Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 8 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network

By Ayoub Bahnasse & Najib EL Kamoun
Chouaib Doukali University, Morocco

Abstract- Although IP VPN technology has recently been imposed because of its cost effectiveness and that several research studies have been proposed for centralized policy management of intra / inter VPN domain, most solutions are only addressed to VPN site-to-site technology, according to our researches no centralized management model based on a server for dynamic multipoint VPN networks was proposed.

In this paper we propose a model "DMVPN Security Management System"for centralized policy management of dynamic multipoint multi-architectures VPN network, using a new web interface.

We have implemented and tested the model on Single Hub Single Cloud architecture consisting of ten Spokes, the time required for an expert on VPN networks for manual set up of this architecture is an hour, we moved that to five minutes with our model, in addition to time effectiveness the margin error is null.

Keywords: *VPN, multipoint, DMVPN, cloud, policy-based, WEB-BASED, HUB, SPOKE.*

GJCST-E Classification : *C.2.1 C.2.2*

Strictly as per the compliance and regulations of:

Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network

Ayoub Bahnasse [α] & Najib EL Kamoun [σ]

Abstract- Although IP VPN technology has recently been imposed because of its cost effectiveness and that several research studies have been proposed for centralized policy management of intra / inter VPN domain, most solutions are only addressed to VPN site-to-site technology, according to our researches no centralized management model based on a server for dynamic multipoint VPN networks was proposed.

In this paper we propose a model "DMVPN Security Management System"for centralized policy management of dynamic multipoint multi-architectures VPN network, using a new web interface.

We have implemented and tested the model on Single Hub Single Cloud architecture consisting of ten Spokes, the time required for an expert on VPN networks for manual set up of this architecture is an hour, we moved that to five minutes with our model, in addition to time effectiveness the margin error is null.

Keywords: VPN, multipoint, DMVPN, cloud, policy-based, WEB-BASED, HUB, SPOKE.

I. Introduction

Through VPN technology, companies can communicate with each other securely through a public infrastructure with the least cost compared to alternatives such as Frame-Relay, ATM… [1] [2]. Companies steadily increasethe number of branches which poses a problem of scalability,

While reconfiguring all sites is mandatory when a change is made. Dynamic Multipoint VPN stands for DMVPN [3] proposed by Cisco corporation solution, offer scalability through its HUB and SPOKE architecture, Remote-Branch Offices (SPOKES) are linked to a central hub node called HUB with a permanent tunnel, but are not linked statically between them . These can communicate with each other through temporary tunnels created on demand, thanks to the intervention of the HUB. With this approach the problem of scalability is resolved, in case we add a SPOKE, other equipment previously configured will undergo no further modifications, we however had to configure the added SPOKE to register with the HUB and become a member of the current architecture.

DMVPN is based on 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 [4] [5], several research works have been conducted to study the impact of routing protocols on dynamic multipoint VPN networks or Non broadcast Multi-Access networks (NBMA) in general [6] [7]. The HUB maintains in its NHRP cache public and tunnel addresses of each SPOKE on the same network, ie the protocol is based on the client-server principle, spokes (NHRP Clients) send periodic NHRP updates containing public and tunnel addresses to the HUB (NHS) of the network, when SPOKE1 wants to communicate with SPOKE2 for example, SPOKE1 consults the NHRP cache of the NHS to determine public IP associated with the IP tunnel of SPOKE2. A GRE interface can maintain multiple IP sec tunnels to both to simplify the configuration and save time of configuration thanks to MGRE protocol. GRE protocol encapsulates various higher layer protocols [8] and carry all traffic types (uni cast, multicast and broadcast), but doesn't provide any authentication mechanism, integrity or confidentiality. IP sec [9] is a suite of protocols Encapsulation Security Payload (ESP) [10] and Authentication Header (AH) [11], the first protocol ensure the integrity, authentication and confidentiality of trade, the second provides data integrity and authentication for data exchange. IP sec 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 [12], the tunnel mode replaces the original IP and encapsulates the entire packet header.

Centralized VPN policy management is an active area of research to date, several contributions were made to negotiate and create VPN policies between equipment from different areas [13] as well as to manage the control plane of IP sec protocol for multiple VPN [14] and provide a man/machinery interaction using a customized web-based interface, for the management of VPN networks[15] [16]. Previous works deal with the central management of site-to-site VPN policies using Web-based interfaces, our contribution is in relation with the dynamic and multipoint aspect of VPN network for various architectures, it provides a model of centralized policy management and a GUI man/machinery application designed for this type of networks.

Author α σ : Lab STIC, Department of Physics, Faculty Sciences El Jadida, University Chouaïb Doukali, Morocco.
e-mails: bahnasse.a@ucd.ac.ma, elkamoun@ucd.ac.ma

This paper is organized as follows: in section 2 we will discuss the developed model "DMVPN Security Management System" and define its various modules in Section 3, we will detail the operation of the model, Section 4 will be reserved for a demonstration and tour on the application implemented, and we will conclude in section 5.

II. DMVPN Security Management System

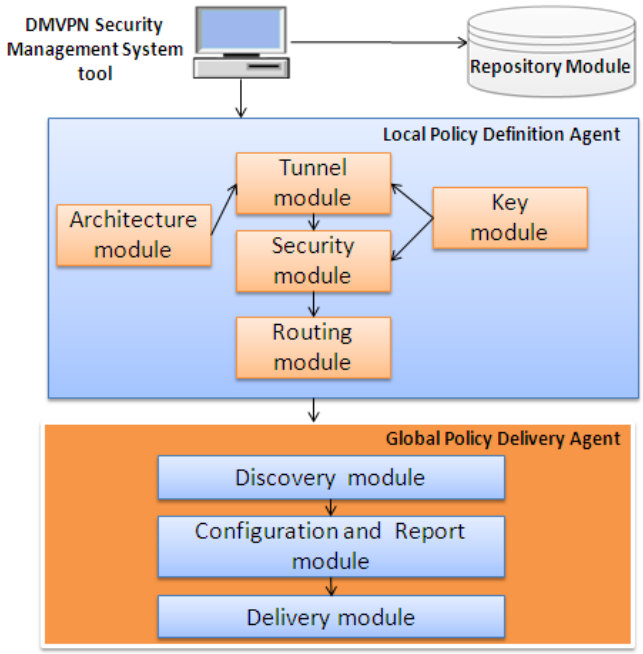

Figure 1 : Architecture of Model DMVPN Security Management System

The proposed model [FIG. 1] is composed of two main agents, "Local Policy Definition Agent" and "Global Policy Delivery Agent";

✓ *Local Policy Definition Agent:* Used to define locally the attributes of security and routing policies of DMVPN networks 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, Multiple Hub Multiple Cloud. Each generated architecture is characterized by a unique sequence number that will be used for further modification or addition of equipment.
- *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 the attributes of Key Module
- *Security Module:* This module defines the IPsec protocol to use and whichcould be AH or ESP, encryption protocols (DES, 3DES, AES) and integrity protocols (MD5, SHA) for both IKE phases, by default the mode used is transport to avoid a third encapsulating of the IP header.
- *Key Module:* This module defines the tunnel key ID, the DMVPN cloud ID, the authentication key for access to the DMVPN network as well as the IP sec password.
- *Routing Module:* This module allows the generation of a more suitable configuration of routing protocol for a specific DMVPN architecture, our model supports; Routing Information Version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Interior Border Gateway Protocol (IBGP).

✓ *Global Policy Delivery Agent:* Detects the version of the manufacturer of the end equipment and convert user data to specific commands, store policies configuration and deliver them remotely using SSH tunnel. This agent consists of three modules; Discovery module, Configuration and report module and Delivery Module.

- *Discovery Module:* This module performs automatic detection of the manufacturer of the end equipment.
- *Configuration and store Module:* This module translates the user data to specific command lines for the equipment detected by the Discovery Module, and stores data on the repository module.
- *Delivery Module:* This module opens an encrypted SSH tunnel to the end devices and delivers encrypted data for safety measures.
- *Repository Module:* This module is a Structured Query Language Server(SQL) used to store the data of each module for a given architecture created by a specific user. With this module when adding new equipment for a specific architecture, security and routing policies applied to previous equipment will be applied by default on new one without manual user specification.

III. Operation of the Model DMVPN Security Management System

Our model allows centralized management of security policies for a dynamic multipoint VPN, ensuring scalability.

The graph shown in [FIG. 2] shows the steps to follow for centralized management.

1. The user must choose the architecture to deploy; Single Hub Single Cloud or Multiple Hub Multiple Cloud;
2. If the user selects Single Hub Single Cloud, 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, the name of the public interface and SSH authentication data for secure data delivery of configurations, the user can check the settings of SSH authentication from the same graphical interface, the model detects the availability of equipment, Round Trip Time (RTT), and state of TCP port 22, and the validity of the SSH authentication data;
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, the SSH authentication data for secure data delivery of configurations and the priority of each HUB, if routers have the same priority, load balancing with equal costwill be made between HUBs, if not the router with the highest priority will be the primary router, the other will be considered secondary. The user can verify the authentication settings from the same graphical interface, the model detects the availability or not of equipment, Round Trip Time (RTT), the state of TCP port 22, and the validity or invalidity of the SSH authentication data;
7. The user defines graphically the security settings of IP sec IKE Phase 1 and 2, specifies NHRP password, NHRP + MGRE keys and finally chooses the routing protocol (RIPv2, EIGRP, OSPF, IBGP)
8. A unique ID will be generated for the created architecture;
9. User data will be stored in a SQL server for future reference or modification;
10. The translation of user data into specific command line and delivery to destinations via the SSH tunnel;

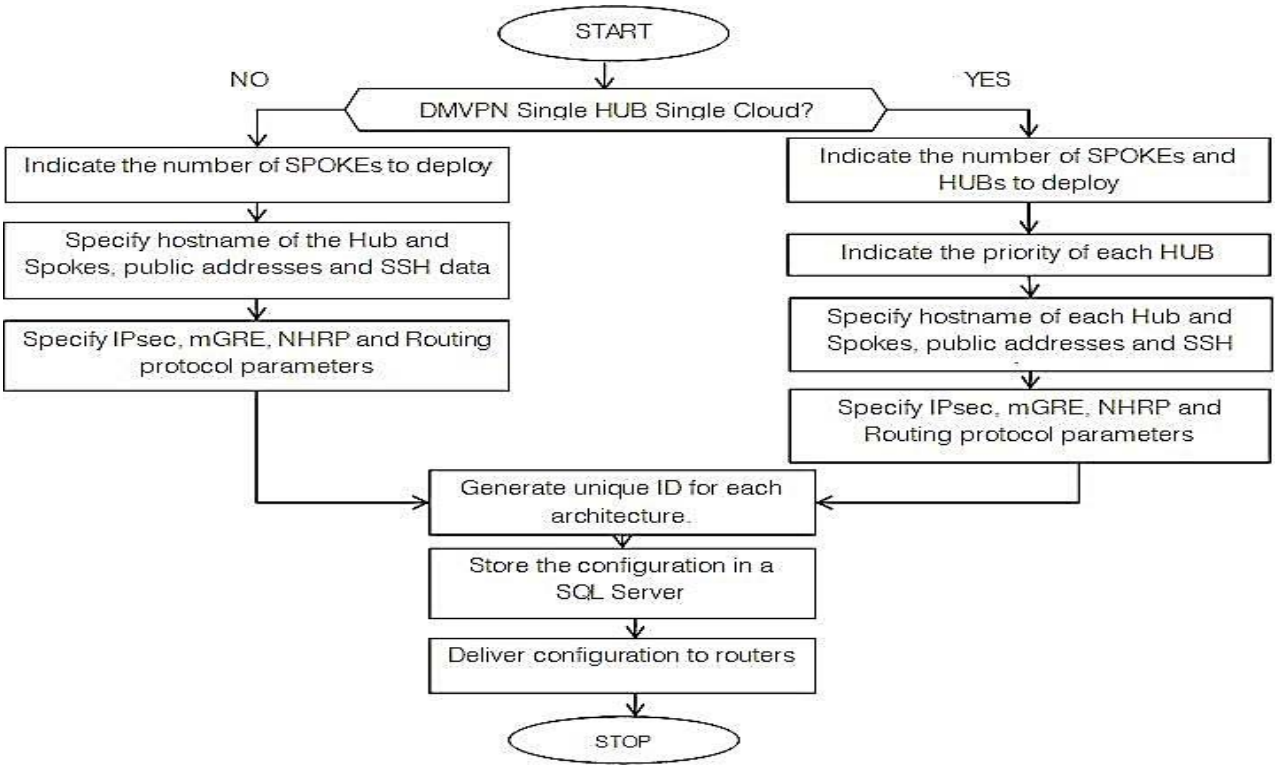

Figure 2 : Diagram illustrating the initial use of the model

Although our model provides scalability, Figure [FIG. 3] shows how a user can make subsequent changes to a given architecture.

1. The user specifies the ID of the architecture to be modified;
2. The application performs a test to check if the currently logged in user is the owner of the architecture to be modified, if the result is false the operation is stopped, if not:

3. If the identifier of the architecture refer to a Multiple HUB Multiple Clouds architecture ,then;
4. The user specifies the number of additional Hubs and Spokes to deploy;
5. The user specifies the priority of each HUB;
6. The user must specify for each device its Public IP address, private IP address, the name of the public interface and SSH authentication data for secure data delivery of configurations, the user can check the settings of SSH authentication data from the same graphical interface, the model detects the availability of equipment, Round Trip Time (RTT), and state of TCP port 22, and the validity or invalidity of the SSH authentication data. Security and routing policies associated with the architecture being modified will be applied automatically to added new equipment;
7. If the identifier of the architecture does not refer to a Multiple HUB Multiple Clouds architecture, then;
8. The user specifies the number of additional Spokes to deploy;
9. The user must specify for each device its Public IP address, private IP address, the name of the public interface and SSH authentication data for secure data delivery of configurations, the user can check the settings of SSH authentication from the same graphical interface, the model detects the availability or unavailability of equipment, Round Trip Time (RTT), and state of TCP port 22, and the validity or invalidity of the authentication data SSH. Security and routing policies associated with the architecture being modified will be applied automatically to added new equipment;
10. A Notification email will be immediately sent to the administrator upon successful addition of new equipment.
11. The new changes of the architecture being modified will be stored on the SQL server;
12. The translation of user data into specific command line and delivery to destinations via the SSH tunnel;

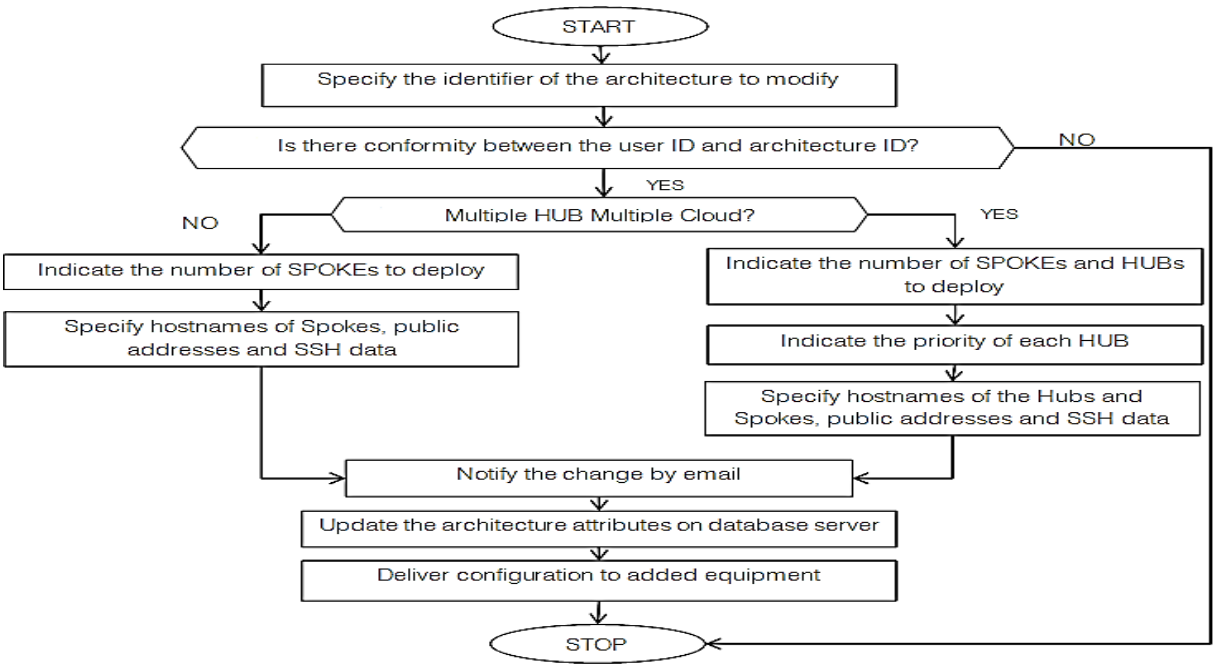

Figure 3 : Illustration Diagram of the operation of the model in case of change

IV. Demonstration and Guided Tours

In order to validate the Designed model, we have implemented and tested it on a network of communicating company; its implementation is based on a graphical web interface usable from any operating system.

The following demonstration will be for the establishment of Dynamic Multipoint VPN Single Hub Single Cloud architecture.

Figure 4 : Main Menu

The user through the menu (FIG.4) can choose to deploy a Single Hub Single Cloud architecture (1) Multiple Cloud Multiple Hub (2) or Edit a specific architecture (3).

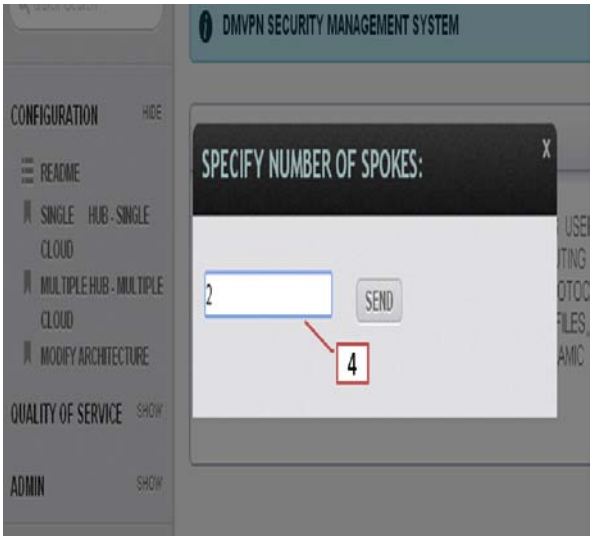

Figure 5 : Number of Spokes to deploy

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

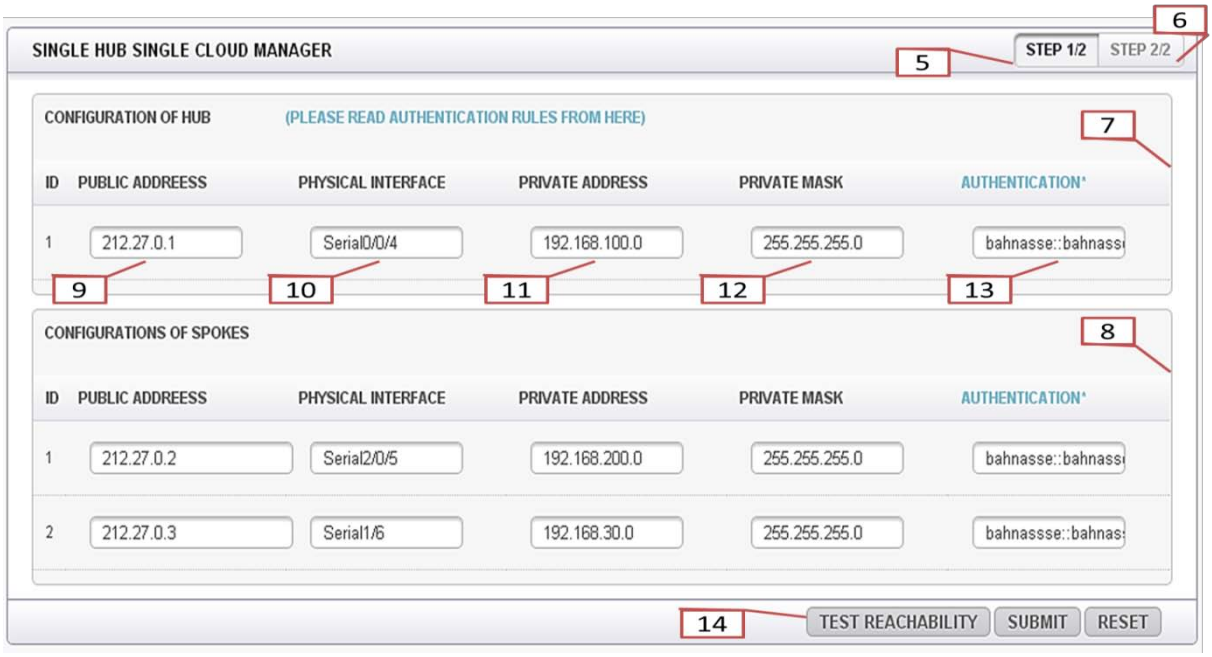

Figure 6 : Configuring identity and authentication SSH

After specifying the number of Spokes to install, a window [FIG. 6] is displayed, the window is mainly composed of two parts: identity configuration and SSH authentication (5) securityand 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) and SSH authentication data (13). The option (14) is used to: test the accessibility or inaccessibility of the remote device, calculate the Round Trip Time (RTT), the status of port 22 (Active or Inactive) and the validity of the authentication or not (refer to FIG. 7).

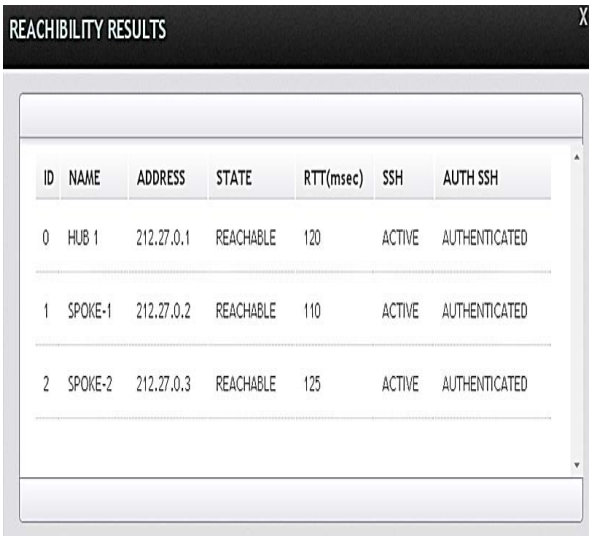

Figure 7 : Accessibility Test

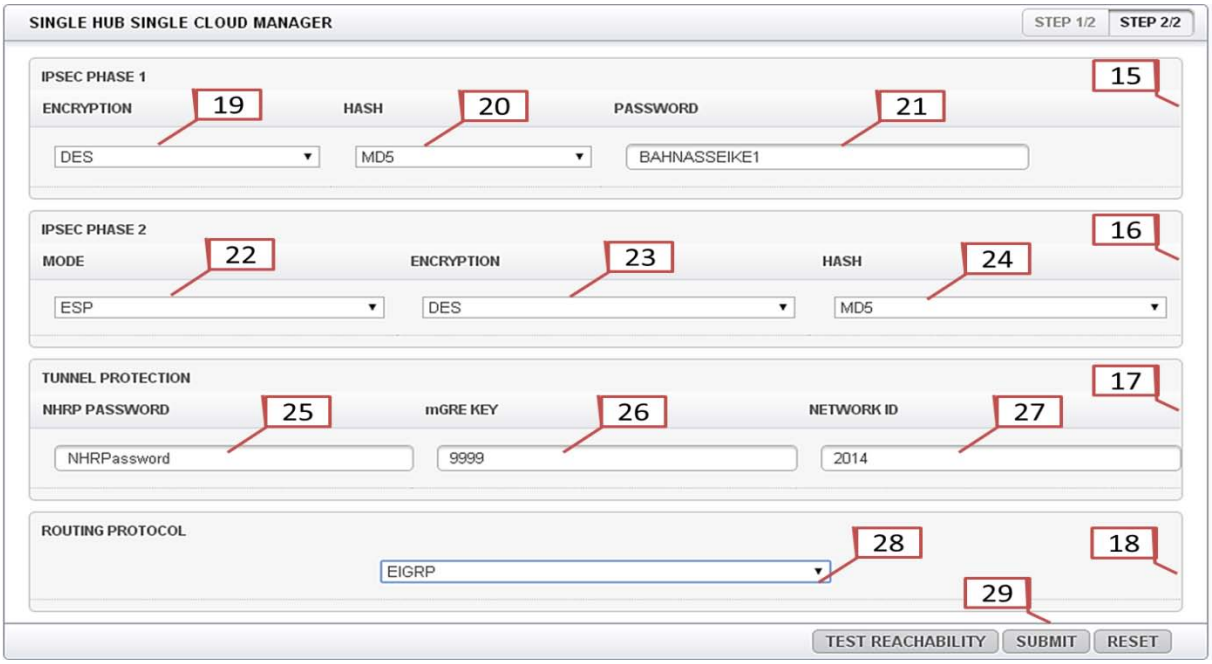

Figure 8 : Configuration of security and routing policies

The second section, security and routing policies configuration consists of four main sections: IPsec phase 1 configuration (15), IP sec second phase configuration(16), tunnel protection (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 IP sec 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).

After completing the customization of the architecture, user clicks on submit button(29), and the application detects and delivers commands to the equipment, if the equipment is not available, the application generates a compressed file containing the configuration of each device, these files can be sent later manually by the user (refer to FIG.9)

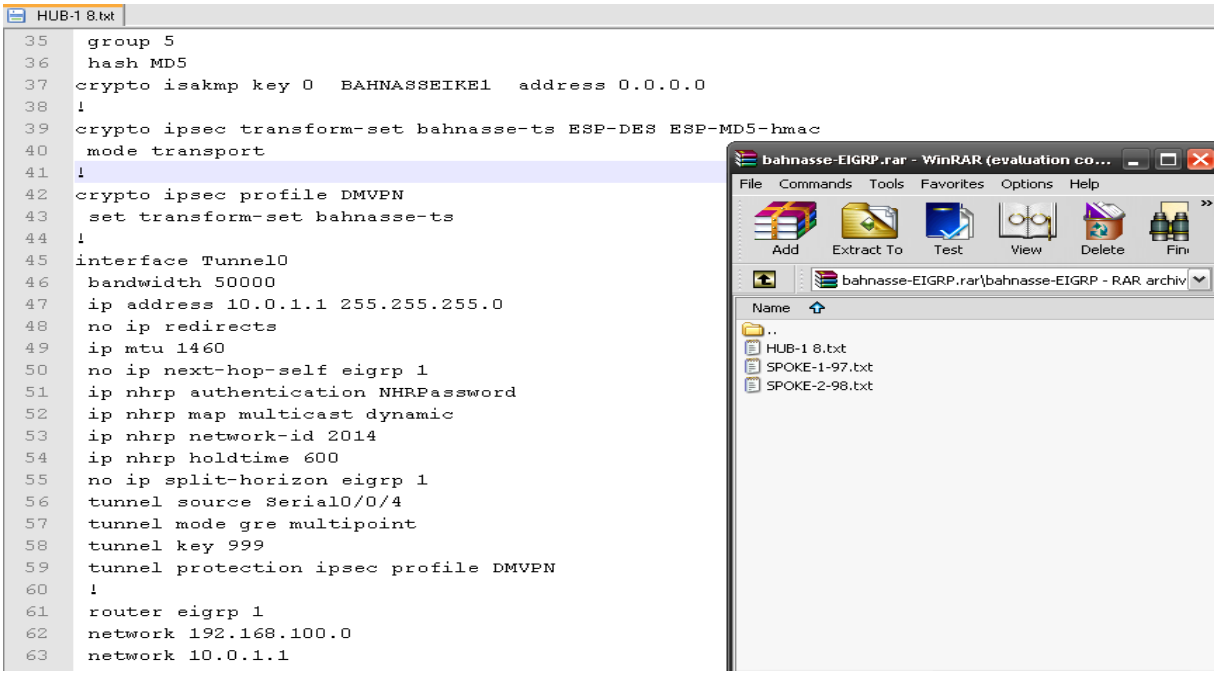

Figure 9 : Configurations files generated

V. Conclusion

In this article we presented our model« DMVPN Security Management System », although the big amount of work addressed only to the management of IP VPN Site to Site network, this model addresses the issue of centralized management of secure dynamic and multipoint VPN through a simple web-based GUI, we discussed the components of the model and its operation and presented the tool via a demonstration.

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 for manual set up of this architecture is an hour, we moved that to five minutes with our model, in addition to time effectiveness the margin error is null.

References Références Referencias

1. Bhaskaran, S., Desai, S., Jou, L., & Matthews, A. R. (2007). U.S. Patent No. 7,263,106. Washington, DC: U.S. Patent and Trademark Office.
2. Chase, C. J., Holmgren, S. L., Medamana, J. B., &Saksena, V. R. (2001). U.S. Patent No. 6,188,671. Washington, DC: U.S. Patent and Trademark Office.
3. Dynamic Multipoint VPN (DMVPN) Design Guide, Corporate Headquarters Cisco Systems, Inc. 2006, 104 p
4. 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.
5. 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.
6. 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.
7. 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.
8. Hanks, S., Meyer, D., Farinacci, D., &Traina, P. (2000). Generic routing encapsulation (GRE).
9. Kent, S., & Atkinson, R. RFC 2401: Security architecture for the Internet Protocol, November 1998. Obsoletes RFC1825 [Atk95a]. Status: PROPOSED STANDARD.
10. Kent, S., & Atkinson, R. (1998). RFC 2406,". Encapsulating Security Protocol.
11. Kent, S., Atkinson, R., & Header, I. A. (1998). RFC 2402.IP Authentication Header.
12. Adoba, B., & Dixon, W. (2004). RFC 3715–IPSec-network address translation (NAT) compatibility requirements.
13. Baek, S. J., Jeong, M. S., Park, J. T., & Chung, T. M. (2000, April). Policy-based hybrid management architecture for IP-based VPN.In NOMS (pp. 987-988).
14. Guo, X., Yang, K., Galis, A., Cheng, M. X., Yang, B., & Liu, D. (2003, April).A policy-based network management system for IP VPN.In Communication

Technology Proceedings, 2003.ICCT 2003.International Conference on (Vol. 2, pp. 1630-1633).IEEE.

15. Ardissono, L., Felfernig, A., Friedrich, G., Goy, A., Jannach, D., Petrone, G., ...&Zanker, M. (2003). A framework for the development of personalized, distributed web-based configuration systems. Ai Magazine, 24(3), 93.
16. MAY, Robert A. Policy-based configuration of internet protocol security for a virtual private network. U.S. Patent Application 13/461,433, 1 mai 2012.