International Journal
Information Technology Applications (ITA)

Volume 9, Number 1, September 2020

CONFIGURING IPSEC-BASED SECURITY FOR VIRTUALIZED NETWORKS

Karol Csivre, Dominik Dermek

Abstract:

In this paper we focus on the latest trends in computer network virtualization. The evolution of data-center networks from L2 Virtual Local Area Networks (VLAN) to more advanced L4-tunnelled Virtual Extensible LANs (VXLAN), necessary for elastic provisioning of overlay networks in a multi-tenant data-center environment, is described. The L3 security implemented by IPsec is identified as a promising method for securing such overlay networks and a complete configuration of tunneling mode IPsec-v3 including IKE-v2 withnin the Cisco IOS is given. Furthermore, quantitative results regarding the effects of various crypthographic algorithms with selected parameter combinations obtained using measurements on an example virtualized topology are presented.

Keywords:

Virtual networks, overlay networks, IPsec, tunneling.

ACM Computing Classification System:

Networks, network components, end nodes, network adapters, network protocols, session protocols.

Introduction

Several current networking trends play an important role in future networks design development. Stacking of several individual active networking boxes, such as the Cisco Catalyst switches, into a single logical device simplifies network configuration and provides substantial network bandwidth improvement [1]. Encryption directly at the MAC layer improves security. The seamless integration of wireless connectivity and management of wireless access points directly from an on-switch built-in controller is now also feasible [2]. The new Linux-kernel based Cisco Open IOS XE [2] brings custom LXC type IOx applications using Docker containers [3], facilitating unprecedented level of programmability directly on the switch, along with standard Linux applications, such a Wireshark.

One of the important trends guiding the design of future networks is massive virtualization. The classic concepts of L2 Virtual LAN (VLAN) is extended to a much more flexible Virtual Extensible LAN (VXLAN) [4] tunneling L2 frames within UDP and the enterprise network topology design, show in (Fig.1) is being slowly replaced by a fully virtualized network design, shown in (Fig.2).

In the classic design, groups of computers are separated into VLANs and the mapping between L2 VLANs and L3 subnets is implemented at the aggregation layer, both for IPv4 and the rising IPv6, which comes with its own challenges (The interested reader can find more details on IPv6 and IPv4/IPv6 interoperability in [5][6]). The venerable Spanning Tree Protocol (STP) and its update Rapid STP (RSTP) [7] are used to prevent loops in topology.

The more modern design emphasizes the use of a switched fabric with traffic spread between multiple physical links and a complete elimination of STP, replacing it usually with a variety of Shortest Path Bridging (SPB)[8].

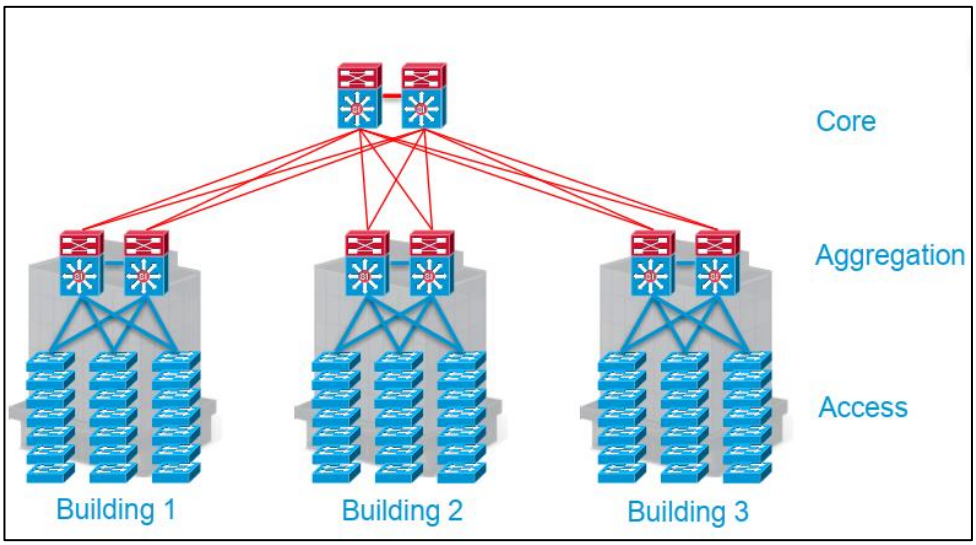


Fig.1. Classic three-tier enterprise network architecture with redundancy [9].

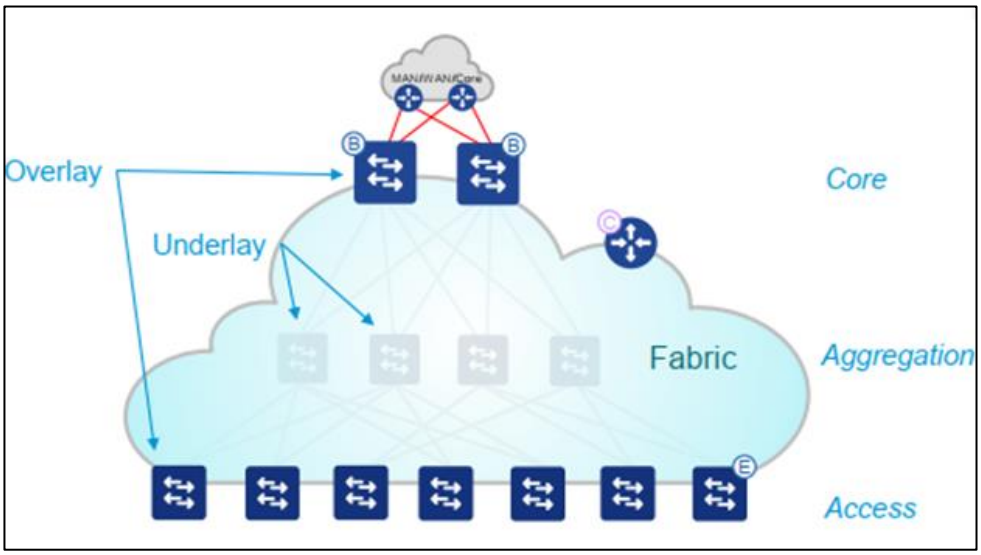


Fig.2. Future enterprise networks with switching fabric
and virtualized set of overlay networks [9].

There are several layers, where security in the form of encryption and authentication can be provided. MACsec has been standardized in 802.1AE [10] and 802.1X-2010 [11] and provides security directly at the link layer, while the venerable IPsec set of standards, dating back to 1995, is extremely mature and widely supported, even in affordable consumer devices.

The utilization of IPsec lies in the focus of this paper and an excellent overview of various IPsec RFCs is provided in RFC6071 [12], bringing a comprehensive information to the interested reader. As demonstrated by [13], the development in this area does not end with the conclusion of the IPsec Working Group, and a new working group dedicated to IPsec is already setting a standardization roadmap.

The challenges of implementing reliable IPsec protection within the context of mobile cellular networks where a moving user equipment (UE) undergoes a handover process when moving between areas covered by different base stations are addresses in [14] and [15], while [16] provides a detailed analysis of the effects of handover latency on IPsec security and suggest a cross-layer L2/L3 security mechanism. [17] then gives realistic values of latency to be expected in cellular networks based on practical measurements.

As described in the IETF charter for the working group: IP Security Maintenance and Extensions (ipsecme) [18] the potential use of IPsec for resource constrained IoT nodes is finally gaining attention of the standardization bodies. Method for reducing ESP and IKEv2 overhead by compressing selected header fields are discussed in several draft RFCs [19][20][21], to be published in 2020.

The paper is organized in the following way: Section one brings a brief recap of the principles of IPsec and GRE. Section two with the help of appendices then gives a full configuration guide for implementing IPsec tunneling on Cisco devices to facilitate the VPN establishment. The next section discusses implementation of the GRE tunneling mode. Section IV then gives quantitative results on the performance of various encryption and hashing algorithm configurations within the GNS3-based virtualized environment. The last section then concludes the paper.

1 IPsec and GRE Overview

Complementary to other transport-layer and application-layer security protocols, such as TLS and SSH, the IPsec provides security directly within the network layer, with implementation built-in the operating system. The advantage of such a design is that an application utilizing the Socket API [22] doesn't need to be modified at all to be protected. The IPsec operates on a per-packet/datagram bases and consists of two slightly different security protocols: Authentication header (AH) and Encryption Security Payload (ESP). Both can operate in transport, or tunneling mode. Since the tunneling mode hides the whole original packet, including its header (and therefore protect also the source and destination IP addresses), it is in the focus of this paper. This is consistent with current data center trends of overlay networks implemented using tunneling, such as VXLAN [23].

Tunneling is a way that is used when it is desired to make connection between the source client somewhere on the Internet or in private network and the destination node or network. IPSec protocol it is one of the tunneling protocol open standards, that provides authentication, encryption and data integrity between the source and destination hosts.

The definition of the current version: IPsec-v3 is given primarily in RFC 4301[24], while many other RFCs amend the basic specification and provide further information. [25] provides an excellent overview of the many RFCs involved along with their status. This protocol provides three main functionalities:

1. Authentication (verification) – it means that the data was not modified during its transmission (it uses and extended authentication header – AH – RFC4302 [26]).
2. Encryption (confidentiality) of transmitted data – this provides protocol Encapsulation Security Payload (ESP), in addition to encryption, it also provides authentication (more information see [27]).
3. Key exchange between the entities – this functionality provide Internet Key Exchange Protocol defined in a much newer RFC [28] that obsoletes previous specifications. Despite its separation to different RFC, motivated by its reuse also out of the scope of IPsec, for all practical purposes IKE must be considered an integral part of successful IPsec deployment.

IPSec use to ensure the secure transmission of data, voice, and data between sites (Site-to-Site). We create a VPN tunnel over a public Internet and the communication among the tunnel encrypted using encryption algorithms that ensure the confidentiality of transmitted data. A key mechanism for authentication and securing confidentiality within the IPSec protocol is the creation of a Security Association (SA), which is stored in the Security Association Database (SAD). A security association is a one-way logical connection (for bidirectional communication two SAs are created own for each direction). The SAs are applied according to security policies, that are stored in the Security Policy Database (SPD).

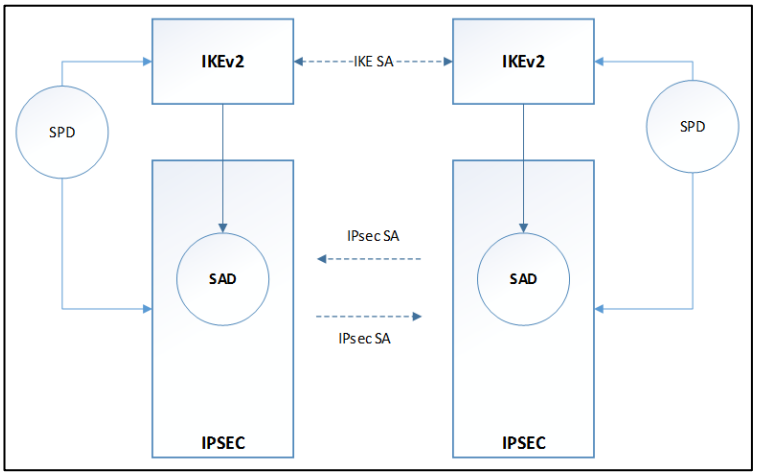


Fig.3. Schematics of IPsec operation:
in phase one the Security Association (SA) parameters are configured by IKE.
These are than used on a per-packet basis for communication securing.

The negotiations of the security association in IKEv1 consisted of two parts. The aim of the first part in IKEv1 was to establish a security association for the exchange of IKE SA keys, and the aim of the second part of IKEv1 is to establish a security association for the transfer data of IPSec SA.

The IKEv2 simplifies the negotiation process of the security association. It uses two exchanges (4 messages in total) to create the IKE SA security association and a pair of messages for the IPSec SA security association. IPSec SA is based on the mutual exchange of messages in pairs.

- The first pair of messages (temporary exchange) - information about cryptographic algorithms and other security parameters. The result is the creation of a special security association (IKE SA). After that, the exchanged messages protect by encryption and authentication.
- During the second exchange, the communicating entities authenticate to each other and create the first IPsec Security Association (IPSec SA), which is used to ensure normal operation between the communicating entities. To creating a security, association requires the exchange of two pairs of messages. The security association is stored in the database of security associations (SAD)

The Generic Routing Encapsulation (GRE) is a tunneling protocol developed to address the shortcomings of basic IP-in-IP tunneling, such as the inability to tunnel multicast traffic. Similarly to IPSec, it can be used to establish a tunneled connection between network nodes. Definition of the GRE is given in [29] and [30]. The GRE protocol is unsecure that means this communication in the tunnel is not encrypted. To implement a secure transmit multicast communication over the internet (for example transmit routing information via OSPF protocol which is the multicast communication) it is common practices to secure the communication with combination of GRE and IPSec protocol.

2 IPsec Implementation Within Cisco IOS

(Fig.4) gives an overview of the example topology to implement a VPN using an IPsec tunnel: the IP traffic is securely tunneled between branch offices at their security gateways RouterA and RouterB, while the middle ISP router models an unsecure Internet connection between the branch offices. The advantage of this approach is that the computers in branch offices' local networks do not even need to implement IPsec – its operation is transparent to them, thus saving precious computing resources.

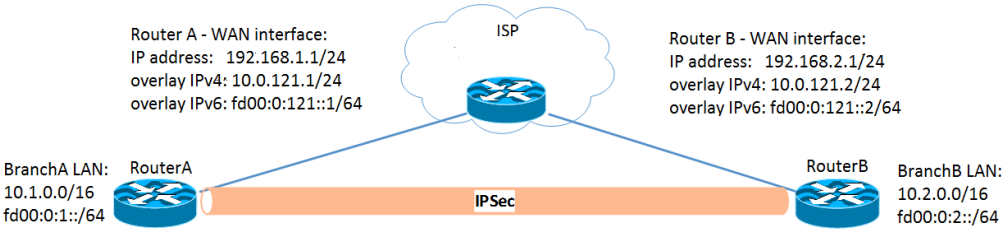


Fig.4. IPsec tunnel between two branch offices over an unsecured Internet modelled by the top ISP router. Tunnel may be configured to carry IPv4 in IPv4 (IP-IP) or IPv6 in IPv4 (6in4) with or without GRE for tunneling multicast traffic.

Before an IPsec tunnel is configured, the IKE configuration should take place. The configuration of IKEv2 consists of the several configuration steps (Note: In all tables, the prompt `RouterA/B` indicates this command is set on both routers with the same arguments.):

IKEv2 Keyring - create the configuration in case if we want to use the shared secret key for authentication. Creating the IKEv2 keyring consist of pre-shared keys associated with the IKEv2 profile as shown in (Tab.1):

Table 1. Configuration of IKEv2 keyring within Cisco IOS.

Step	Command	Description

1	`RouterA(config)#`
	`  crypto ikev2 keyring KEYRING-RA`
	`RouterB(config)#`
	`  crypto ikev2 keyring KEYRING-RB`
		Define the name of the IKEv2 Keyring and enter into configuration mode.

2	`RouterA(config-ikev2-keyring)#peer RouterB` `RouterB(config-ikev2-keyring)#peer RouterA`	Define the name for the opposite side of the future tunnel.

3	`RouterA(config-ikev2-keyring-peer)#`
	`  address 192.168.2.1`
	`RouterB(config-ikev2-keyring-peer)#`
	`  address 192.168.1.1`
		Specify the IPv4 or IPv6 address on the remote peer – the other end of the IPsec tunnel (the delivery protocol).

4	`RouterA/B(config-ikev2-keyring-peer)#` `  pre-shared-key` *`Passw0rd2020`*	Specify the shared secret key.

IKEv2 Proposal - consists of definitions of transformations and defines parameters such as the encryption algorithm, the algorithm of the data integrity, pseudorandom functions and the choice of Diffie-Hellman group.

Table 2. Configuration of IKEv2 proposal within Cisco IOS.

Step	Command	Description

1	`RouterA(config)#`
	`  crypto ikev2 proposal PROP-RA`
	`RouterB(config)#`
	`  crypto ikev2 proposal PROP-RB`
		Define the name of the IKEv2 Proposal and enter into configuration mode.

2	`RouterA/B(config-ikev2-proposal)#` `  encryption aes-cbc-256`	(Optional) Define one or more transformation for the encryption.
3	`RouterA/B(config-ikev2-proposal)#` `  integrity sha512`	(Optional) Define one or more transformation for the integrity.
4	`RouterA/B(config-ikev2-proposal)#group 14`	(Optional) Define one or more transformation for the Diffie-Hellman group

IKEv2 Policy – define the name of the IKEv2 Policy and interlinking with the IKEv2 Proposal that the IPsec will to use in the negotiation of the IKE SA security association in the exchange of IKE_SA_INIT messages.

Table 3. Configuration of IKEv2 policy within Cisco IOS.

Step	Command	Description
1	RouterA(config)# crypto ikev2 policy POLICY-BRANCHA RouterB(config)# crypto ikev2 policy POLICY-BRANCHB	Define the name of the IKEv2 Policy and enter into configuration mode.
2	RouterA(config-ikev2-policy)# proposal PROP-RA RouterB(config-ikev2-policy)# proposal PROP-RB	Specify the name of the IKEv2 Proposal that will be interlinking with the IKEv2 Policy.

IKEv2 Profile – define the IP address of the remote peer, specify the local and remote authentication mode.

Table 4. Configuration of IKEv2 profile within Cisco IOS.

Step	Command	Description
1	RouterA(config)# crypto ikev2 profile PROF-RA-TO-RB RouterB(config)# crypto ikev2 profile PROF-RB-TO-RA	Define the name of the IKEv2 Profile and enter into configuration mode.
2	RouterA(config-ikev2-profile)# match identity remote address 192.168.2.1 255.255.255.255 RouterB(config-ikev2-profile)# match identity remote address 192.168.1.1 255.255.255.255	Select the profile based on the remote IP address
3	RouterA/B(config-ikev2-profile)# authentication local pre-share	Specify the local authentication method.
4	RouterA/B(config-ikev2-profile)# authentication remote pre-share	Specify the remote authentication method.
5	RouterA(config-ikev2-profile)# keyring local KEYRING-RA RouterB(config-ikev2-profile)# keyring local KEYRING-RB	Specify the name of the IKEv2 Keyring for this profile.

An Access Control List (ACL) must be created to specify, which packets are to be sent to the tunnel and secured using IPSec:

Table 5. Configuration of ACL within Cisco IOS.

Step	Command	Description
1	RouterA(config)# ip access-list extended VPN-RA-TO-RB RouterB(config)# ip access-list extended VPN-RB-TO-RA	Define the name of the extended ACL and enter into configuration mode.
2	RouterA(config-ext-nacl)# permit ip 10.1.0.0 0.0.255.255 RouterB(config-ext-nacl)# permit ip 10.2.0.0 0.0.255.255	Permit all packets that meets the conditions.

Set the transformation set that defines how the data is protected:

```
RouterA(config)#
  crypto ipsec transform-set TS-RA-TO-RB esp-aes 128 esp-sha512-hmac
RouterB(config)#
  crypto ipsec transform-set TS-RB-TO-RA esp-aes 128 esp-sha512-hmac
```

Crypto map – this configuration joins the previous parts of the IPSec configuration (ACL, transformation set, IP address of the remote peer, lifetime of the data connection, etc.).

Table 6. Configuration of crypto map within Cisco IOS.

Step	Command	Description

1	RouterA(config)#
	  crypto map CRYPTO-MAP-RA-RB 10 ...
	  ipsec-isakmp
	RouterB(config)#
	  crypto map CRYPTO-MAP-RB-RA 10 ...
	  ipsec-isakmp
		Create or change the crypto map

2	RouterA(config-crypto-map)#
	  set peer 192.168.2.1
	RouterB(config-crypto-map)#
	  set peer 192.168.1.1
		Specify the hostname or IP address of the remote peer.

3	RouterA(config-crypto-map)#
	  set transform-set TS-RA-TO-RB
	RouterB(config-crypto-map)#
	  set transform-set TS-RB-TO-RA
		Specify the transformation set.

4	RouterA(config-crypto-map)#
	  match address VPN-RA-TO-RB
	RouterB(config-crypto-map)#
	  match address VPN-RB-TO-RA
		Specify the name of the extended ACL.

5	RouterA(config-crypto-map)#set pfs group14 RouterB(config-crypto-map)#set pfs group14	Optional – define for IPSec, that should request password confidentiality when requesting new SA.

6	RouterA(config-crypto-map)#
	  set ikev2-profile PROF-RA-TO-RB
	RouterB(config-crypto-map)#
	  set ikev2-profile PROF-RB-TO-RA
		Specify the name of the IKEv2 Profile

7	RouterA(config-crypto-map)#
	  set security-association lifetime
	  seconds 3600
	RouterB(config-crypto-map)#
	  set security-association lifetime
	  seconds 3600
		Optional – specify the lifetime of the Security Association

An finally, the crypto map must be activated on the WAN interface on the both routers.

Table 7. Activation of crypto map within Cisco IOS.

Step	Command	Description
1	RouterA(config)#int e0/0 RouterB(config)#int e0/0	WAN Interface selection.

2	RouterA(config-if)#
	  crypto map CRYPTO-MAP-RA-RB
	RouterB(config-if)#
	  crypto map CRYPTO-MAP-RB-RA
		Applying crypto map on the interface..

Table 8. Creating virtual interface for the tunnel.

Step	Command	Description

1	`RouterA(config)#interface tunnel 1`
	
	`RouterB(config)#interface tunnel 1`
		Create virtual interface for the tunnel and enter into the configuration mode.

2	`RouterA(config-if)#tunnel source 192.168.1.1`
	
	`RouterB(config-if)#tunnel source 192.168.2.1`
		Specify the outside source IP address for the virtual interface.

3	`RouterA(config-if)#`
	`  tunnel destination 192.168.2.1`
	
	`RouterB(config-if)#`
	`  tunnel destination 192.168.1.1`
		Specify the destination IP address of the delivery protocol.

4a	`RouterA(config-if)#`
	`  ip address 10.0.121.1 255.255.255.0`
	
	`RouterB(config-if)#`
	`  ip address 10.0.121.2 255.255.255.0`
		For IPv4-in-IPv4 tunnel.
		Assign the IP address into virtual interface `tunnel 1`.

4b	`RouterA(config-if)#`
	`  ipv6 address FD00:0:121:0:0:0:0:1/64`
	
	`RouterB(config-if)#`
	`  ipv6 address FD00:0:121:0:0:0:0:2/64`
		For IPv6-in-IPv4 (6in4) tunnel.
		Assign the IPv6 address into virtual interface `tunnel 1`.

Further configuration steps regarding routing (static or OSPF) must also be taken, but since they aren't really part of IPsec, are omitted here. The successful configuration is then tested using the classic integrated ping command from within the router's IOS command line interface. In a virtualized, GNS3-based topology however, it is straightforward to test the encryption using the Wireshark packet analyzer, as show in (Fig.5).

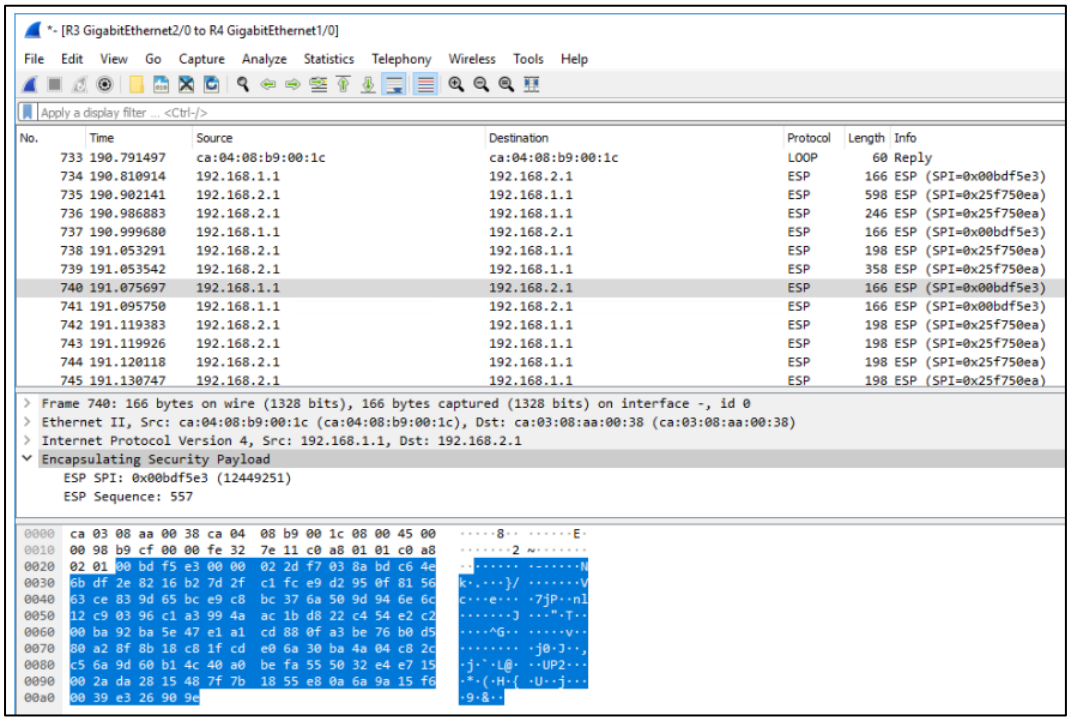


Fig.5. Wireshark analysis at ISP link shows the traffic is indeed encrypted and therefore protected.

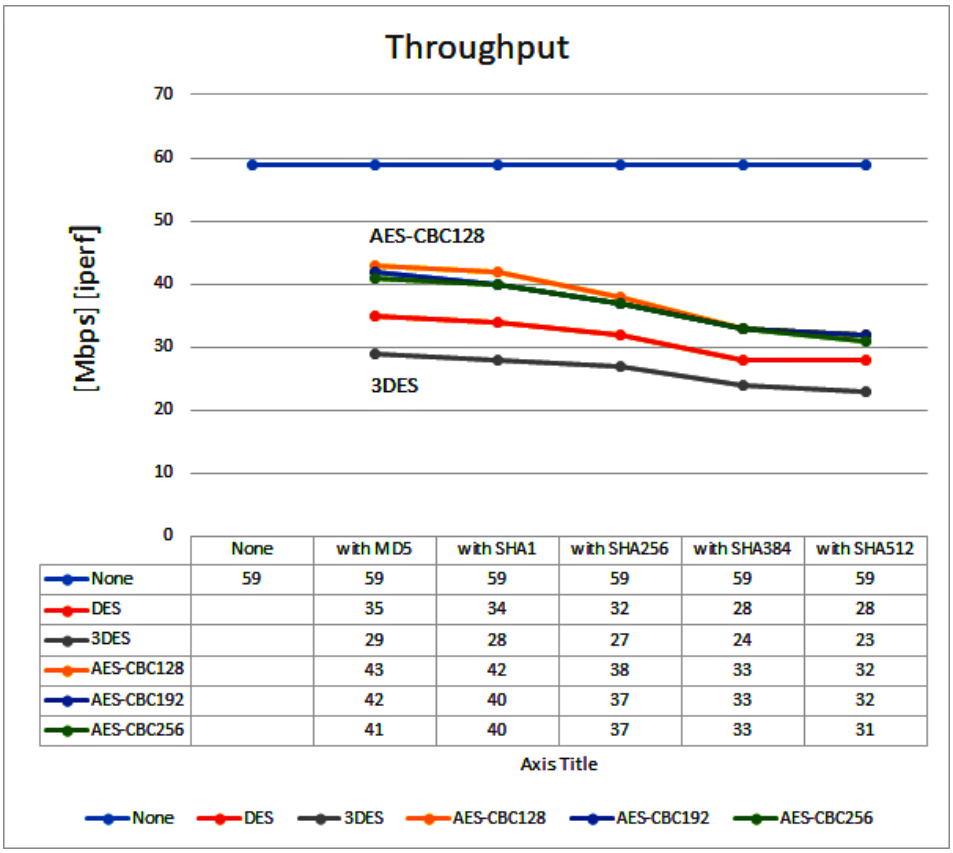
3 Measurements on Virtualized Topology

Since the virtualization of computer networks becomes ever more important, interesting questions regarding the throughput and latency parameters of such virtualized design, and their effect on CPU-utilization when simulating network operation arise. These have to be measured by affordable, or better free and open tools, such as `iperf`. For a simple topology show in (Fig.4), the throughput and latency were measured in a virtualized GNS3-based topology along with the CPU utilization on a Intel(R) Core(TM)-i7-8650U CPU 1.90 GHz processor.

Table 9. Results of measurements.

Protection parameters	**Throughput [Mbps]**	**CPU utilization [%]**	**Average latency [ms]**
None	59	61-66	3
DES with MD5	35	61-66	3
DES with SHA1	34	62-67	4
DES with SHA256	32	60-64	3
DES with SHA384	28	61-64	3
DES with SHA512	28	62-66	3
3DES with MD5	29	59-65	2
3DES with SHA1	28	60-65	4
3DES with SHA256	27	59-64	3
3DES with SHA384	24	60-65	3
3DES with SHA512	23	60-67	3
AES-CBC128 with MD5	43	60-65	4
AES-CBC128 with SHA1	42	60-65	4
AES-CBC128 with SHA256	38	60-66	2
AES-CBC128 with SHA384	33	60-67	3
AES-CBC128 with SHA512	32	61-68	3
AES-CBC192 with MD5	42	59-63	4
AES-CBC192 with SHA1	40	59-63	3
AES-CBC192 with SHA256	37	58-63-	4
AES-CBC192 with SHA384	33	59-63	4
AES-CBC192 with SHA512	32	59-62	5
AES-CBC256 with MD5	41	58-63	3
AES-CBC256 with SHA1	40	59-64	3
AES-CBC256 with SHA256	37	61-65	4
AES-CBC256 with SHA384	33	58-63	5
AES-CBC256 with SHA512	31	58-64	4

As shown in the (Tab.9) the CPU utilization and average latency played no major role on virtual environment. CPU utilization without running the test was at the level of 15% on the physical machine, during data transfer using the `iperf` tool, CPU utilization was at the level of 58-66% for all encryption algorithms. These parameters did not change even when we increased the number of cores on end workstations. Network latency can play a significant role in large networks and CPU utilization in turn can be affected based on the HW equipment of the router e.g. whether the encryption is performed on the basis of the operating system on the router (SW) or the given HW has a special chip which provides encryption at the motherboard level.



	None	with MD5	with SHA1	with SHA256	with SHA384	with SHA512
None	59	59	59	59	59	59
DES		35	34	32	28	28
3DES		29	28	27	24	23
AES-CBC128		43	42	38	33	32
AES-CBC192		42	40	37	33	32
AES-CBC256		41	40	37	33	31

Fig.6. Comparison of measured throughput values of selected encryption and hash algorithms. (*to distinguish color lines, see the online version of journal*)

However, it can be seen from the experiment that turning on encryption reduces data transmission throughput by 27% for the best result using AES-CBC128 with a legacy (and therefore not practical) MD5, to for a more realistic AES-CBC256 with SHA256 with a 37% performance penalty. Older legacy encryption algorithms such as DES and 3DES performed worse in the measurement than newer AES encryption algorithms which gives one more reason, apart from their know weaknesses, not to use them.

Conclusion

In this paper we have focused on the latest trends in the evolution of data-center networks from L2 based VLANs to more advanced L4-tunnelled VXLANs, necessary for elastic provisioning of overlay networks in a multi-tenant data-center environment. The L3 security implemented by IPsec was identified as a promising method for securing such overlay networks and a complete configuration of tunneling mode IPsec-v3 including IKE-v2 within the Cisco IOS was given along with a simple example topology. Quantitative results regarding the effects of various cryptographic algorithms on throughput, latency and CPU utilization were presented.

Acknowledgement

This work was supported by the Slovak Research and Development Agency under the Contract no. APVV-19-0436 and it was also supported by the Scientific Grant Agency of the Ministry of Education of Slovak Republic and Slovak Academy of Sciences (grant VEGA 1/0477/18) and and by the Tatra bank foundation programme Quality of Education, within the project "SDRLab 2.0 – technologies of 5G networks and IoT in classroom".

References

[1] Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE [Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html]

[2] Cisco IOS XE [Available: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html]

[3] Cisco devnet Tutorial: Build sample LXC type IOx app using Docker toolchain [Available: https://developer.cisco.com/docs/iox/#!lxc-workflow/tutorial-build-sample-lxc-type-iox-app-using-docker-toolchain

[4] M. Mahalingam et al. RFC 7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, Aug 2014,IETF [Available: https://tools.ietf.org/html/rfc7348]

[5] Palenik, T.: Computer Networks. ForPress, Slovakia 2014, ISBN 978-80-89731-13-8.

[6] Stas F., Palenik T.: Mechanism of interoperability between IPv4 and IPv6 Protocols. In proc of Redzur 2016: 10th anniversary International Workshop on Multimedia and Signal Processing, Bratislava, Slovakia, May 2016, ISBN: 978-80-227-4560-4.

[7] IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges, in IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998) , vol., no., pp.1-281, 9 June 2004, doi: 10.1109/IEEESTD.2004.94569.

[8] IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks, in IEEE Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014) , vol., no., pp.1-1993, 6 July 2018, doi: 10.1109/IEEESTD.2018.8403927.

[9] J. Pilař, P. Křižanovský, Z. Roubal, R. Boch: Připravte si infrastrukturu na novou realitu – Přepínané síťe. webinar Cisco Engage 25.6.2019

[10] IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security, in IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006) , vol., no., pp.1-239, 26 Dec. 2018, doi: 10.1109/IEEESTD.2018.8585421

[11] IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, in IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004) , vol., no., pp.1-205, 5 Feb. 2010, doi: 10.1109/IEEESTD.2010.5409813.

[12] S. Frankel, S. Krishnan: RFC 6071: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, Feb 2011, IETF [Available: https://tools.ietf.org/html/rfc6071]

[13] T. Pauly, S. Touati, R. Mantha: RFC8229: TCP Encapsulation of IKE and IPsec Packets, Aug 2017, IETF. [Available: https://tools.ietf.org/html/rfc8229]

[14] S. Smaoui, F. Zarai and L. Kamoun: IPSec tunnel establishment for 3GPP-WLAN interworking, 8th International Conference on Informatics and Systems (INFOS), Cairo, 2012, pp. NW-74-NW-80.

[15] A. Hussein, I. H. Elhajj, A. Chehab and A. Kayssi: Securing Diameter: Comparing TLS, DTLS, and IPSec, 2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, 2016, pp. 1-8, doi: 10.1109/IMCET.2016.7777417.

[16] F. Leu, Y. Huang and C. Chen: The IPSec Security Problems and a Cross-layer Security Mechanism for PMIPv6 Handover when an IPSec Security Association is Established on an L2 Direct Link, 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, Victoria, BC, 2012, pp. 452-457, doi: 10.1109/BWCCA.2012.80.

[17] Kloibhofer R.,Fresolone F. et al.: Throughput and One-Way Latency Measurements in a 3G/4G Live-Network Hi-Mobility Uplink.
In proc. TSP 2016 – 39th International Conference on Telecommunications and Signal Processing, Vienna, Austria, June 2016, ISBN: 978-1-5090-1287-9, ISSN: 1805-5435.

[18] IETF Datatracker: IP Security Maintenance and Extensions (ipsecme) Working Group: Charter for Working Group [Available: https://datatracker.ietf.org/wg/ipsecme/about/]

[19] D. Migault, T. Guggemos, C. Bormann, D. Schinazi: draft-mglt-ipsecme-diet-esp: ESP Header Compression and Diet-ESP, March 2019, IETF [Available: https://tools.ietf.org/html/draft-mglt-ipsecme-diet-esp-07

[20] V. Smyslov: draft-smyslov-ipsecme-ikev2-compression: Using compression in the Internet Key Exchange Protocol Version 2 (IKEv2). March 2020, IETF
[Available: https://tools.ietf.org/html/draft-smyslov-ipsecme-ikev2-compression-08]

[21] V. Smyslov: draft-smyslov-ipsecme-ikev2-compact: Compact Format of IKEv2 Payloads. March 2020, IETF [Available: https://datatracker.ietf.org/doc/draft-smyslov-ipsecme-ikev2-compact/]

[22] Linux programmer's Manual, socket(2). Linux man-pages v5.07, 2020
[Available: https://man7.org/linux/man-pages/man2/socket.2.html]

[23] IETF, RFC7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, 2014, ISSN: 2070-1721,
[Available: https://tools.ietf.org/html/rfc7348]

[24] IETF, RFC4301: Security Architecture for the Internet Protocol, 2005
[Available: https://tools.ietf.org/html/rfc4301]

[25] IETF, RFC6071: IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap
[Available: https://tools.ietf.org/html/rfc6071]

[26] IETF, RFC4302: IP Authentication Header, 2005 [Available: https://tools.ietf.org/html/rfc4302]

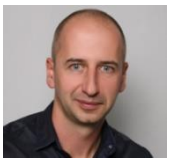
[27] IETF, RFC4303: IP Encapsulating Security Payload (ESP), 2005
[Available: https://tools.ietf.org/html/rfc4303]

[28] IETF, RFC7296: Internet Key Exchange Protocol Version 2 (IKEv2), 2014
[Available: https://tools.ietf.org/html/rfc7296]

[29] IETF RFC2784: Generic Routing Encapsulation (GRE), 2000
[Available: https://tools.ietf.org/html/rfc2784]

[30] IETF, RFC2890: Key and Sequence Number Extensions to GRE, 2000
[Available: https://tools.ietf.org/html/rfc2890]

Authors



Bc. Karol Csivre
Allianz Technology
karol.csivre@gmail.com
Works at the middle-tier IT process management, leading projects and manages a team of people who take care of information systems (hardware, software, network infrastructure LAN, MAN, SAN, WAN, firewall, DB). Has 25 years of experience with operating and building systems in a corporate data center environment.



Bc. Dominik Dermek
Slovak University of Technology
Faculty of Electrical Engineering and Information Technology
Bratislava, Slovakia
xdermekd@stuba.sk