both the payload and the IP header within a virtual tunnel between two networks.

In the majority of cases, third-party software is needed on the host/device to access the IPsec VPN. This can be argued as both a pro and a con. The pro is the extra layer of security it provides. Not only do you need to have the correct software, you must also have it properly configured. It might not seem significant, but it is an additional hurdle an unauthorized user would have to get over. The con, licenses for client software can be expensive and difficult to install and support. This con is probably the largest pro for the rival - SSL. ⁶

Pre-thesis, a normal IPsec VPN in mode tunnel is setup between project area and the customers’ network.

7.2.1.2 SSL
As previously mentioned, in 8.2.4.1 IPsec, one of the biggest (if not the biggest) pro with SSL VPN is that you don't need to buy expensive licenses. SSL is a very common protocol, most web browsers have SSL capabilities built in and therefore almost all computers got the required “client software” to connect to an SSL VPN. SSL provide tunnels to specific applications rather than to an entire network.

With SSL you access the desired application(s) through a web browser, which means that it have limited support for other than web-based applications. To access other than web-based applications can be done, but is complex and kind of beats the purpose of SSL (Need third-party software) [3] [4]. While having access to web-based applications, users do not have access to network resources such as file shares or printers.

7.2.1.3 Decision
Upon viewing the pros and cons of an IPsec-based VPN and SSL-based VPN, looking at the requirements – to have a network-to-network tunnel and allowing customers to use certain non-web-based applications – IPsec is the obvious choice.

⁶ Anders Berggren, 2013-04-17
7.3 Bibliography

[1] Cisco.com; IPsec Encryption
http://www.cisco.com/.../technologies_tech_note.shtml
Last accessed: April 15th, 2013

[2] Networksorcery.com; RFC2401
http://www.networksorcery.com/enp/rfc/rfc2401.txt
Last accessed: April 15th, 2013

[3] InformationWeek; SSL VPN Basics
http://www.informationweek.com/ssl-vpn-basics/16700677
Last accessed: April 16th, 2013

[4] Techexams.net; Secure Sockets Layer (SSL)
http://www.techexams.net/..../ras_sec_prot.shtml
Last accessed: April 16th, 2013
Appendix B

Project Formulation
Masters thesis project:

Implementation of a secure network solutions for Project Area
Ventyx – an ABB Company is seeking 1-2 students for the following thesis project.

Short description
We need to secure our network communication both with secure access and secure authentication for our projects in the Project Area. Customer and internal demands force us to separate network, authentication and access for our projects.

Project Directions
- Develop a Plan for how to secure our network communication both with secure access and secure authentication for our projects in the Project Area.
- Test and Implement an AD based solution regarding user authentication
- Test and Implement VRF/NAT/VLAN based infrastructure
- Test and Implement Remote Access and Authentication
- Test and Implement ASA Session Authentication

Prerequisites
The project is suitable for one/two masters students with hardware and/or software orientation. Knowledge of Cisco Network Equipment, Microsoft Active Directory and VMware Virtual Environment.

Contact Person
Peter Dahlberg <peter.dahlberg@ventyx.abb.com>
Phone: +4621324175
Appendix C
Guide: How-to RADIUS server
9.1 Cisco Configuration

This is a how-to guide of how you setup RADIUS authentication for Cisco routers, switches or other Cisco network equipment.

First of all, proper configuration is needed on the Cisco network equipment. The router must be able to reach the server and a few additional parameters of code will be needed on the network equipment, all necessary configurations will be displayed and explained in this appendix.

To get things started, we start configure the Cisco equipment. The Cisco equipment used in this guide is a Cisco router of model 3725.

First of all it is best to add a local user on the router, this prevent us from being totally locked out if from the router if the RADIUS server would go down or is inaccessible for any reason.

(config)# username <username> privilege 15 password <password>

Next we add the actual AAA – RADIUS configuration.

(config)# aaa new-model
(config)# aaa authentication login <group name> group radius local
(config)# aaa authorization exec <group name> group radius local
(config)# ip radius source-interface <interface>
(config)# radius-server host <ip address> key <password>

The last of the configuration needed on the Cisco router is to specify that RADIUS should be used when logging in via SSH/Telnet and/or console port if wanted.

(config)# line con 0
authorization exec <group name>
login authentication <group name>
(config)# line vty 0 4
authorization exec <group name>
login authentication <group name>

That is all configurations needed on the Cisco side, now it is time to head over to the Windows Server 2008 NPS configurations.
9.2 Windows Server 2008 NPS

In this guide I will assume that your server is already setup with an Active Directory or is part of a domain. The server used is a Windows Server 2008 R2.

Step 1: To begin with we will create clients. These will be our various Cisco equipment, in this guide this will be the Cisco 3725 Router. First of all add the Network Policy and Access Services role, when the role is installed click Start, Administrative Tools and there you will find Network Policy Server.
Step 2: On the left hand side, expand RADIUS Clients and Servers, right-click on RADIUS Clients and choose New.

Step 3: From here you will have to add information regarding the new RADIUS Client, such as its IP address, friendly name and shared secret. The shared secret is the same secret you entered when configuring the Cisco device, `radius-server host <hostname> key <password>`, these secrets need to match else the RADIUS server will not work. Also note that I begin my friendly name with “Cisco-“, this because later on when specifying the Client Friendly Name under conditions it is possible to add all devices at once rather than specifying them one for one, more on that later though.
Step 4 (Optional): Press Advanced to specify a Vendor Name. The default of “RADIUS Standard” will work, however I prefer to choose Cisco since it is a Cisco device we are working with.

Step 5: The device is now successfully added. Now we need to add a policy for to be used for users connecting to the RADIUS Client we just made. Head back to Network Policy Server, expand Policies, right-click on Network Policies and choose New.
Step 6: Specify an appropriate Policy Name. Since this policy will be used to specify users allowed to login on the Cisco devices I named my policy to CiscoAdmins.

![Network Policy](image)

Step 7: Add a condition by pressing Add. Since we want to restrict login based on users from the AD, find and select Windows Groups.

![Select Condition](image)
Step 8: Click Add Groups. Here I will specify a group named RADIUS Admins, this is a group of users that are allowed to login on the Cisco devices. If you don’t have a group, go and add one and start over at step 5.

Step 9: Now we want to specify the RADIUS Clients that should be used within this policy, the ones starting with “Cisco-” that we made earlier, click Add.
Step 10: Find **Client Friendly Name**, located under **RADIUS Client Properties**. Click Add.

![Select condition dialog](image)

Step 11: Here we will be tasked to specify the friendly name of the RADIUS client. To add a specific client just simply type the name you gave it during Step 3, however if you followed my advice regarding naming all your clients to begin with “Cisco-“ you can simply type “Cisco-?” to add all clients at once. Press **OK** to add the the condition.

![Client Friendly Name dialog](image)
Step 12: These are all conditions needed, click Next.

Step 13: Here we are asked what we should do when a match is made with this policy, allow or deny access. We want our RADIUS Admins to have access to the Cisco devices so select Access granted and click Next.
Step 14: Chose the authentication methods to be used. I checked everything to allow any type of authentication method.

Step 15: Next you get the option to set constraints. I chose to not set any constraints, press Next.
Step 16: Neither PPP- or Framed attribute is needed, remove them both and press Add.

Step 17: Find and mark Service-Type, click Add.
Step 18: Choose Others and in the drop-down list choose Login. Click Ok and Close.

Step 19: On the left hand side, press Vendor Specific and click Add.
Step 20: Yet again, find **Vendor-Specific** in the list, mark it and press *Add*.

Step 21: Press *Add*, check *Select from list* and in the drop-down list choose *Cisco* as your vendor, check *Yes* and click *Configure Attribute*.
Step 22: Under Attribute value type `shell:priv-lvl=15` to give successful authentication privilege level 15 on the Cisco device. Click OK.

![Configure VSA (RFC Compliant)](image)

Step 23: The remaining was only default configuration, so no changes on Network Access Protection nor Routing and Remote Access. Click Next.

![Configure Settings](image)
Step 24: And that is all for the Network Policy, press Finish.

Step 25: Since we removed PPP and Framed attribute on Step 16, we must also remove it from the default Connection Request policy – WindowsAuthentication. Right-click on the policy and choose Properties.
Step 26: Find the tab Settings, and under RADIUS Attributes mark Standard. Delete both the PPP and Framed attribute. Click OK to apply the changes.