Analytical performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP.

Faycal Bensalah[†], Najib El Kamoun[†] and Ayoub BAHNASSE[††]

[†]lab. STIC, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco
[††]lab. LTI, Faculty of Sciences Ben M'SIK, University Hassan II, Casablanca, 9167 Morocco

Summary
With the proliferation of computer attacks and the sophistication of tools threatening data availability, network infrastructure security has become one of the most critical and challenging tasks. Virtual Private Network (VPN) technology allows two or more remote sites to be securely connected across an infrastructure, which is often publicly shared, such as the Internet.

VPN technology is increasingly used by most companies because of its multiple advantages, but the latter influences the quality of the traffic carried. In this paper we will (i) study and measure the impact of different network layer VPN technologies on Voice over IP performance. (Ii) Determine the scalability of each technology with the load rise of the packets.

The study was carried out under GNS3, simulating the different VPN technologies: GRE, IPsec, GRE over IPsec, DMVPN, and DMVPN protected by IPsec.

Key words:
VPN, IPsec, GRE, DMVPN, GNS3, Scalability, VOIP.

1. Introduction

The distribution of data at multiple sites or the distribution of sites are two paradigms that most companies are increasingly tending. These strategies are justified by its multiple advantages, in particular in terms of data availability and decentralization of backup plans. However, the intermediate network through which these operations are carried out is often the Internet. No one can deny that this Internet network offers no mechanism of confidentiality, integrity or authentication.

VPN technology is a solution for interconnecting remote sites across a shared public infrastructure. This technology relies on several protocols, some of which offer no security mechanism but encapsulate all types of messages (Unicast, Multicast, Broadcast or Anycast), such as the Generic Routing Encapsulation (GRE) or multipoint protocols GRE (mGRE). Other protocols offer the three basic security features but encapsulate only Unicast messages such as IPsec. Combining the two protocols remains feasible.

The VPN technology until the last years, was static, not scalable and not modular. With the massive expansion of the number of sites, the interconnection task becomes tedious, costly and difficult to manage subsequently. As an alternative, vendors have proposed technologies that allow rapid and modular deployment of VPN technology across multiple sites while ensuring scalability. As an example, the Auto Discovery VPN (ADVPN) [1], Dynamic Smart VPN (DSVPN) [2] and Dynamic Multipoint VPN (DMVPN) [3].

The above-mentioned VPN technologies serve primarily as data carriers. The real question most researchers have asked is mainly about the cost of these technologies on the performance of applications being transported. Several research work has been carried out to evaluate the performances of the applications transported in the VPN networks, according to our research no scientific work has been proposed evaluating the scalability of each technology taking into account the VOIP as transported flow.

Through the present study we will study in a succinct manner the different VPN technologies through the second section. In the third section we will present the related works and our motivations. The presentation of the testbed network and the discussion of the results obtained will be devoted respectively to the fourth and fifth sections. We will conclude in the last section.

2. VPN Technologies

As mentioned earlier, VPN is a technology allowing the interconnection of two or more remote sites through an infrastructure, which is often public shared, such as the Internet.

We will see in this section the different tunneling protocols GRE, IPsec, GRE over IPsec and DMVPN.

2.1 GRE

The generic routing encapsulation (GRE) [4] described in RFC 2784 (previously obsolete RFC 1701 and 1702) is a communication protocol used to establish a direct point-to-point connection between gateways. Being a

Manuscript received April 05 ,2017.
Manuscript revised April 20 ,2017.

simple and efficient method of transporting data over a public network, like the Internet, GRE allows two peers to share data that they could not share on the public network directly.

In addition, GRE tunnels can encapsulate multicast data streams for Internet transmission. The GRE protocol offers a number of advantages, including:

1. Connection of non-contiguous subnets
2. Being less demanding of resources than its alternatives (IPsec VPN)
3. Support Unicast, Multicast and broadcast messages
4. Can encapsulate any layer 3 protocol [5].

Fig.1. shows an example of GRE encapsulation

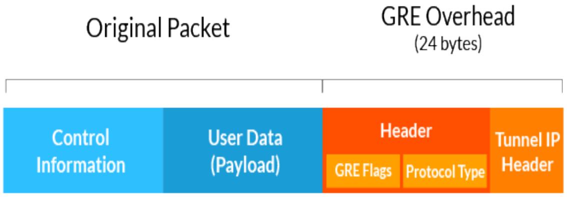

Fig. 1 GRE encapsulation

With a tunnel in place, a GRE packet can travel directly between the two ends. Even when the packet traverses other routers, there is no interaction with its payload (Fig.2).

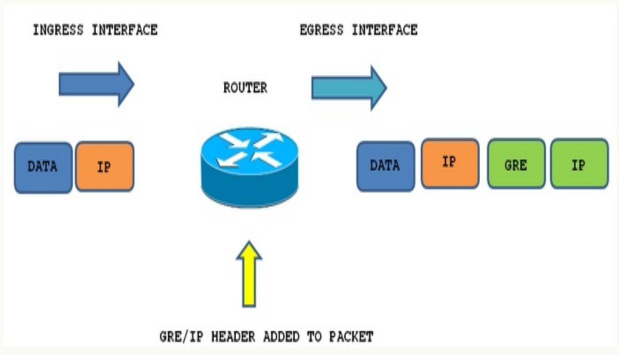

Fig.2 GRE Packet Forwarding

Encapsulation process of GRE packet as it traversers the router and enters the tunnel interface

You might use GRE in the following situations:

- Connect networks that are running non-IP protocols, such as native LAN protocols, across the public IP network. Non-IP protocols, such as Novell IPX or Appletalk, are not routable across an IP network. A GRE tunnel allows you to create a virtual point-to-point link between two such networks over the public WAN.
- Route IPv6 packets across an IPv4 network, or connect any two similar networks across an infrastructure that uses different IP addressing.
- Encrypt multicast traffic. 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.

2.2 IPsec VPN

IPsec (Internet Protocol Security) was developed by the Internet Engineering Task Force (IETF) as an end-to-end mechanism to ensure data security in IP communications. IPSec has been defined in a series of RFCs, including RFCs 1825, 1826 and 1827, which define the overall structure, an authentication header ensuring the integrity and confidentiality of the data.

IPSec defines two functions that ensure confidentiality: encryption and data integrity. As defined by the IETF, IPSec uses an Authentication Header (AH) [6] to ensure authentication and integrity of the source without encryption, and ESP [7] (Encapsulated Security Payload) to ensure authentication And integrity with encryption.

IPsec operates in two modes:

- Transport mode: In this mode, IP packets are secured between two end devices. Only the payload is concerned by the processing and the IP packet header is preserved to allow the routing to operate seamlessly.
- Tunnel mode: In this mode, IP packet exchanges are secure from network to network. The entire IP packet (header + payload) is encapsulated and a new IP packet header is created.

Table 1 describes encapsulation of both ESP and AH protocols on tunnel and transport mode

Table 1. IPsec encapsulation

Protocol	**Transport mode**	**Tunnel mode**
AH	IP AH data	IP AH IP data
ESP	IP ESP data ESP-T	IP ESP IP data ESP-T
AH+ESP	IP AH ESP data ESP-T	IP AH ESP IP data ESP-T

2.3 Protected GRE

IPsec can encapsulate only unicast traffic. This is an essential criterion to consider when choosing a VPN solution. In the context of this paper, we are apparently facing a serious problem given that all exchanges between dynamic routing protocols bodies are multicast. Fortunately, there is a solution: the GRE tunnel.

GRE tunnels can overcome the limitation of unicast traffic.

In order to achieve high security level, GRE + IPsec can be used, with tunnel mode, without restriction on the nature of the traffic conveyed.

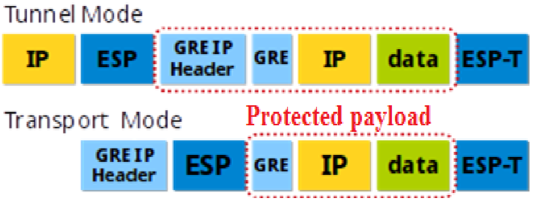

Fig. 3 Protected GRE

In the above representation, the GRE IP Header field corresponds to the IP header introduced by the use of the GRE tunnel.

Using tunnel mode involves encapsulating an additional IP header that penalizes the payload space.

2.4 DMVPN

Dynamic Multipoint VPN (DMVPN) is a Cisco IOS Software solution for building scalable IPsec Virtual Private Networks (VPNs). Cisco DMVPN uses a centralized architecture to provide easier implementation and management for deployments that require granular access controls for diverse user communities, including mobile workers, telecommuters, and extranet users.

DMVPN allows branch locations to communicate directly with each other over the public WAN or Internet, such as when using voice over IP (VOIP) between two branch offices, but doesn't require a permanent VPN connection between sites. It enables zero-touch deployment of IPsec VPNs and improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

Among the benefits of DMVPN technology are:

• Lowers capital and operational expenses -- Reduces costs in integrating voice, video with VPN security

• Simplifies branch communications -- Enables direct branch-to-branch connectivity for business applications like voice

• Reduces deployment complexity -- Offers a zero-touch configuration, dramatically reducing the deployment complexity in VPNs

• Improves business resiliency -- Prevents disruption of business-critical applications and services by incorporating routing with standards-based IPsec technology

A Dynamic Multipoint VPN is an evolved iteration of hub and spoke tunneling (note that DMVPN itself is not a protocol, but merely a design concept). A generic hub and spoke topology implements static tunnels (using GRE or IPsec, typically) between a centrally located hub router and its spokes, which generally attach branch offices. Each new spoke requires additional configuration on the hub router, and traffic between spokes must be detoured through the hub to exit one tunnel and enter another. While this may be an acceptable solution on a small scale, it easily grows unwieldy as spokes multiply in number.

DMVPN offers an elegant solution to this problem: multipoint GRE tunneling. Recall that a GRE tunnel encapsulates IP packets with a GRE header and a new IP header for transport across an untrusted network. Point-to-point GRE tunnels have exactly two endpoints, and each tunnel on a router requires a separate virtual interface with its own independent configuration. Conversely, a multipoint GRE tunnel allows for more than two endpoints, and is treated as a non-broadcast multi-access (NBMA) network.

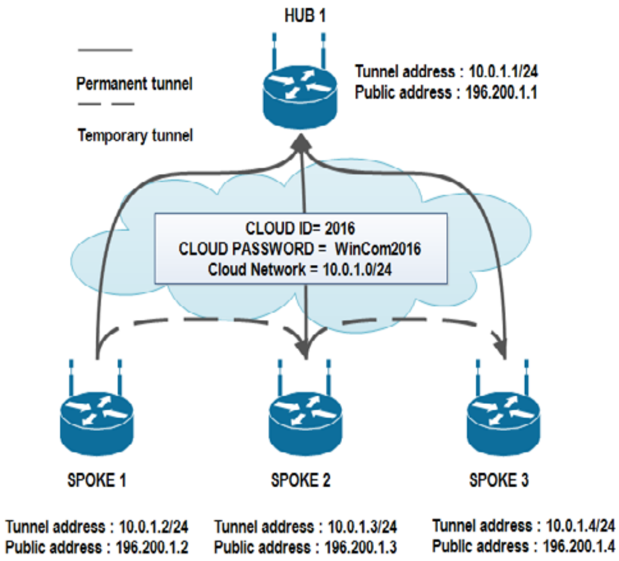
HUB 1
Permanent tunnel
Temporary tunnel
Tunnel address : 10.0.1.1/24
Public address : 196.200.1.1
CLOUD ID= 2016
CLOUD PASSWORD = WinCom2016
Cloud Network = 10.0.1.0/24
SPOKE 1
SPOKE 2
SPOKE 3
Tunnel address : 10.0.1.2/24
Public address : 196.200.1.2
Tunnel address : 10.0.1.3/24
Public address : 196.200.1.3
Tunnel address : 10.0.1.4/24
Public address : 196.200.1.4

Fig. 4 DMVPN network example

DMVPN relies mainly on Next Hop Resolution Protocol [8] (known as NHRP) protocol to create dynamic tunnels. NHRP is a NBMA of client-server architecture, allowing to record clients, usually spokes by the server which often is the HUB. The HUB's NHRP cache dynamically filled in multicast by tunnel and public addresses of each client of its group. To communicate with each other, the Spokes consult HUB cache to determine the public address of the destination.

2.5 Cisco IOS IP SLA Flow generator

IP SLA is a tool used as a traffic generator. We'll do some calculations. Imagine that we want to send 16 kbps of traffic from one router to another on Ethernet. How many packets should we send and what should be the payload size?

Here is an example of a frame, an Ethernet header has 14 bytes, IP is 20 bytes and UDP is 8 bytes.

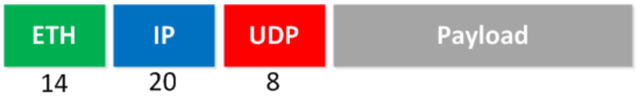

Fig. 5 Ethernet Header

First we will calculate total frame size, the appropriate formula is: Total frame size = L2 header + L3 header + L4 header + payload. Routers will be connected using Ethernet so that's 14 bytes. IP add another 20 bytes and UDP requires 8 bytes. The reason that we use UDP is that we will configure IP SLA to use UDP jitter. So, 14 + 20 + 8 = 42 bytes, to keep the calculation simple, we will use a payload of 58 bytes so that the total packet will be 42 + 58 = 100 bytes.

We will now calculate bandwidth, the bandwidth is calculated by multiplying frame size with the number of packets. We know our frame size is 100 bytes so how many packets should we send per second? Our goal is to generate 16 kbps of traffic, that's 16.000 bits per second (2000 bytes). This is how we calculate it: Number of packets = Bandwidth / frame size.

Our packet size is 100 bytes and we need 2000 bytes per second to reach 16 kbps, so we must send 20 packets (2000/100) per second with a frame size of 100 bytes to hit 16 kbps.

3. Related Works

Evaluation of virtual private network (VPN) performance is an active area of research. The author [9] carried out a comparative study between the two tunneling protocols IPsec and GRE. The study showed the degradation of performance that this protocol brings to the network level.

The author Eskandar [10-11], on his part, carried out a study evaluating the impact of the GRE VPN layer on the performance of VOIP, the author varied Codecs (G.711 G.723) and Signaling protocols (SIP and H.323). As a result, the study showed that the additional GRE layer degrades the quality of communications relatively. Hence the advantage of deploying Quality of Service mechanisms.

The work proposed by Narayan [12] makes a comparative study between different tunneling protocols PPTP, IPsec, and SSTP in wired and wireless networks. The study was carried out on physical equipment using UDP and TCP traffic as measurement flows. The measurement policy consists of increasing the buffer size while varying the UDP and TCP applications. As a conclusion, the author has shown that the IPsec protocol offers the lowest bit rate and a considerable loss rate compared to other tunneling protocols.

In another study, Mazalek [3] performs an evaluation of VoIP performance in an IPsec secure environment. The author in this work took into consideration the rise in charge in terms of calls. The evaluation was done by increasing the number of calls and varying Codecs. This study made it possible to measure the scalability of each codec in terms of calls.

Works evaluating the performance of DMVPN technology are limited. The works [14-19] discuss the DMVPN architectures and their good configurations in terms of scalability, high availability and quality of service. Nowosielski, through article [20], shows the efficiency of DMVPN technology for mobile users and evaluates its performance by varying encryption protocols (DES, AES and 3DES).

According to our research, no scientific work has been done comparing the various tunneling technologies (GRE, IPsec, IPsec GRE, DMVPN and DMVPN IPsec) in terms of VOIP load. This was for us a motivation to conduct this work under the GNS3 simulator.

4. Presentation of the measurement environment

4.1 Network Testbed

In order to conduct our measurements, we have created a project conforming to Fig.6. The studies were carried out under Graphical Network Simulator GNS3. As background traffic, we used VOIP traffic. For the generation of traffic, we have operated IP SLA.

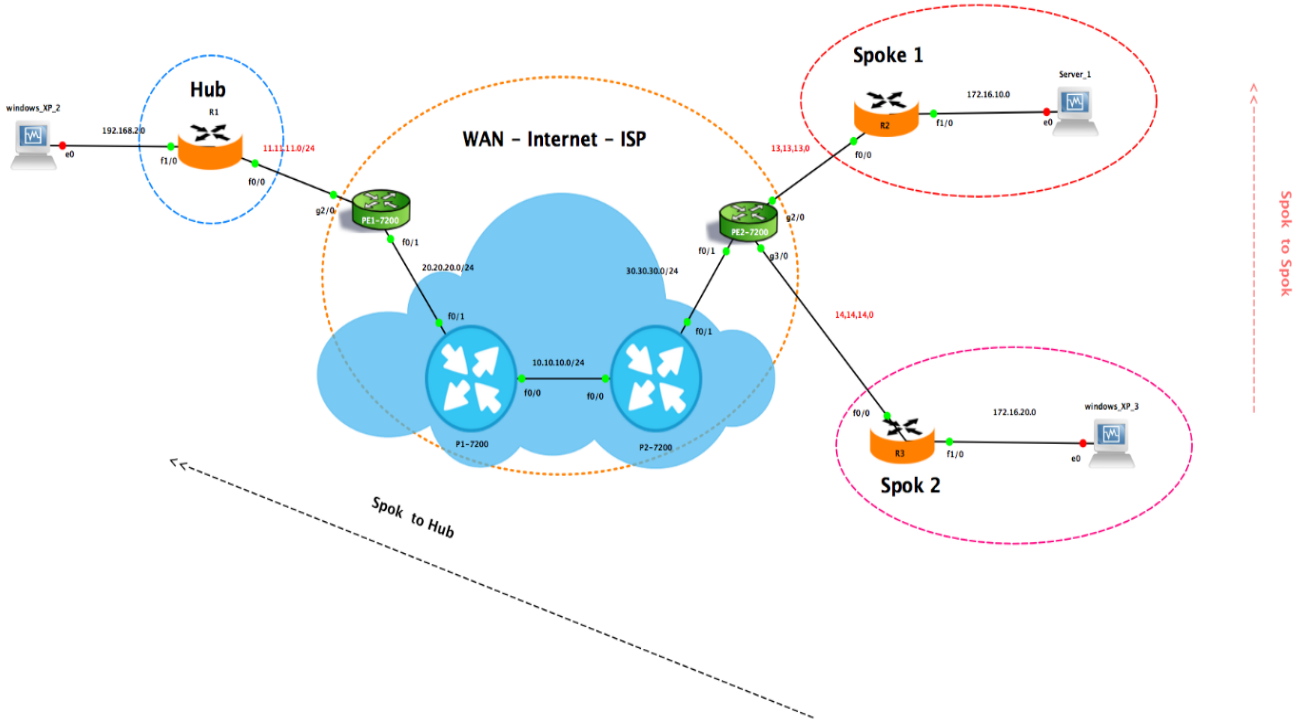

Fig. 6 Network testbed

Based on this project we created 96 different scenarios. For each technology (IP, GRE, IPsec, GRE over IPsec, DMVPN, DMVPN IPsec) we have increased the packet load to the order of 2 ^ n ranging from 64 to 375000.

Gigabit Ethernet technology is used in the backbone of the provider. The link between client sites and vendor borders is performed by Fast Ethernet technology.

4.2 Traffic and Measurement Attributes

Table 1 shows the VOIP application settings.

Table 2. VOIP parameters

Traffic	VOIP
Codec	G.711 silence suppression
Packet interval	20 milliseconds
Number of packets	1000

The evaluation criteria used for the comparison are:

1. Jitter: Jitter is the variation of latency. Packets arrive irregularly depending on network traffic. It is therefore decisive in the case of the VOIP, the greater the jitter increases the conversation becomes rough.
2. Latency: defines the delay of end-to-end transmission of information on the computer network.
3. MOS Score: Meaning Opinion Score, is a scale ranging from 0 to 5 judging the quality of the voice intercepted. This score depends on the codec used, for the G.711 codec (our case), the MOS score is 4.3.
4. Loss of packets: the number of packets rejected compared to packets sent

For scenarios with IPsec, the security associations used in the two IKE phases are:

- Encryption protocol: AES 256
- Integrity Protocol: SHA
- Key length: 1024 bits
- Authentication Method: Pre shared Key
- IPsec protocol: ESP
- IPsec mode: Transport for DMVPN and Tunnel for site to site scenario.

5. Obtained Results and discussion

5.1 Jitter

The results obtained in Fig. 7 represents the jitter in milliseconds of the various VPN technologies taking into account different sizes of the packets.

According to a first reading, the variation of the delays is relatively stable for the scenarios whose IPsec protocol is not deployed. It should be noted that this stability is mainly justified by the non-congestion in the queue caused by (i) the verification processes of both security association and policy databases, (ii) the encryption and integrity control.

The IP and VPN GRE, DMVPN technologies offer lower jitter compared to IPsec. It is true that the jitter obtained in all the scenarios do not exceed the tolerable standards 50 milliseconds. jitter obtained in the DMVPN technology is almost identical to the results of the GRE technology with a small difference due to the process of NHRP resolution.

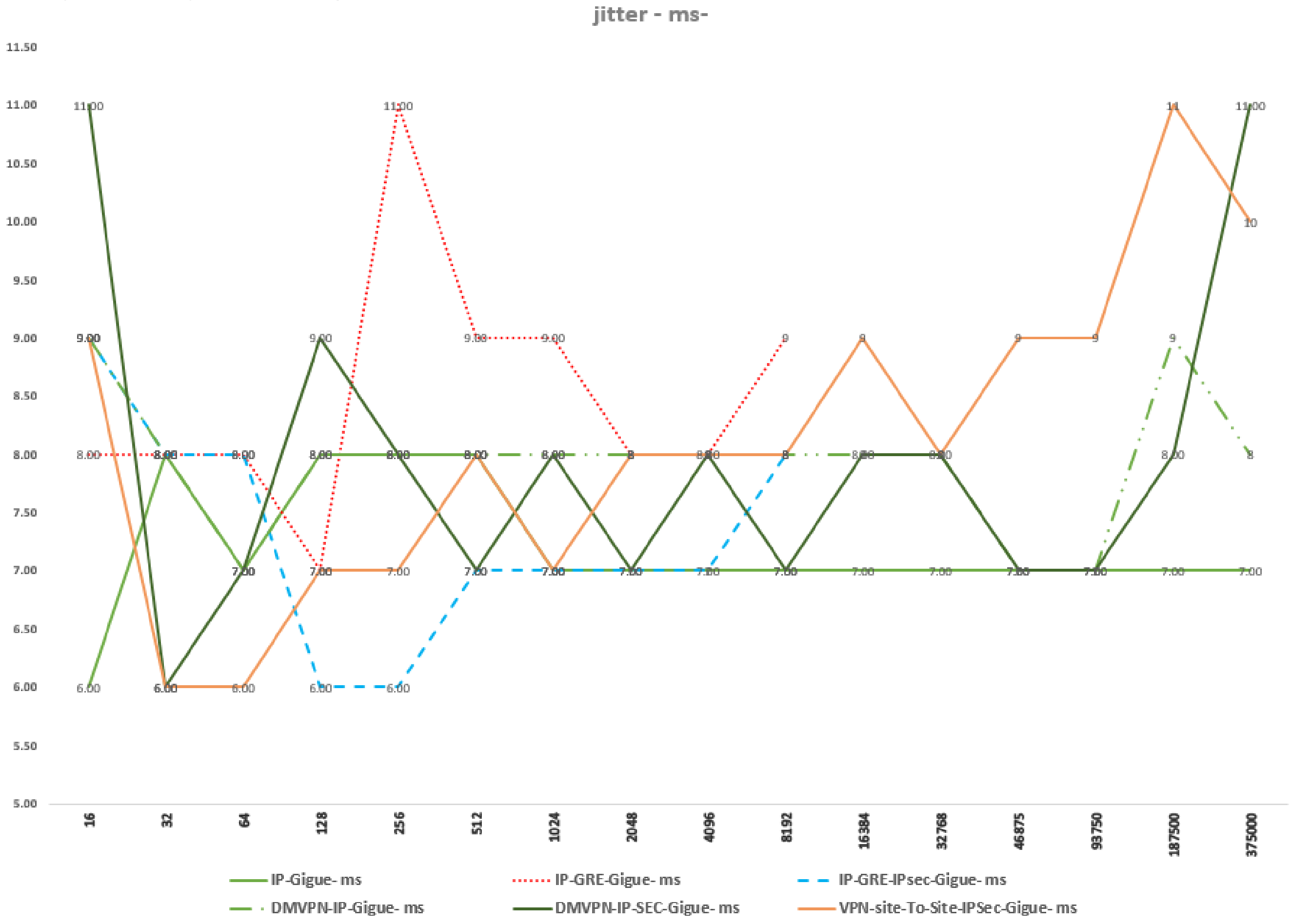

Fig. 7 Jitter

5.2 Loss Rate

Fig.8 shows the loss rate, the results show that the IPsec protocol offers a very low loss rate compared to other scenarios without IPsec. This may seem strange since a first reading, but it should be noted that the IP protocol is considered Best Effort with no retransmission mechanism, so it does not attempt to retransmit the rejected packets. The same logic applies to the GRE or mGRE protocol. It can be seen that the IPsec protocol, alone or combined with GRE, is the most scalable in terms of loss rates.

Taking into account the loss rate only, and knowing that the tolerable threshold is 1%, it is clear that:

- The IP protocol exceeds the tolerable threshold from the 4096-byte scenario.
- VPN GRE exceeds the tolerable threshold from the 256-byte scenario.

- VPN DMVPN exceeds tolerable threshold from scenario 32768 bytes
- All site-to-site IPsec and IPsec-protected DMVPN scenarios are stable for all packet sizes.
- GRE over IPsec exceeds the tolerable threshold from the 1024-byte scenario.

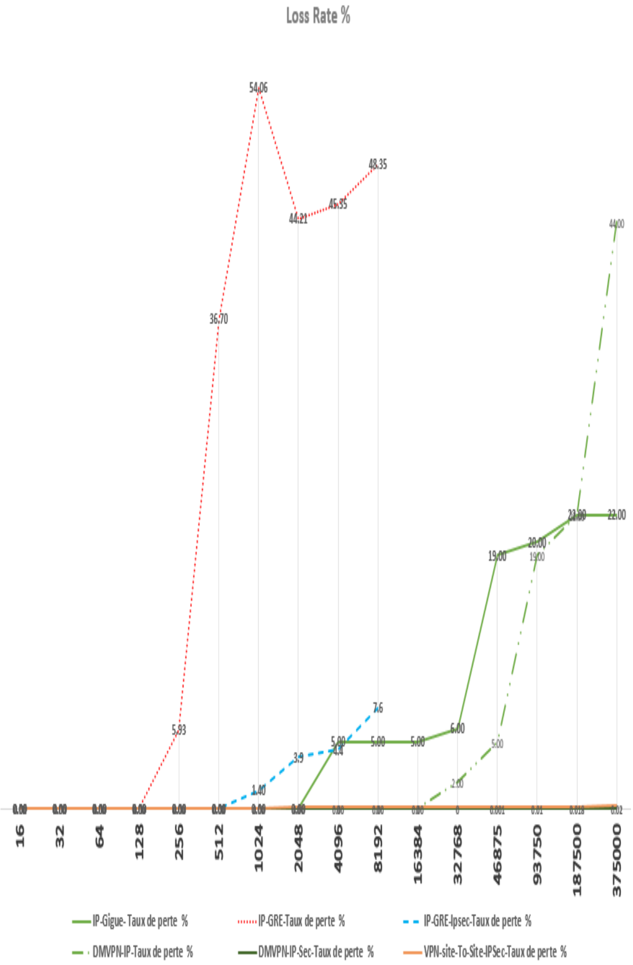

Fig 8. Loss Rate

5.3 Latency

Fig.9 shows latency or end-to-end delay. Unlike loss rate results, the IPsec protocol adds remarkable latency across scenarios compared to other technologies. This is justified by the additional encryption tasks and its costs induced in terms of delay and also by the number of packets transmitted by the IPsec protocol which exceeds those sent by the other technologies.

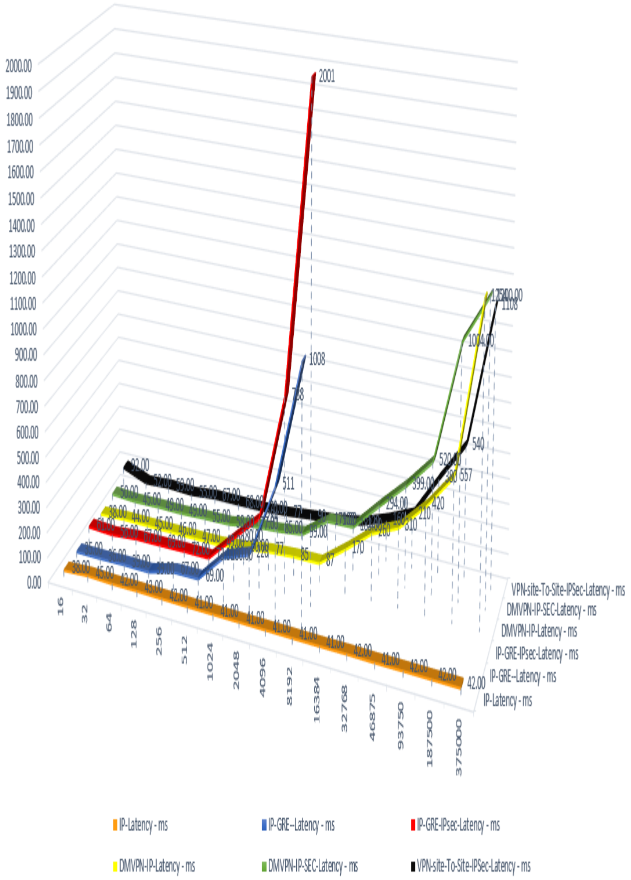

Fig 9. Latency

To judge the scalability of VPN technologies, we must now consider both the loss rate and the latency at the same time. We observe that:

- The IP protocol offers a lower delay in all scenarios, but with the loss rate measured earlier, IP cannot route the VOIP from the 4096 byte load.
- The GRE protocol provides a delay of only 67 milliseconds in the 256-byte scenario, but with a loss rate of 5.93% in the same scenario.
- GRE over IPsec VPN exceeds 150 milliseconds from the 1024-byte scenario.
- DMVPN even if its loss rate in the 16384 bytes scenario is 0%, it reaches 170 milliseconds in the same scenario.
- IPsec DMVPN reaches 160 milliseconds in the 32768 bytes scenario while its loss rate in the same scenario is zero.

5.4 MOS Score

Fig.10 represents the MOS score obtained from the various scenarios. The effect of the increase in the load is clearly seen on the quality of the VOIP. IPsec clearly affects the MOS score.

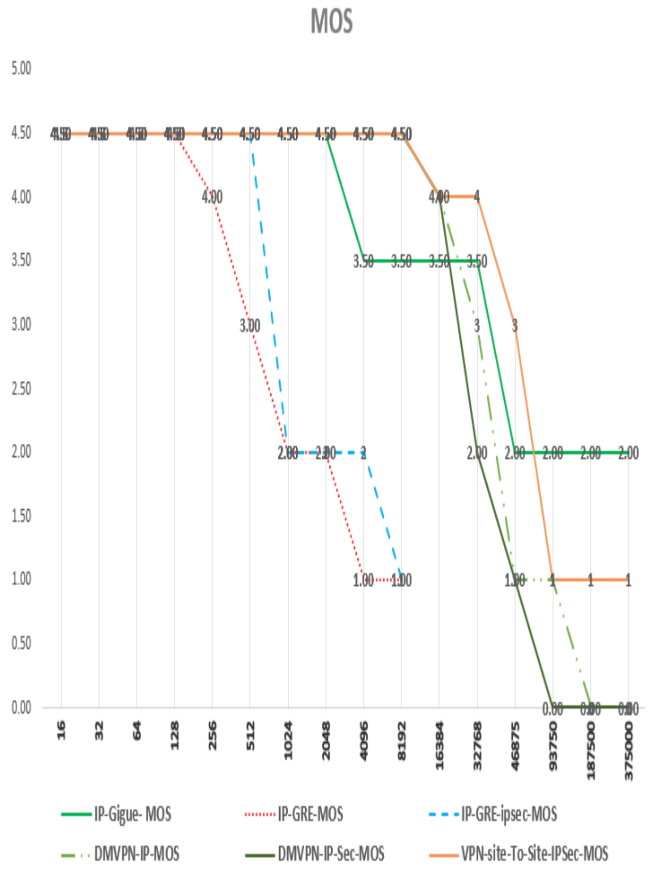

Fig. 10. MOS Score

Judging the scalability of the VOIP must include the MOS Score. As an example, we have deduced earlier that VPN GRE over IPsec can offer a loss rate and a tolerable delay up to a scenario of 1024 bytes, but taking into account the MOS score, in the same scenario the Quality is poor (MOS = 2).

As a synthesis, Fig.11 shows the degree of scalability of the different technologies taking into account the three parameters Latency, loss rate and MOS score.

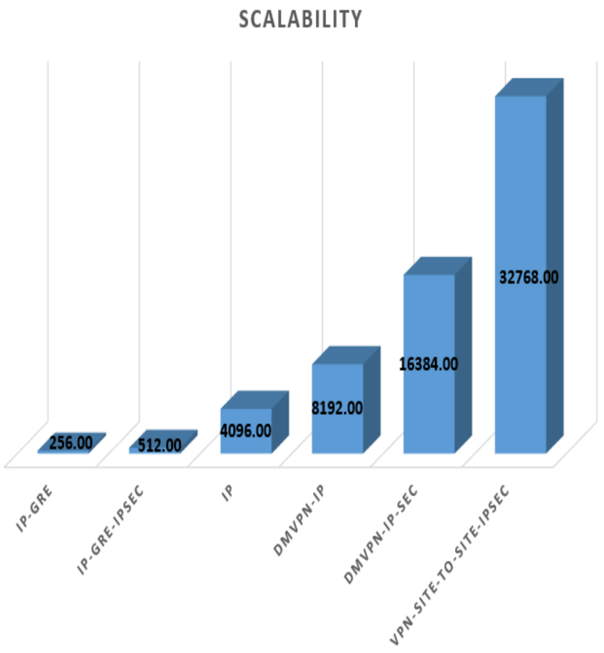

Fig. 11. Scalability Synthesis

6. Conclusion

In this paper, we studied and measured the scalability of different VPN technologies (GRE, GRE over IPsec, DMVPN, IPsec DMVPN, and IPsec site to site) by increasing the load of VOIP packets. The simulations were carried out under GNS3. The results showed that all GRE-based VPN technologies suffer in terms of scalability.

The order of preference obtained is as follows: GRE, GRE over IPsec, IP, DMVPN, IPsec DMVPN and IPsec site to site.

References

[1] Manral, V., & Hanna, S. (2013). Auto-Discovery VPN Problem Statement and Requirements.

[2] Huawei DSVPN(Dynamic Smart VPN) (2013), url: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009655&partNo=100122, visited: April 2017

[3] Dynamic Multipoint VPN (DMVPN) Design Guide, Corporate Headquarters Cisco Systems, Inc. 2006, 104

[4] Hanks, Stan, David Meyer, Dino Farinacci, and Paul Traina. RFC 2784-"Generic routing encapsulation (GRE)." (2000).

[5] P. Christian. RFC 3147 - Generic Routing Encapsulation over CLNS Networks. Nortel Networks, July 2001

[6] Huttunen, Ari, Brian Swander, Victor Volpe, Larry DiBurro, and Markus Stenberg. UDP encapsulation of IPsec ESP packets. RFC 3948, January, 2005.P.

[7] Kent, Stephen. IP authentication header. RFC 4302, December, 2005

[8] Luciani, J., D. Katz, D. Piscitello, B. Cole, and N. Doraswamy. "Next hop resolution protocol (NHRP)." RFC2332 (2001).

[9] AKINOLA, Azeez Paul, et al. Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec). Technical report, 2012.

[10] Eskandar, A. A., Syed, M. R., & Bahareh, Z. M. (2015). Performance Analysis of VOIP over GRE Tunnel. International Journal of Computer Network and Information Security, 7(12), 1.

[11] Eskandar, A. A., Syed, M. R., & Zarei, M. B. (2014, January). SIP over IP VPN: Performance Analysis. In Proceedings on the International Conference on Internet Computing (ICOMP) (p.1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[12] Narayan, S., Williams, C. J., Hart, D. K., & Qualtrough, M. W. (2015, January). Network performance comparison of VPN protocols on wired and wireless networks. In Computer Communication and Informatics (ICCCI), 2015 International Conference on (pp. 1-7). IEEE

[13] Mazalek, A., Vranova, Z., & Stankova, E. (2015, May). Analysis of the impact of IPSec on performance characteristics of VoIP networks and voice quality. In Military Technologies (ICMT), 2015 International Conference on (pp. 1-5). IEEE.

[14] BAHNASSE, Ayoub et EL KAMOUN, Najib. Security of Dynamic and Multipoint Virtual Private Network. International Journal of Computer Science and Information Security, 2016, vol. 14, no 7, p. 100.

[15] Bahnasse, A., & El Kamoun, N. (2015). Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network. International Journal of Computer Applications, 123(2).

[16] BAHNASSE, Ayoub et EL KAMOUN, Najib. Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network. Global Journal of Computer Science and Technology, 2014, vol. 14, no 8-E, p. 63.

[17] BENSALAH, Faycal, EL KAMOUN, Najib, et BAHNASSE, Ayoub. Evaluation of tunnel layer impact on VOIP performances (IP–MPLS–MPLS VPN–MPLS VPN IPsec). IJCSNS, 2017, vol. 17, no 3, p. 87.

[18] BAHNASSE, A., & ELKAMOUN, N. (2015). Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network. Revue MéDiterranéEnne Des TéLéCommunications, 5(2).

[19] BAHNASSE, Ayoub et EL KAMOUN, Najib. Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler. Policy, 2014, vol. 5, no 12.

[20] Nowosielski, L., Wielemborek, R., Laskowski, D., & Wnuk, M. (2015, May). Confidentiality of data in backbone networks based on scalable and dynamic environment technologies. In Communications and Networking (BlackSeaCom), 2015 IEEE International Black Sea Conference on (pp. 68-71). IEEE.

Faycal Bensalah received the Master degrees, Network and telecommunication, from Faculty of sciences El Jadida in 2014. Network administrator at Chouaib Doukkali University, Actually a Ph.D Student on STIC Laboratory on Faculty Of sciences El Jadida, Network and Telecommunications team. His research interest are : NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Najib Elkamoun Ph.D, professor higher education degree at Faculty of sciences El Jadida.in the dept. of physics. Researcher member on STIC laboratory, header of Network and Telecommunications team. His research interest includes, NGN, MPLS , Networks, QoS on mobile networks, wireless networks, networks and telecommunications.

Ayoub BAHNASSE Ph.D on Networks and telecommunication, received the master degrees, in 2013 and 2017 respectively. Actually a researcher associate on LTI laboratory Ben M’sik faculty of sciences. Reviewer on ELSEVIER journals. His research fields are: Security of networks, mobile learning, Wireless Sensor networks, QoS of networks, MPLS, IMS and NGN.