Available online at www.sciencedirect.com

ScienceDirect

IFAC-PapersOnLine 49-29 (2016) 144–147

Enterprise Integration, Networking and Virtual Communications

Besnik Qehaja * Ardian Bajraliu **
Ahmet Shabani * Edmond Hajrizi ******

** Computer Science Department, University for Business and Technology UBT,*
Prishtina, Kosova (e-mail: besnik.qehaja@ubt-uni.net).
*** Computer Science Department, University for Business and Technology UBT,*
Prishtina, Kosova (e-mail: ab32809@ubt-uni.net).
**** Computer Science Department, University for Business and Technology UBT,*
Prishtina, Kosova (e-mail: ametshabani@gmail.com).
***** CEO and Founder, University for Business and Technology UBT,*
Prishtina, Kosova (e-mail: e.hajrizi@ubt-uni.net).

Abstract: In this publication, I have chosen an important field in Computer Networks which is DMVPN (Dynamic Multi VPN). Each institution that uses the Internet as a service, should use VPNs for secure communications.

Our internal internet communications is always at risk, so we have to prevent and secure this gap in our communications. For that reason to prevent and to escape being a target or losing information and sensitive documents, I will present some of the main problems that are in the moment, using Private VPN and advantages of using Dynamic Multi VPN (DMVPN) in our private and public communications.

Keywords: Integration, Networking technologies, Virtual Communications, DMVPN

1. INTRODUCTION

Today's businesses have many subsidiaries in many locations and they all need a secure communication. For offering secure services, DMVPN allows secure networks to exchange data between sites without the need to pass traffic through an organizations headquarter virtual private network VPN (DMVPN 2006 Cisco Systems) server or router.

VPNs traditionally connect each remote site to the headquarters (They are centralized). Using DMVPN essentially creates a mesh VPN topology. This means that each site (spoke) can connect directly with all other sites, no matter where they are located.

Every serious business generates data that needs to be analyzed sent, received, managed, and mostly trusted and secured. The year 2015 was the year of data breaches, many organizations got penetrated, business lost their and customers money and assets, many breaches also resulted with employee and custommer damages with data exposure and this trend is evolving very much. Those breaches are the reason that this paper is mainly focused in the security aspects of networking and software.

This publication explains some new methods and best practices which every enterprise business should implement to ensure enhanced security on communication over their remote location offices and it covers detailed analysis of the advantages of using secure DMVPN and comparison between the VPN and DNMVP.

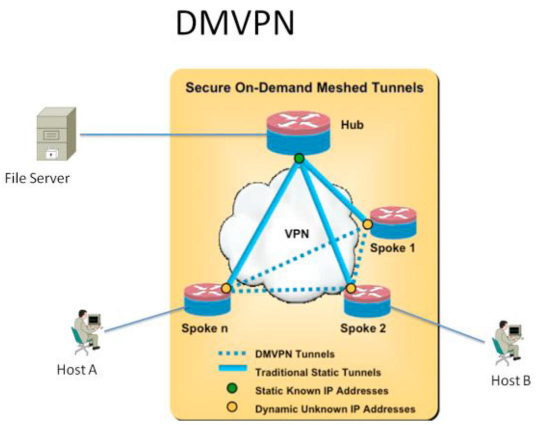
DMVPN
Secure On-Demand Meshed Tunnels
Hub
File Server
VPN
Spoke 1
Spoke n
Spoke 2
Host A
Host B
DMVPN Tunnels
Traditional Static Tunnels
Static Known IP Addresses
Dynamic Unknown IP Addresses

Fig. 1. DMVPN: The visual overview of a network.

2. PROBLEM STATEMENT

2.1 Concepts

The domain of Enterprise integration research has been developed since 1990's as the extension of Computer Integrated Manufacturing (CIM). Enterprise integration research usually done out in two main areas: enterprise modeling and Information Technology (IT). The notion of Enterprise Integration is understood in the frame of enterprise modeling refers to a set of concepts and approaches such as for example the definition of a global architecture of the

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.11.090

system, the consistency of system-wide decision making (Brad Edgeworth 2014).

2.2 Evolutions

A dynamic multipoint VPN improves scaling for hub-and-spoke networks by allowing IPsec tunnels to be dynamically added as needed, without configuration. This greatly simplifies hub configuration and reduces the need for IP address space. In addition, after the hub-and-spoke network has been dynamically built out (Lammle, Todd 2015), network spokes can learn to communicate directly with each other thereby reducing the burden on the hub.

DMVPN fixes many gaps that existed before on networks, but now this new technology is the best practice to ensure real time communication and higher security for enterprise businesses in one package.

2.3 MGRE

The Generic Routing Encapsulation (GRE) protocol provides a simple general purpose mechanism for encapsulating packets from a wide variety of network protocols to be forwarded over another protocol. In DMVPN, GRE encapsulates IP packets and transports them over VPN tunnels (Keith Barker 2012). An example is multicast routing advertisements, which are multicast. IPsec, which is a standard mechanism for providing security on IP networks, cannot encrypt multicast packets. However, multicast packets can be encapsulated within a GRE tunnel and then routed over a VPN connection, so that the encapsulated packets are protected by the IPsec tunnel.

2.4 NHRP

To build the dynamic tunnels, mGRE uses the Next Hop Resolution Protocol (NHRP)addressing service. The hub router maintains a NHRP database, acting as a route server. Spoke routers register their public IP addresses with the hub, acting as clients (Ruixi Yuan, 2001). The spokes query the hub database to obtain the IP addresses of the logical tunnel endpoints.

2.5 IPsec

In DMVPN, tunnels are secured using the IP Security (IPsec). IPsec is a suite of protocols that protect the network communication at the Layer 3 which is the network layer of the OSI model in which the IP protocol is part of it (Michael Stewart 2010). As described in figure 2, IP sec is configured between the two routers which operate on the given tunnel0 and flow all their data through this secure tunnel further on.

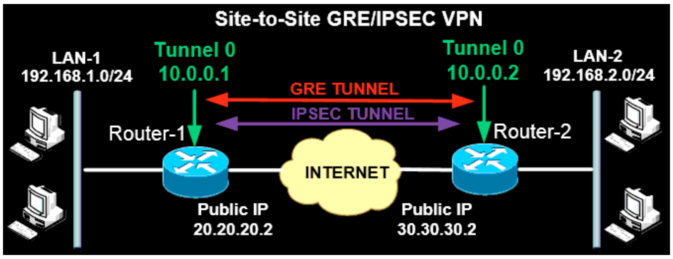

Fig. 2. IPsec: Implementation on the network.

2.6 Routing

DMVPN uses a dynamic routing protocol to advertise the private networks within the DMVPN network. Supports the Routing Information Protocol (RIP),Open Shortest Path First (OSPF), andthe Border Gateway Protocol (BGP) (Larry L. Peterson 2011).

3. PREREQUISITES AND HUB-SPOKE EXPLANATION

The examples given in this part have some elements in common:

•Any Ethernet interface to be used must already be configured with proper IP addressing like given on figure 3, and interface configurations. The examples do not show Ethernet interface configurations.

•Loopback or Ethernet interfaces are typically configured as tunnel endpoints. Configuring a loopback interface as the tunnel endpoint is advantageous in systems in which there are multiple paths between tunnel endpoints. If the endpoint is the loopback interface, the tunnel does not fail if an Ethernet interface fails.

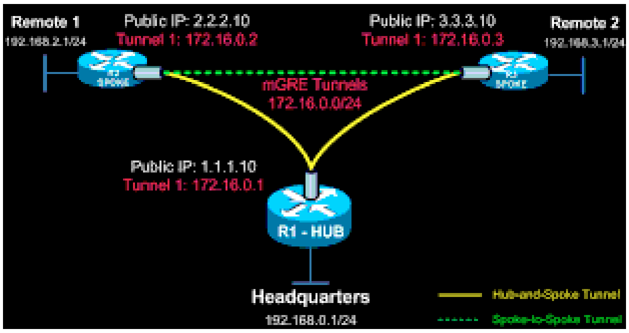

Fig. 3. mGRE: Solutions on tunnels.

3.1 Overview

The basic mGRE tunnel environment is not protected by IPsec encryption, which means they are not secure and would not be suitable for a production network unless otherwise secured. DMVPN uses mGRE, NHRP, and IPsec to provide a secure hub-and-spoke tunnel environment to protect information flowing into that line of communication. This section presents the model which is required to properly secure the networking flow environment and provide a complete DMVPN solution regarding information security.