Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler

Ayoub BAHNASSE
Department of physics
University Chouaïb Doukali
Faculty of science El Jadida
EL Jadida, MOROCCO

Najib EL KAMOUN
Department of physics
University Chouaïb Doukali
Faculty of science El Jadida
EL Jadida, MOROCCO

***Abstract*—The simulation of large-scale networks is a challenging task especially if the network to simulate is the Dynamic Multipoint Virtual Private Network, it requires expert knowledge to properly configure its component technologies. The study of these network architectures in a real environment is almost impossible because it requires a very large number of equipment, however, this task is feasible in a simulation environment like OPNET Modeler, provided to master both the tool and the different architectures of the Dynamic Multipoint Virtual Private Network.**

Several research studies have been conducted to automate the generation and simulation of complex networks under various simulators, according to our research no work has dealt with the Dynamic Multipoint Virtual Private Network. In this paper we present a simulation model of the Dynamic and Multipoint Virtual Private network in OPNET Modeler, and a WEB-based tool for project management on the same network.

Keywords—VPN; multipoint; Opnet; automation; DMVPN; cloud; policy-based; WEB-BASED

I. INTRODUCTION

Dynamic multipoint Virtual Private Network "DMVPN" is a solution for building dynamic Virtual Private Network tunnels in an easy, scalable and dynamic manner supported on Cisco IOS routers and Unix Operating System, DMVPN is based on standard technologies such as Resolution Next Hop Protocol (NHRP) and multipoint Generic Routing Encapsulation (mGRE) for the dynamic creation of tunnels, and Internet Protocol Security (IPsec) to ensure security of data exchanges between multiple sites, as well as routing protocols to route data optimally [1] [2], several scientific studies have been conducted to study the effect of routing protocols on Non Broadcast Multi-Access networks (NBMA) [3] [4]. The HUB maintains in its NHRP cache, public and tunnel IP addresses of each SPOKE on the same network, this protocol is based on the client-server principle, the spokes (NHRP Clients) send periodic NHRP updates containing public and tunnels addresses to the HUB (NHS) of the network, for example when SPOKE1 wants to communicate with SPOKE2, SPOKE1 consults the NHRP cache of NHS to determine public IP associated with the IP tunnel of SPOKE2. A GRE interface can maintain multiple IPsec tunnels, both to simplify configuration and save time thanks to mGRE protocol. GRE protocol encapsulates various higher layer protocols and carry all traffic types (unicast, multicast and broadcast), but doesn't provide any authentication, integrity or confidentiality mechanism. IPsec is a suite of protocols; Encapsulation Security Payload (ESP) and Authentication Header (AH), the first protocol ensure the integrity, authentication and confidentiality of trade, the second provides integrity and authentication for data exchange. IPsec operates in two modes, tunnel and transport mode, transport mode does not change the initial header it sits between the network layer and transport of the OSI model, for this mode, NAT can cause a problem of integrity [5], the tunnel mode replaces the original IP and encapsulates the entire packet header.

OPNET Modeler is a software tool for network modeling and simulation. It allows to design and study communication of large scale networks, devices, protocols, and applications with great flexibility, it allows to study the system performance under varying conditions, it also contributes to the development of new protocols and architectures and their optimization and the analysis of the impact of emerging technologies, several books have been written to master OPNET Modeler environment and properly handle its associated objects [6, 7].

The process of setting up an Opnet project can be done by several methods including: Drag drop objects to the workspace;

Data Router configuration, to create the project based on the configuration files of routers such as Cisco and Juniper, to benefit from this feature the module Multi Vendor Import " MVI " must be turned on from license management;

Extensible Markup Language " XML ", the required form of the XML file to import to Opnet is specified in the Document Data Type " DTD " , the file path is ″<opnet_dir> / <reldir> / sys / etc / network.dtd″.

The simulation of communication network is paramount in the design process task, planning and optimization of architectures. Through a simulation environment, many conditions can be studied such as scalability that is difficult to simulate in a real environment because of its very high cost, such as simulation of the dynamic and multipoint virtual private networks. Several scientific research simulators can be

used as OPNET Modeler, NS2…[8,9,10], but managing a dynamic and multipoint VPN under OPNET Modeler simulator requires firstly a mastery of the tool and secondly the technology, this is a good motivation to develop a system for automatically creating projects for various architectures of the same network, for this reason we have created an automation model for simulating dynamic multipoint and multi architectures Virtual Private Network, and a GUI man/machinery application designed for this type of networks.

The simulation of a large scale network such as DMVPN in a simulator such as Opnet Modeler requires a mastery of VPN technology and the simulator, and since these VPNs can be composed of hundreds sometimes thousands of sites its simulation by the manual method without mistakes is a big challenge, various works has been done in the automation of networks simulations for Opnet modeler [11, 12] and the design of GUI-based tool for the conversion of simulation scenarios to the XML files meant for various simulators[13], unfortunately according to our research no automation model of generation and simulation of such networks was proposed, this is a good motivation to develop a new model for automating simulations of DMVPN networks for Opnet Modeler "DMVPN Automatic Simulation" and create a WEB-based tool for personalized management of projects.

The rest of the paper is organized as follows, in Section 2 we will discuss the developed model "DMVPN Automatic Simulation" and define its various modules, in Section 3 we will describe thoroughly various steps required by the model to automatically generate projects, Section 4 will be reserved for a sample demonstration of an automatic generation of project using the application implemented, and we will conclude in section 5.

II. DMVPN Automatic Simulation Model

DMVPN Automatic Simulation model [Fig. 1] allows policy-based simulation automation for DMVPN network, multi-architectures, for Opnet model using a web graphical interface, the model is composed of two main agents "User Policies Definition" and "Treatment and generation";

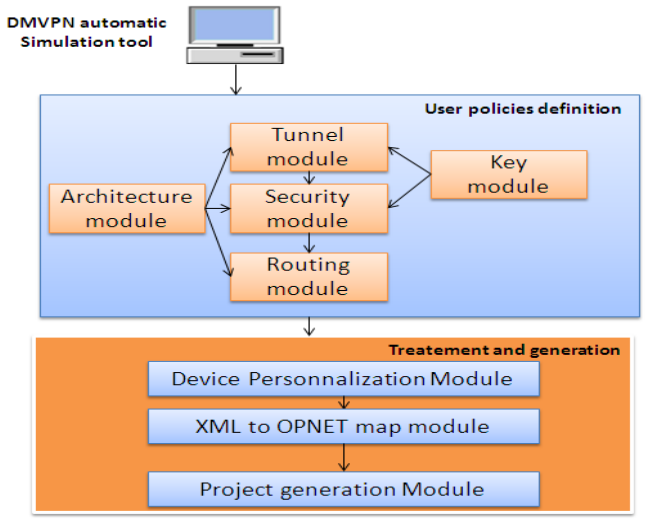

Fig. 1. Architecture of DMVPN Automatic Simulation

A. User Policies Definition:

This agent allows defining the attributes of security and routing policies of the DMVPN network, through a graphical man/machinery interaction.

This agent is composed of several modules; Architecture Module, Tunnel Module, Security Module, Routing Module and Key Module.

- Architecture Module: This module defines the type of architecture to handle: Single Hub Single Cloud or Multiple Hub Multiple Cloud.
- Tunnel Module: This module is responsible of establishing tunnels between the Hubs and Spokes depending on the type of architecture described in the previous module. The identification and authentication of tunnels will be made by Key Module attributes.
- Security Module: This module defines the IPsec protocol to use and which could be AH or ESP, encryption protocols (DES, 3DES, AES) and integrity protocols (MD5, SHA) for two IKE phases, by default the mode used is transport to avoid a third encapsulating of the IP header.
- Key Module: This module defines the identification key of the tunnel, the DMVPN cloud ID, the authentication key for access to the DMVPN network as well as the IPsec password.
- Routing Module: This module allows the generation of a more suitable configuration of routing protocol for a specific DMVPN architecture, the proposed model supports; Routing Information Version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Interior Border Gateway Protocol (iBGP).

B. Treatment and generation:

This agent describes the processing that occurs on the server side, converting user data into a project already configured ready to be simulated in Opnet Modeler, this agent is composed of three modules:

- Device personalization module: This module allows the generation of nodes (routers and IPV4 clouds) with a customized number of interfaces according to the user-specified architecture.
- XML to map OPNET Module: This module check the attributes of the file network.dtd to prepare a customized XML file with user specified data, XML attributes may differ from architecture to another, equipment generated by the previous module will be defined in the XML file.
- Project generation module: This module allows the generation of XML file prepared by the previous module and run the simulation in Opnet Modeler.

III. FUNCTIONING OF THE DMVPN AUTOMATIC SIMULATION MODEL

In this section we will describe various steps required by the model ″DMVPN Automatic Simulation″ to automatically generate projects, [Fig. 2] shows the operation of the model.

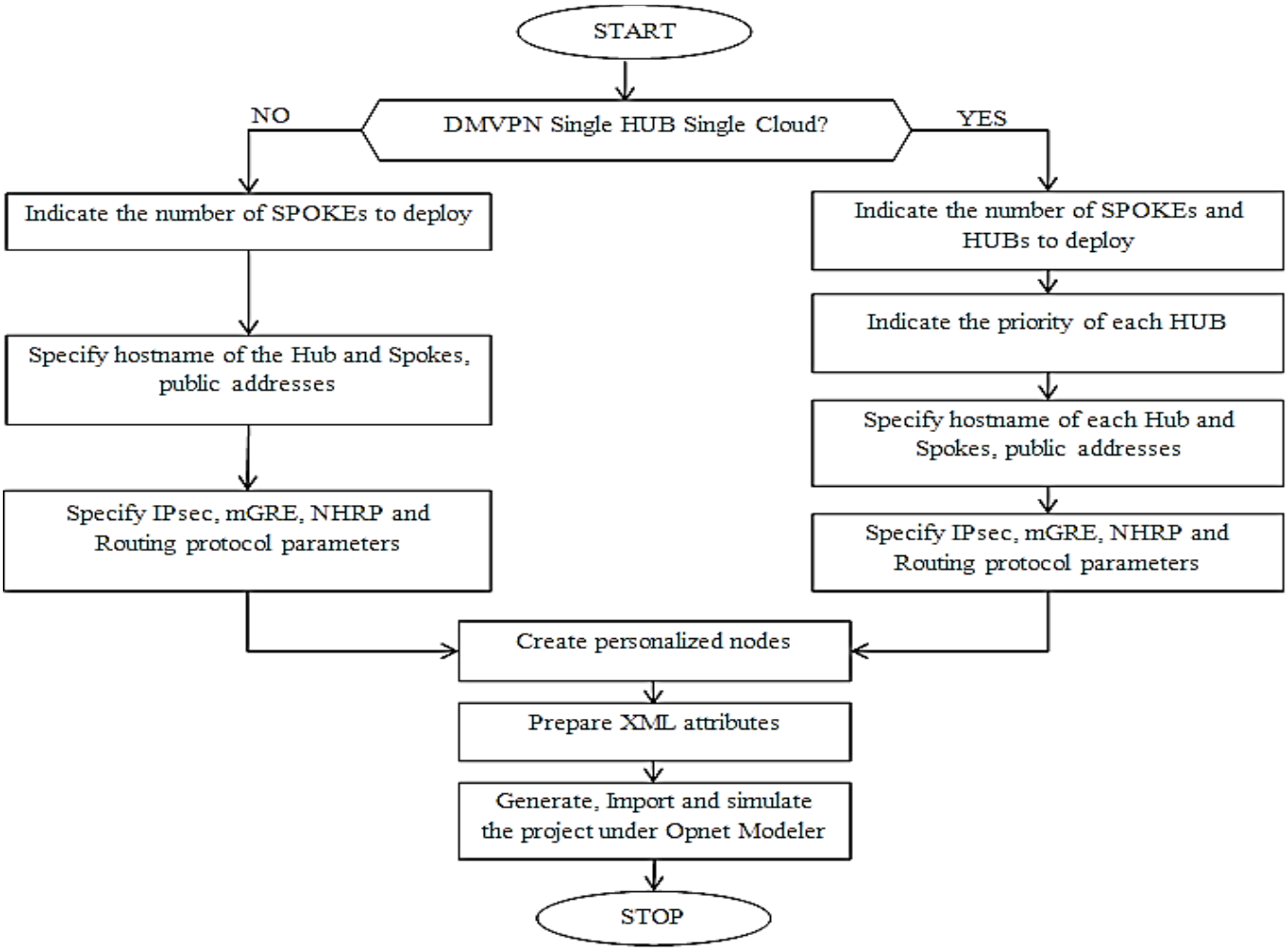

Fig. 2. Flow chart illustrate the operation of DMVPN Automatic Simulation

1) The user must choose the architecture to deploy; Single Hub Single Cloud or Multiple Hub Multiple Cloud;

2) If the user chooses to simulate Single Hub Single Cloud architecture, a specification of number of Spokes to deploy is necessary, according to the specified number by the user a graphical user interface will be generated automatically composed of n + 1 rows, where n is the number of Spokes and 1 is the HUB line;

3) The user must specify for each device its Public IP addresses, private IP address and the name of the public interface;

4) The user defines graphically the security settings of IKE Phase 1 and 2, specifies the NHRP password, NHRP + mGRE keys and finally chooses the routing protocol (RIPv2, EIGRP, OSPF, iBGP);

5) If the user chooses Multiple Hub Multiple Cloud, a specification of number of Hubs and Spokes to deploy is necessary;

6) The user must specify for each device its Public IP address, private IP address, the name of the public interface and the priority of each HUB, if routers have the same priority, load balancing with equal cost will be made between HUBs, if not the router with the highest priority will be the primary router, the other will be considered secondary;

7) The user defines graphically the security settings of IPsec IKE Phase 1 and 2, specifies NHRP password, NHRP + mGRE keys and finally chooses the routing protocol (RIPv2, EIGRP, OSPF, iBGP)

8) The nodes are created with a customized number of interfaces according to user-specified architecture.

9) XML attributes to be used for a specific version Opnet model are prepared according to DTD file of current version of Opnet Modeler installed;

10)The final generated XML file containing the position of each node and its associated configuration ready to be simulated in Opnet Modeler.

IV. Demonstration and Guided Visit

In order to validate the Designed model, an implementation is required, the tool created is based on a guided web graphical interface extremely easy to manipulate, any web browser and operating system can be used.

Developed tool (DMVPN Automatic Simulation Tool) has two mains purposes. First purpose is to provide a user-friendly entering and editing of parameters of DMVPN network. Second purpose is to automatically map user parameters into OPNET Modeler project and create custom nodes.

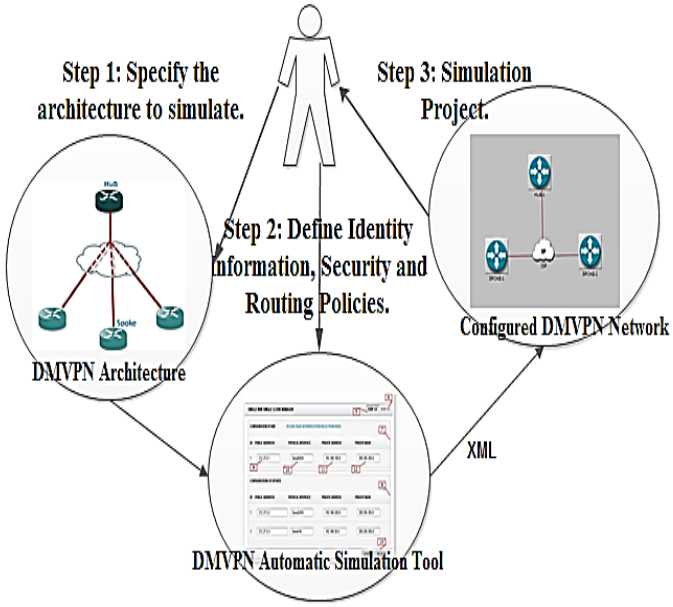

Fig. 3. Use Case Diagram of proposed tool

The modeling procedure [Fig. 3] consists of four steps:

Step 1: User must choose the architecture to deploy;

Step 2: User must indicate for each specific device its identity information (public, private and tunnel IP addresses, outside interface and private address mask);

Step 3: User must indicate Security policy (IPsec attribute, NHRP password and mGRE and NHRP Keys) and routing protocol (RIPv2, EIGRP, OSPF, iBGP) to be applied for all equipment on the same architecture;

Step 4: DMVPN Automatic Simulation Tool convert automatically user parameters into XML configuration file ready to be simulated under OPNET Modeler.

The following demonstration will be for the simulation of DMVPN network, Single Hub Single Cloud architecture, composed of two Spokes.

Step 1- Specify the architecture to simulate:

The user through the menu [Fig. 4] can choose to deploy a Single Hub Single Cloud architecture (***1***) Multiple Hub Multiple Cloud (***2***)

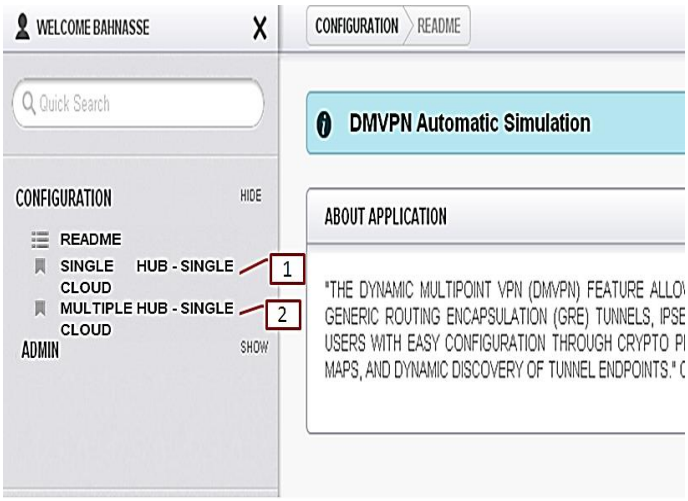

Fig. 4. Main Menu

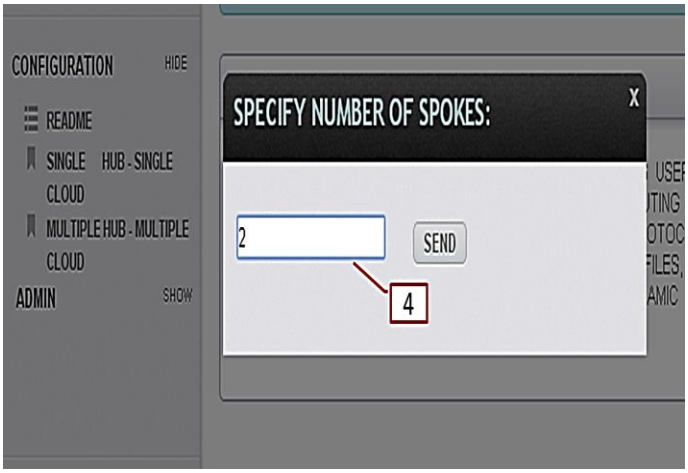

Fig. 5. Specifying the number of Spokes to deploy

A window appears [Fig. 5], prompting the user to specify the number of Spokes to deploy (***4***).

Step 2 : Define identity information:

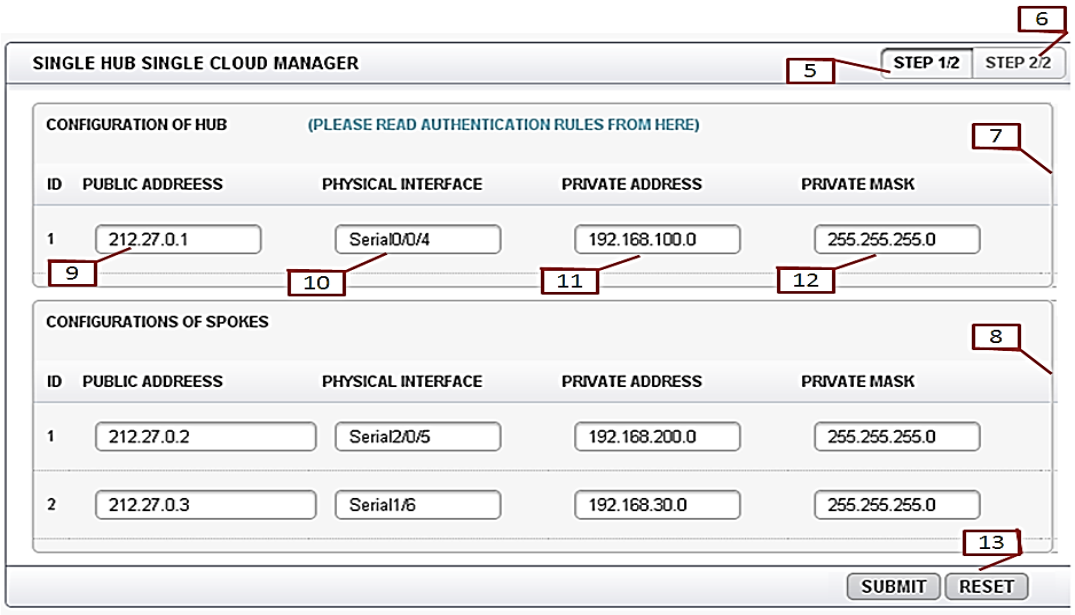

Fig. 6. Specifying equipments data

After specifying the number of Spokes to install, a window [Fig. 6] is displayed, the window is mainly composed of two parts: identity configuration (***5***) security and routing policies configuration (***6***). The flap (***5***) consists of two sections: HUB Configuration (***7***) and Spokes Configuration (***8***), the two sections are composed of the following fields: public IP address (***9***) outside interface (***10***), private IP address (***11***), subnet mask of private address (***12***), option (***13***) to reset all fields the current window.

Step 3 : Define security policy and routing protocol:

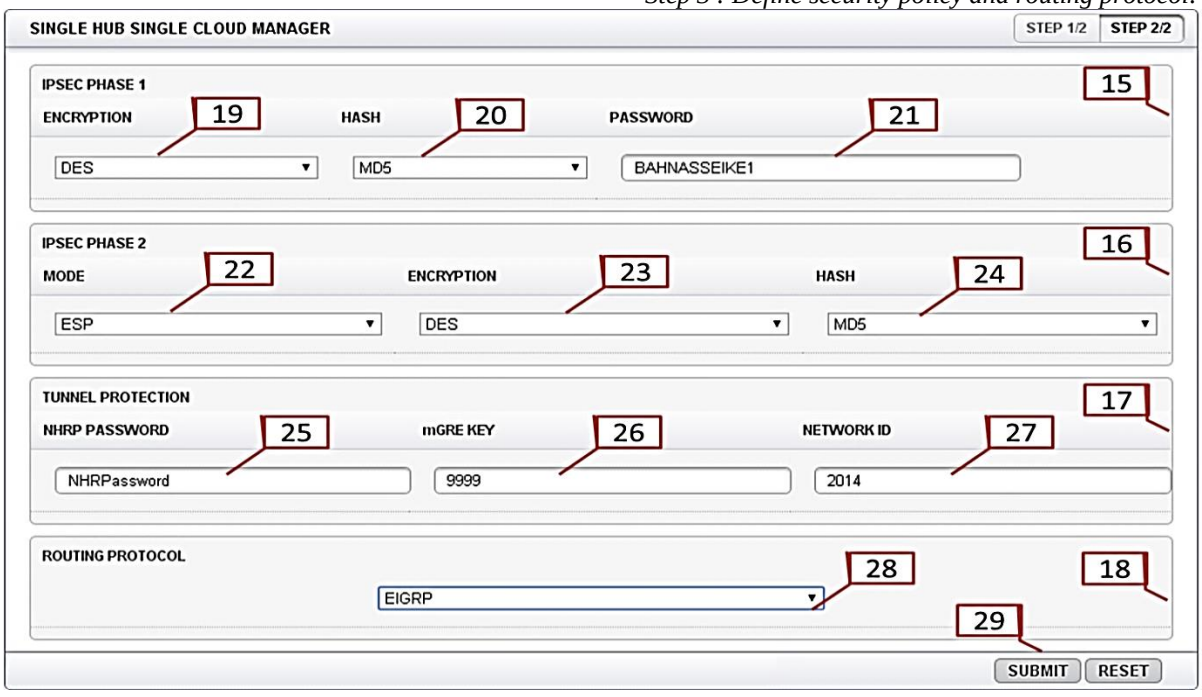

Fig. 7. Configuration of security and routing policies

The second section, security and routing policies configuration [Fig. 7] consists of four main sections: IPsec phase 1 configuration (***15***), IPsec phase 2 configuration (***16***), protection of the tunnel (***17***) and the choice of routing protocol (***18***).

Section (***15***) is composed of three fields, the choice of encryption protocol (***19***), the integrity protocol (***20***) and the password key derivation (***21***).

Section (16) is composed of three fields, the protocol IPsec to use ESP or AHP (***22***), encryption protocols and integrity respectively (***23***) and (***24***); the default mode is set to Transport.

Section (17) is composed of three fields, NHRP password of current network (25), mGRE tunnel key (26) used to separate tunnels and provide authentication and the identifier of the NHRP network (27).

The last section (***18***) allows the user to pick through a list the protocol to be implemented which can be one of these protocols RIPv2, EIGRP, OSPF or iBGP (***28***).

Step 4 : Import generated XML File to OPNET Modeler:

After completing the customization of the architecture, submit button (***29***) send user parameters to remote server in order to generate custom nodes and an XML file containing the configuration of the project ready to be simulated in Opnet Modeler [Fig.8].

Final step consist of importing generated XML file to Opnet Modeler, [Fig. 9] illustrate the resulting topology.

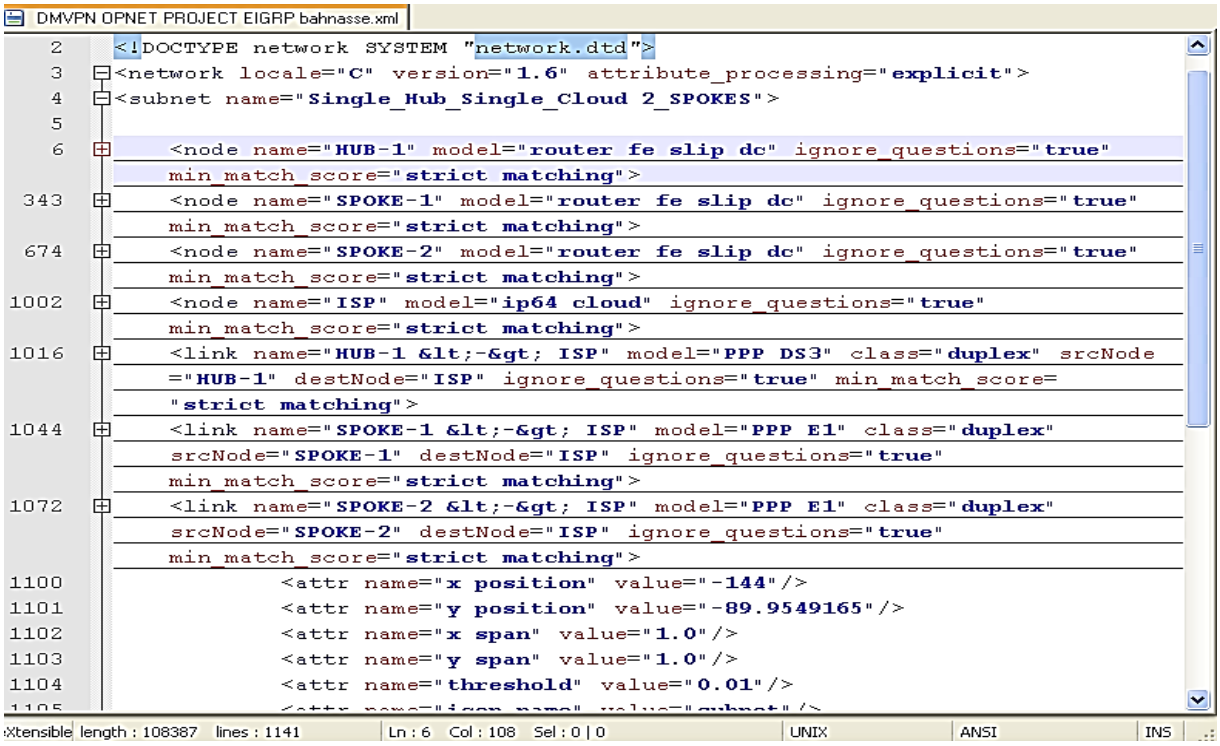

Fig. 8. resulting XML file

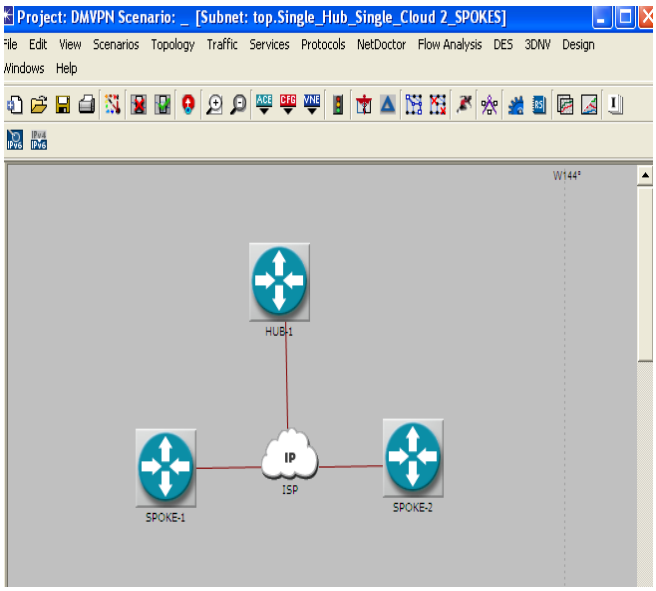

Fig. 9. Designed and configured Architecture

V. CONCLUSION

Manual stimulation of a Dynamic Multipoint multi-architecture VPN network, in Opnet Modeler is a time-consuming task, which also requires expertise in technology to simulate and the simulator as well as the margin of error is not null. The model proposed and the tool designed allows automating the generation of dynamic scenarios VPN multipoint multi- architectures projects for Opnet modeler based on a WEB-Based interface easy to manipulate.

The model was implemented and tested on Single Hub Single Cloud architecture consisting of ten Spokes, the time required for an expert on VPN networks and Opnet Modeler for manual set up of this architecture is 40 minutes, we moved that to 3 minutes with the proposed model, in addition to time effectiveness the margin error is null.

The independence of the modules of the model proposed will allow in future work to adapt it with other simulators such as NS3 simulator.

REFERENCES

[1] Asati, R., Khalid, M., Retana, A. E., Van Savage, D., & Sethi, P. P. (2013). U.S. Patent No. 8,346,961. Washington, DC: U.S. Patent and Trademark Office.

[2] Chen, H. (2011, May). Design and implementation of secure enterprise network based on DMVPN. In Business Management and Electronic Information (BMEI), 2011 International Conference on (Vol. 1, pp. 506-511). IEEE.

[3] Jankuniene, R., & Jankunaite, I. (2009, June). Route creation influence on DMVPN QoS. In Information Technology Interfaces, 2009. ITI'09. Proceedings of the ITI 2009 31st International Conference on (pp. 609-614). IEEE.

[4] Thorenoor, S. G. (2010, April). Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET modeler. In Computer and Network Technology (ICCNT), 2010 Second International Conference on (pp. 191-195). IEEE.

[5] Adoba, B., & Dixon, W. (2004). RFC 3715–IPSec-network address translation (NAT) compatibility requirements.

[6] Lu, Zheng, and Hongji Yang. Unlocking the power of OPNET modeler. Cambridge University Press, 2012.

[7] Ibrahim, Q., & Khudher, I. A. (2011). Network Simulation Guide: Lecture Notes and Lab Manual.

[8] Altman, E., & Jimenez, T. (2012). NS Simulator for beginners. Synthesis Lectures on Communication Networks, 5(1), 1-184.

[9] Siraj, S., Gupta, A., & Badgujar, R. (2012). Network simulation tools survey.International Journal of Advanced Research in Computer and Communication Engineering, 1(4), 199-206.

[10] Borboruah, G., & Nandi, G. (2014) A Study on Large Scale Network Simulators5. International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 7318-7322.

[11] Mohorko, J., Klampfer, S., Fras, M., & Cucej, Z. Expert System for Automatic Analysis of Results of Network Simulation.

[12] Li, H., & Lin, X. (2005, October). An OPNET-based 3-tier network simulation architecture. In Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on (Vol. 2, pp. 793-796). IEEE.

[13] Canonico, R., Emma, D., & Ventre, G. (2003, October). An XML description language for web-based network simulation. In Distributed Simulation and Real-Time Applications, 2003. Proceedings. Seventh IEEE International Symposium on (pp. 76-81).IEEE.