International Conference on Applied Internet and Information Technologies, 2016 DOI:10.20544/AIIT2016.25

Virtual Private Network Implementation with GRE Tunnels and EIGRP Protocol

Tihomir Stojchevski, Tome Dimovski and Nikola Rendevski

Faculty of information and communication technologies, Partizanska bb, 7000 Bitola, Macedonia
stojcevski@gmail.com, {tome.dimovski, nikola.rendevski}@fikt.edu.mk

Abstract. Nowadays, the modern companies and institutions have a inevitable need for secure connections with remote locations trough broadband WAN networks. The reason for such requisite is mainly the need for shared services utilization like application servers, database servers, messaging servers, etc., physically located at remote datacenters. In this paper, we present realistic VPN implementation and configuration for a company with two central locations (head office and warehouse) and branch offices in several cities. For secure communication between central locations and branch offices, Generic Routing Encapsulation (GRE) tunnels are implemented. EIGRP protocol is used for routing the data between networks. From the implementation analyses conducted in this paper, we can figure out that this approach allows low-complexity realization and low-cost maintenance solution.

Keywords: computer network, virtual private network, routing.

1. Introduction

Establishing network communication between more commercial entities located in different geographical locations, becomes a inevitable operation in contemporary enterprises. The early VPNs (virtual private networks)[1] used for connecting remote sites were realized by special types of connections like peer-to-peer (P2P), multiprotocol label switching (MPLS), that fall into the category of very expensive lines [2]. Today, the most prevalent method of connection is through the Internet.

In this paper we present VPN implementation and configuration for a key customer company with two main locations in Skopje (HQ Office and Warehouse) and remote branch offices located in several cities throughout the country. The customer need is to deal with frequently network topology changes, i.e., opening temporary branch offices with short time of usage (few days only), but without daily routing configuration changes which is usually practice in implementations where static-routing complex networks are designed.

Starting from specific company needs for quality of service (QoS), we decide to build network based on two most popular methods today, Generic Routing

Encapsulation (GRE) tunneling [3] for establishing VPN connections between HQ offices and branches, and Cisco Enhanced Interior Gateway Routing Protocol (EIGRP) [4-5] to automate the routing decisions and configuration for all networks that will exist within the company.

The paper is organized as follows. Section 2 gives a survey of tunneling and EIGRP routing protocol. In Section 3 we present VPN implementation and configuration for the key costumer company, and finally, in Section 4 discussion and conclusions are drawn.

2. Tunneling and EIGRP routing protocol

2.1. Tunneling

In the computer networks, a **tunneling protocol** allows a network user to access or provide a network service that the underlying network does not support or provides directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol, in example, running IPv6 over IPv4. Another important use is providing services that are impractical or unsafe to be offered using only the underlying network services. In example, providing a corporate network address to a remote user whose physical network address is not part of the corporate network. Tunneling involves repackaging the traffic data into a different form to hide the nature of the traffic that is passing through the tunnels.

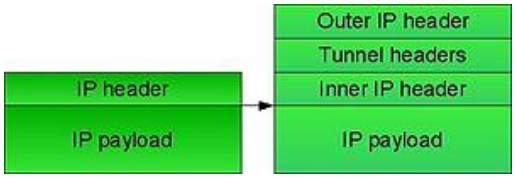

Fig. 1. IP Tunneling encapsulation – IP packet before and after tunnel encapsulation

Tunneling protocol encapsulates each packet, including the address of the source and destination IP network, and the new package is part of the transmition network. For the border areas between the original and the transmission network, as well as transport and destination network, intermediate routers are used for establishing endpoints of the IP tunnel through the transmission network. Thus, endpoints of the tunnel provide route for normal IP communication between source and destination network.

IP tunnel "overrides" simpler firewall rules as the addressing of source datagrams are hidden. Encapsulation is developed like tool for tunneling, with purpose of caring any type of protocol from OSI layer 3 level over IP networks. IP Tunnels carry different protocols over IP protocol, provide communication between networks with a limited number of hops, connect physical connectionless networks and allow VPN connections over WAN networks

2.2. Enhanced Interior Gateway Routing (EIGRP) Protocol

EIGRP is a network protocol that allows routers to exchange information with each other more efficiently than current network protocols. EIGRP derived from IGRP (Interior Gateway Routing Protocol), but this is not a compatibility issue during their mutual exchange of routing information because the metrics used within one protocol can be translated to the corresponding metrics of the second protocol.
Router using EIGRP protocol, has a copy of the routing tables of its neighbors (routers). If it is not able to find a suitable route in these tables, addresses a request for information for that route to its neighbors, which still turns to their neighbors, until the required route is not found.

When the contents of one routing table is changed (adding or removing some network segments), that router sends information to its own neighbors only for the occurred change. Some of the earlier routing protocols had "bad" practice for exchanging the entire routing tables. Therefore, the actual state of each router was detected by sending "hello" packets across the network. The router from which the "hello" packet is not received in a certain time, will be considered as unreachable and its routing table is deleted at its neighbors. EIGRP protocol use Diffusing-Update Algorithm (DUAL) for detecting most effective routes (with smaller cost path) to some location. The information about the final status of routing tables, used by DUAL algorithm is to learn the lowest-cost path (loop-free).

EIGRP protocol does not use TCP or UDP protocols which means that port number for identifying type of traffic is not in use. Instead of this, it is designed to work on the top on the level 3 from IP protocol. Because it does not use TCP for communication, it implements Cisco Reliable Transport (RTP) to secure that EIGRP updates will be delivered to all of the neighbors. EIGRP is often considered as a hybrid protocol because it also sends link state updates when the link states change.

Some of the key EIGRP operational characteristics include:

- Full support for Classless Inter-Domain Routing (CIDR) and variable length subnet masking. Routes are not summarized at the classful network boundary unless auto summary is enabled.
- Support for load balancing on parallel links between sites.
- The ability to use different authentication passwords at different times.
- MD5 authentications between two routers.
- Sends topology changes, rather than sending the entire routing table when a route is changed.
- Periodically checks if a route is available and propagates routing changes to neighboring routers if any changes have occurred.
- Backwards compatibility with the IGRP routing protocols.

3. VPN implementation for the key customer with GRE Tunnels and EIGRP Protocol

On Fig. 2, network topology for a key customer company is depicted, with two main locations in Skopje (HQ Office and Warehouse) and remote branch offices located in

several cities throughout the country.

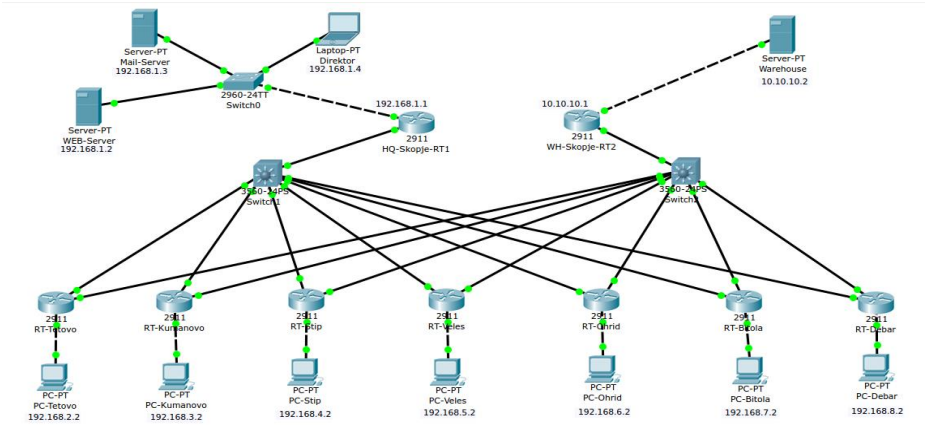

Fig. 2. Network topology for the key customer company

At the central location (HQ-Skopje-RT1) we have installed Cisco 2911 router, Cisco 2960 switch, WEB/SQL server and e-mail server - all connected in one Local Area Network (LAN) segment. The Cisco 2911 router has the role of HUB router that keeps connection with so-called spoke routers form the remote offices. At the second central location (Warehouse) we have installed Cisco 2911 router, Cisco 2960 switch and FTP server - connected in the same LAN segment.

The WAN interfaces on the Cisco 2911 routers (HQ-Skopje-RT1 and HQ-Skopje-RT2) are the destination points for all GRE tunnels, configured with IP addresses from the transport network (172.30.30.1 and 172.40.40.1).

On each spoke router (Cisco 2911) in branch offices, we configured two WAN interfaces, used to separate the communication in the same transport network, with the HUB routers at the central location. For each spoke router we implemented tunnel interfaces for GRE connections to each HUB router in the central location. We configured IP addresses from tunneling pools as 172.16.16.0 and 172.17.1.0.

After configuration of the VPN network, the next phase is exchanging the routing information between routers about local network pools using EIGRP pre-defined area 20. From that moment, all of the network elements which uses private LAN networks (192.168.0.0 and 10.10.10.0) are reachable trough transport network. Main parts of the network configuration is shown in the next section.

3.1. Network configuration

Table 1. Central office addressing scheme

Host/Device	IP address
Cisco 2911	192.168.1.1
WEB server	192.168.1.2
Mail server	192.168.1.3

Table 2. Warehouse addressing scheme

Host/Device	IP address
Cisco 2911	10.10.10.1
FTP server	10.10.10.2

Table 3. List of the addressing scheme on remote locations (branches)

Location	IP Network
Tetovo	192.168.2.0/28
Kumanovo	192.168.3.0/28
Shtip	192.168.4.0/28
Veles	192.168.5.0/28
Ohrid	192.168.6.0/28
Bitola	192.168.7.0/28
Debar	192.168.8.0/28

Table 4. Major coniguration blocks on HUB 1 router

Cisco 2911 RT-1 (Headquarter)	HUB 1
interface Tunnel0 ip address **172.30.30.1** 255.255.255.240 tunnel source GigabitEthernet0/0	MultiGRE tunnel 0 source IP address
interface GigabitEthernet0/0 description LAN ip address **192.168.1.1** 255.255.255.248	Local LAN interface
interface GigabitEthernet0/1 description WAN ip address **172.16.1.1** 255.255.255.240	WAN interface (tunnel 0 destination IP for spoke Routers)
router eigrp 20 network **172.30.30.0** 0.0.0.15 network **172.16.1.0** 0.0.0.15 network **192.168.1.0** 0.0.0.7	EIGRP sends updates for this networks from HUB-1 router

Table 5. Major coniguration blocks on HUB 2 router

Cisco 2911 RT-2 (Warehouse)	HUB 2

interface Tunnel0 ip address **172.40.40.1** 255.255.255.240 tunnel source GigabitEthernet0/0	MultiGRE tunnel 0 source IP address
interface GigabitEthernet0/0 ip address **10.10.10.1** 255.255.255.248	Local LAN interface
interface GigabitEthernet0/1 description WAN ip address **172.17.1.1** 255.255.255.240	WAN interface (tunnel 0 destination IP for spoke Routers)
router eigrp 20 network **172.40.40.0** 0.0.0.15 network **172.17.1.0** 0.0.0.15 network **10.10.10.0** 0.0.0.7	EIGRP sends updates for this networks from HUB-1 router

Table 6. Major coniguration blocks on SPOKE routers

RT-Bitola (Branch office)	Spoke router
interface **Tunnel0** ip address **172.30.30.5** 255.255.255.240 tunnel source GigabitEthernet0/1 tunnel destination **172.16.1.1**	GRE tunnel source and destination IP addresses for connection with HUB-1
interface **Tunnel1** ip address **172.40.40.5** 255.255.255.240 tunnel source GigabitEthernet0/2 tunnel destination **172.17.1.1**	GRE tunnel source and destination IP addresses for connection with HUB-2
interface GigabitEthernet0/0 ip address **192.168.5.1** 255.255.255.248	LAN interface IP
interface GigabitEthernet0/1 ip address **172.16.1.5** 255.255.255.240	WAN interface IP
router eigrp 20 network **172.30.30.0** 0.0.0.15 network **172.40.40.0** 0.0.0.15 network **172.17.1.0** 0.0.0.15 network **192.168.5.0** 0.0.0.7	EIGRP sends updates for this networks from RT-Bitola spoke router

4. Conclusion

In this paper we presented VPN network implementation and configuration for company with two central locations in Skopje (head office and warehouse) and branch offices in several cities. GRE tunneling was used as a secure solution for secure

communication between central locations and branch offices. We used EIGRP dynamic routing protocol for routing the data between networks. Using such approach, low-cost and low-complex solution is presented completely meeting the company needs and fulfilling the QoS requirements, while providing solution for the dynamic topology without routing configuration changes.

5. References

1. Andrew, M.: Cisco Secure Private Networks. Cisco Press. (2001)
2. Stuart, D. F.: A CCIE v5 guide to Tunnels, DMVPN, VPNs and NAT (Cisco CCIE Routing and Switching v5.0) (Volume 3), 13-32. (2015)
3. Point-to-Point GRE over IPSec Design Guide. Cisco System, San Jose, USA. (2006)
4. Jeff, D., Jennifer, C.: Routing TCP/IP, Volume 1 (2nd Edition), 297 – 315. (2005)
5. Diane, T., Bob, V., Rick, G.: Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: (CCNP ROUTE 300-101), 576-582. (2015)