Secured Communication Using Virtual Private Network (VPN)

Paul Joan Ezra, Sanjay Misra, Akshat Agrawal, Jonathan Oluranti, Rytis Maskeliunas, and Robertas Damasevicius

Abstract The evolution and era of the latest programs and services, collectively with the enlargement of encrypted communications, make it difficult for site visitors within a safety enterprise. Virtual private networks (VPNs) are an instance of encrypted communique provider that is becoming famous, as a way for bypassing censorship in addition to gaining access to offerings which are geographically locked. This paper reviews the layout of an IP security, VPN. The Cisco Packet lines platform is used for the simulation, evaluation and verification. It uses a virtual connection to carry the records packets from a non-public network to remote places.

Keywords Virtual private network · Authentication · Security · Confidentiality

1 Introduction

Individuals who use the Internet are highly exposed to social media exploitation where they are victims of attacks. Due to the various attack and vulnerability that data are exposed to when been transmitted from a sender to a receiver, a protection mechanism ought to be provided to address several safety assaults on statistics transmission through the Internet. There are different attacks over the Internet, such

P. J. Ezra · S. Misra (✉) · J. Oluranti
Center of ICT/ICE Research, Covenant University, Ota, Nigeria
e-mail: Sanjay.misra@covenantuniversity.edu.ng

J. Oluranti
e-mail: jonathan.oluranti@covenantuniversity.edu.ng

A. Agrawal
Amity University, Gurgaon, Haryana, India

R. Maskeliunas · R. Damasevicius
Silesian University of Technology, Gliwice, Poland
e-mail: rytis.maskeliunas@polsl.pl

R. Damasevicius
e-mail: robertas.damasevicius@polsl.pl

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_27

as the denial-of-service attack which makes the network service unavailable by flooding network traffic to the target which exhausts the processing power of the target [1, 2]; information has been changed either accidentally or by malicious attack affects the integrity of the data or creates false information. Eavesdropping on data containing confidential information, such as the location, keys and even passwords of the node, can be redirected to another location. Many security mechanisms have been reviewed to protect data integrity, confidentiality, availability, authenticity and non-repudiation. Cell users want to get entry to assets from their company or domestic network in an efficient but relaxed manner which is done with the help virtual private network (VPN) connections. VPN is a virtual connection routed through the Internet on a public network, from the sender's private network to the receiver. VPN aims to initiate a secure communication path among different networks. It is usually created across the public network [3]. VPN tunnels are used to maintain the privacy of statistics shared over the physical network connection protecting packet-level encryption, consequently making it very hard to become aware of the programs strolling through these VPN services [4].

Authors in [5] showed that a current survey indicated that almost 50% of agencies would adopt the preceding idea by 2025. VPN provides privacy which prevents intermediated users from eavesdropping, altering or deleting the data, authentication which validates that the packet sent by the authorized sender, checks that the data is not altered and prevent intermediate users from copying and resending the information. A VPN tunnel is created for the information to be secured over the physical community connection, maintaining packet-stage encryption, making it very hard to discover the software passing through the VPN offerings. This paper focuses on secure communication using a VPN.

VPNs continue to develop with an increasing number of options that is frequently used in both big and small organization. They also have an advantage of flexibility, connectivity and security at cheap cost. Organizational gains from VPN are reduction in cost and increases in scalability and productivity without compromising the security [6]. This study covers the simulation, evaluation and verification with the help of a packet tracer simulator.

The main aim of the present work is to design a simple system that uses a VPN to secure wireless communication. The following are the main objectives of the presented work.

1. To show how to protect data from being attack over the Internet.
2. To enable communication to be kept private between only the receiver and sender.
3. To show how VPN is over other security mechanisms such as firewall defense.

A brief knowledge of the work is given in this section. Section 2 presented related works in the field of secured communication. Section 3 outlines the method that is used for design and implementation and results. Section 4 describes the conclusion and future work.

2 Related Works

We have reviewed the related works in several databases. The summary of all those important and selected studies is given in Table 1.

There are several other related works [8, 23, 24] available in the literature but due to limitation of work, we are not providing details.

3 Methodology and Results

CISCO packet tracer is used for the design and the simulation of the proposed network using VPN. Only the authorized user will be able to communicate with the other network. The routers will be configured with advance encryption standard to protect data and privacy, Hash-sha tool for IP security authentication, ISAKMP protocol to ensure that two hosts agree on how to build a security association.

3.1 Design and Implementation

Any device connected to the Internet has an IP address which is a sequence of number; a VPN will mask the IP address. An IP address identifies address and location, and a VPN erases IP address from been detected, encrypts your data and keeps your activities private but they do reduce the speed due to the extra security.

For a system to have a working VPN, the following must be configured.

1. Access-list to permit corresponding traffic that will go over the tunnel.
2. ISAKMP policy and ISAKMP key. It is used to set up key authentication and tunnel.
3. IP sec transform-set. It provides authentication and integrity.
4. Crypto map. The crypto map should be applied to the interface.

VPN tunnel must have a security license on the router. The encryption algorithm that was used is the advanced encryption standard (AES) with a key of 256, to protect data and ensure privacy. The IPsec message integrity used is the HMAC-SHA which defines the key size to support different encryption key size. The pre-shared authentication key was used to require VPN devices on each end to configure with the identical mystery key.

Figure 1 shows a conceptual diagram of the VPN network within an organization with all configured interfaces. If the interfaces are not connected to an IP address, there cannot be any form of communication, secured or not secured. This IP address is a unique identifier that indicates the location of a device and governs the way data is sent over the Internet. In the fig above, router 3 interface is

Table 1 Summary of the literature review

Summary of the literature review		
Authors	Work done	Result
Liyanage and Gurtov [7]	VPN architecture for LTE backhaul was addressed. The Internet key exchange model 2(IKEv2) and host identity protocol (HIP) were used as the safety key	Provided secured backhaul traffic during DoS, DDoS and TCP reset attacks
Deshmukh and Iyer [5]	A secure VPN for remote access was addressed. The advanced encryption standard (AES) algorithm was used for data security. The work was carried out on a packet tracer	The smart devices can securely get linked with users on the Internet as if they had been part of the equal non-public network
Busschbach [4]	Enhancing the QoS of a VPN by using an asynchronous transfer mode (ATM) and multiprotocol label switching is studied	An MPLS-based VPN using next-technology IP switches as the best method to enhance the QoS for VPNs
Jaha et al. [8]	A VPN formula that relies on remote access connections requirements and a site-to-site VPN formula that relies on site-to-site connections requirements	Provide a basis while creating business enterprise WAN which connects websites and customers using VPN technology
Azhar et al. [9]	A social media detection on SMS and camera by using application programming interface (API) and permissions was addressed	Identify measures for API and permission for SMS and camera and possible methods for API and permission SMS and API exploitation
Chze and Leong [10]	Proposed a secure multi-hop (SMRP) to merge the routing and authentication processes	Result suggests that the SMRP produces a secured multi-hop IoT communication network without performance degradation in comparison with the well-known optimized link nation routing protocol (OLSR)
Das and Islam [11]	A remarks-based dynamic computation version that could correctly come across unexpected strategic alteration in malicious behavior with the additional feature of balancing workload among service provider was addressed	Strategic behavior of a malicious agent was detected. They provided a mathematical definition of secured trust
Sarika et al. [12] Wu et al. [13] Dinesh et al. [14] Zhou and Hass [15]	Studied the vulnerabilities, attacks and security mechanisms for mobile ad hoc networks (MANETs)	Gives more understand on MANETs, their traits, uses, the criterion for the network security

(continued)

Table 1 (continued)

Summary of the literature review		
Authors	Work done	Result
Manvi and Tangade [16]	The authentication schemes in vehicular ad hoc networks (VANETs) were studied	Security was based on cryptography systems and digital signature. VANET became famous in transport because of the broadcast of safety messages between vehicles
Assadhan et al. [17]	Monitoring and analyzing of a botnet by the command and control (C2) communication traffic	The result achieved was by evaluating a periodogram of the packet and address count sequences
Lan et al. [18]	The hardware implementation of a lightweight Chaskey algorithm using different implementation scheme was studied	A hardware implementation of 3334.33 gate equivalent is achieved with an operating clock frequency of 1 MHz
Liu [19]	Hash-based message authentication codes (HMAC) was studied to achieve authenticity and integrity without the support of a digital signal	Prove that the HMAC is cheap and easy to implement, and it can be used on websites
Draper-gil et al. [3]	Two standard machine learning algorithms, C4.5 and KNN, were used as classification techniques for time-related features	The results prove that the proposed set of time-related features are good classifiers, reaching accuracy levels above 80%. C4.5 and KNN had a similar performance in all experiments; C4.5 has achieved better results
Padmavathi [20]	Zone routing protocol (ZRP) with wireless transport layer security (WTLS) models was addressed to provide security	The proposed work provided security in both routing and transport layer of MANET
Liang et al. [21] Kobayashi and Shitz [22] Nawej and Technologiae [6]	Secured communication over fading channel was addressed They evaluated the impact of VPN on network performance. The network performance covers the hypertext transfer protocol (HTTP), file transfer protocol (FTP) and constant bit rate (CBR)	They establish a capacity state of the parallel broadcast channel, parallel Gaussian broadcast channel and an optimal power location A simulation was done on NS2 for network on VPN and no VPN. network with VPN always delivers better results

having an IP address of 209.165.100.2 and 209.165.200.2, router 4 209.168.100.1 and 192.168.1.1 and router 5 209.165.100.2 and 192.168.3.1

Figure 2 shows that the router does not have a security license. Without this security license VPN encryption, secure collaborative encryption, dynamic multipoint VPN is impossible. The securityk9 can be checked by using the “show version” command in the privilege mode. The security license has been configured and shown in Figs. 3 and 4

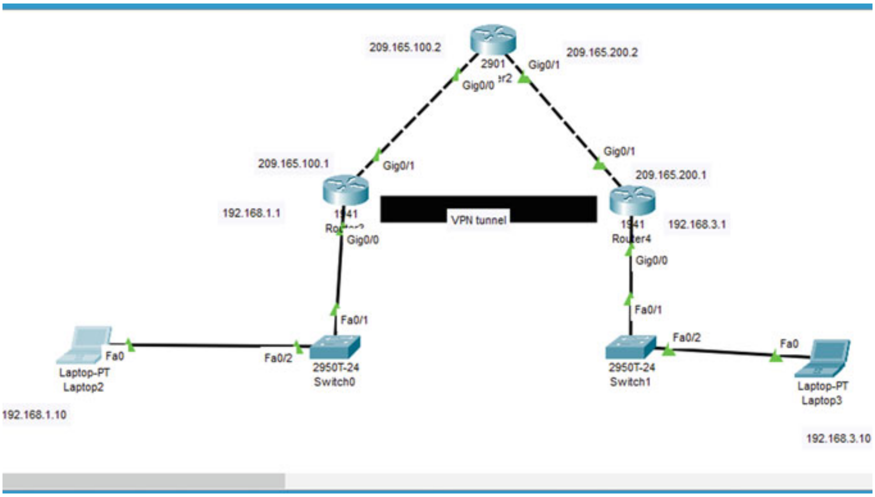
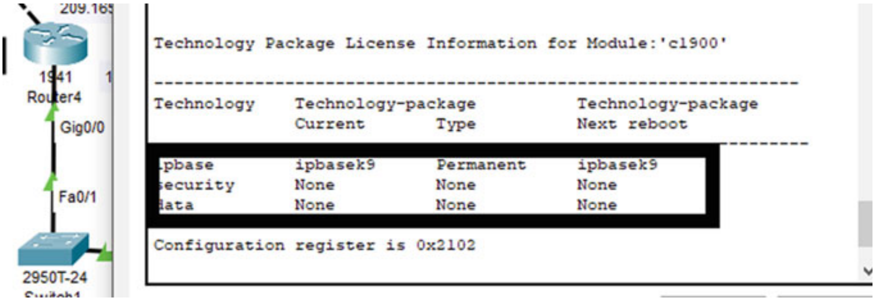
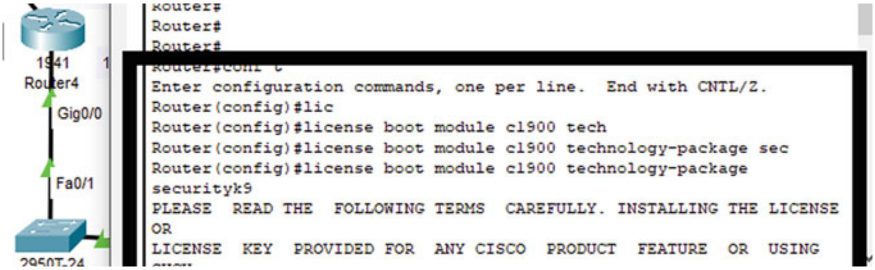


Fig. 1 Theoretical diagram of a VPN network



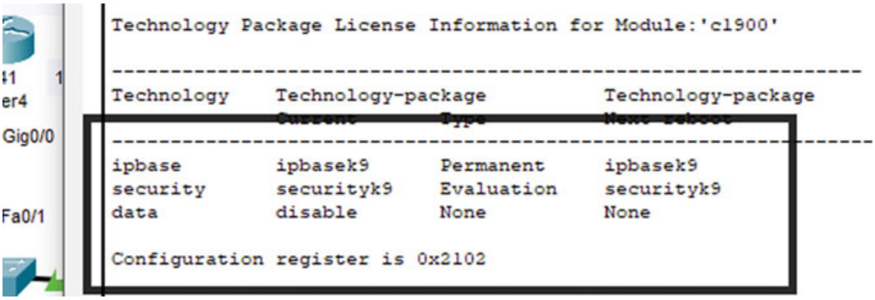
```
Technology Package License Information for Module:'c1900'

------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
-------------------------------------------------------------------
pbase         ipbasek9      Permanent      ipbasek9
ecurity       None          None           None
ata           None          None           None

Configuration register is 0x2102
```

Fig. 2 Router without security license



```
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#lic
Router(config)#license boot module c1900 tech
Router(config)#license boot module c1900 technology-package sec
Router(config)#license boot module c1900 technology-package
securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE
OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING
```

Fig. 3 Configuration of the security license



```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
--------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102
```

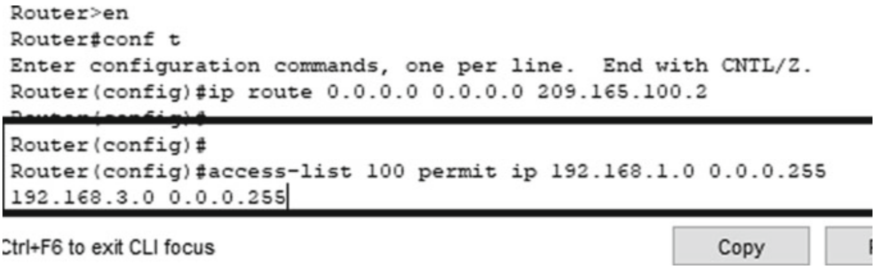
Fig. 4 Router with security license

Figure 5 shows the access-list configuration. The access-list grants permission to allow traffic from one network to the other through the tunnel. The access-list only allow listed IP addresses to communicate across the tunnel.

The policy and key enable the router to utilize IP security as showed in Fig. 6. Every ISAKMP coverage is assigned a unique precedence number among 1 and 10,000. The coverage with precedence number 1 is considered the highest priority policy.

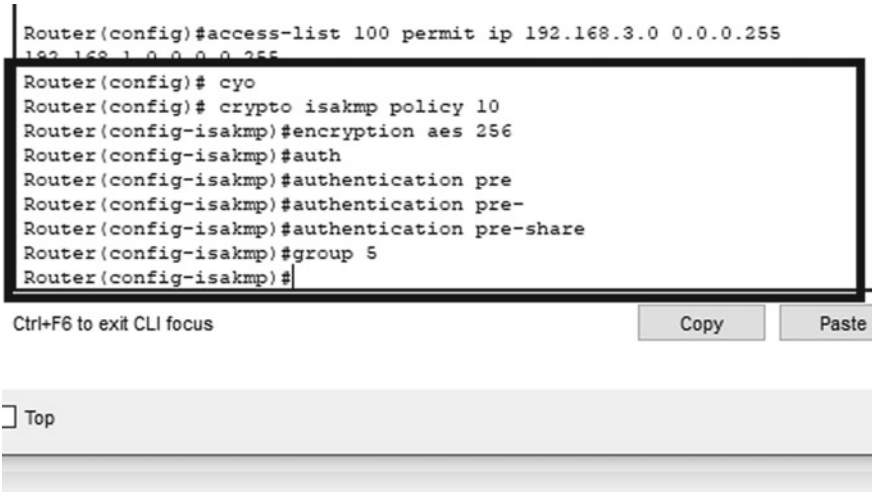
Figure 7 shows the IP sec transform-set configuration, which verifies authentication and integrity. A transform set is a merger of an IP sec transforms designed to enact a particular protection coverage for data traffic

Figure 8, shows the crypto mapping configuration. A crypto map is a configuration entity that select data flow that needs security processing. A crypto map must be named. In the configuration above, the crypto map name is "IPSEC-MAP". Figure 9 shows interface of the crypto map.



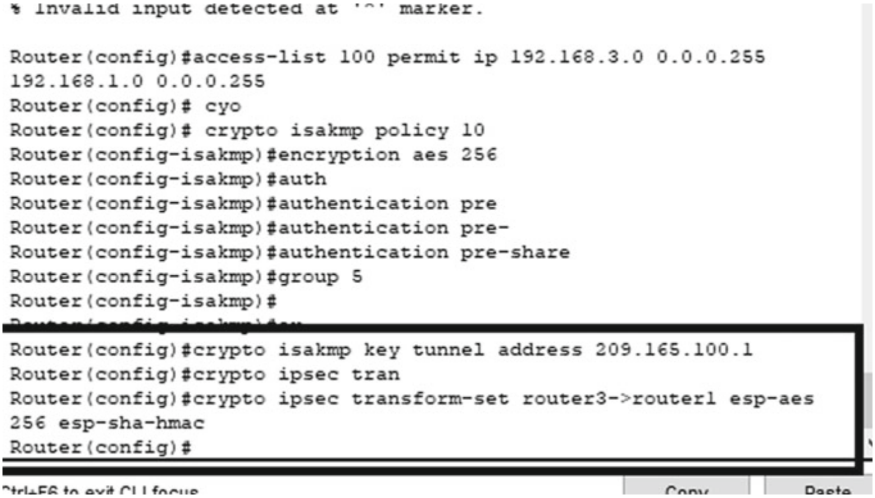
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
Router(config)#
Router(config)#
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

Fig. 5 Access-list



```
Router(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config)# cyo
Router(config)# crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#
```

Fig. 6 ISAKM policy and ISAKM key

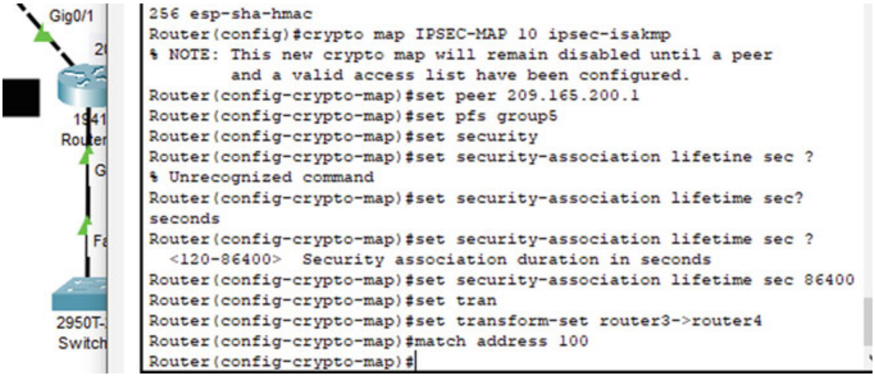


```
% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
Router(config)# cyo
Router(config)# crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#auth
Router(config-isakmp)#authentication pre
Router(config-isakmp)#authentication pre-
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#
Router(config-isakmp)#ex
Router(config)#crypto isakmp key tunnel address 209.165.100.1
Router(config)#crypto ipsec tran
Router(config)#crypto ipsec transform-set router3->router1 esp-aes
256 esp-sha-hmac
Router(config)#
```

Fig. 7 IPsec transform-set

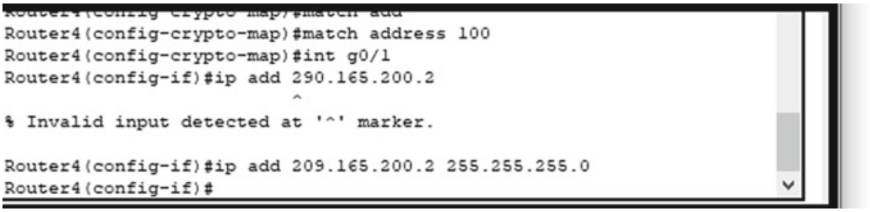
3.2 *Result and Discussion*

When using the real-time mode to check for the communication process, it is observed that laptop 2 could communicate with laptop 3 without router three been aware of the network; this process is seen using the simulation mode as shown in Fig. 10. Information about the VPN is checked from the inbound PDU details; it is



```
256 esp-sha-hmac
Router(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 209.165.200.1
Router(config-crypto-map)#set pfs group5
Router(config-crypto-map)#set security
Router(config-crypto-map)#set security-association lifetine sec ?
% Unrecognized command
Router(config-crypto-map)#set security-association lifetime sec?
seconds
Router(config-crypto-map)#set security-association lifetime sec ?
  <120-86400>  Security association duration in seconds
Router(config-crypto-map)#set security-association lifetime sec 86400
Router(config-crypto-map)#set tran
Router(config-crypto-map)#set transform-set router3->router4
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#
```

Fig. 8 Crypto map



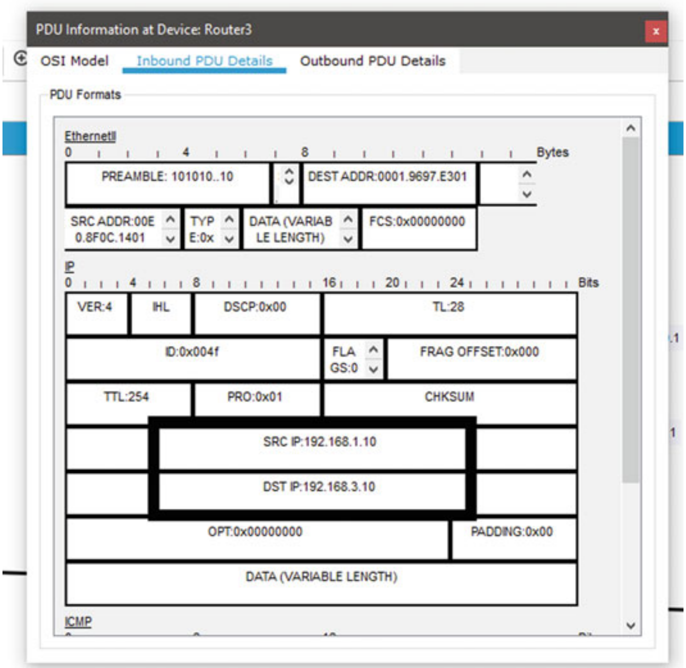
```
Router4(config-crypto-map)#match add
Router4(config-crypto-map)#match address 100
Router4(config-crypto-map)#int g0/1
Router4(config-if)#ip add 290.165.200.2
                              ^
% Invalid input detected at '^' marker.

Router4(config-if)#ip add 209.165.200.2 255.255.255.0
Router4(config-if)#
```

Fig. 9 The interfaces applied to the crypto map

noticed that router 3 had no idea about router 4 and router 5 but they are pinging across router 3 because of the VPN. From the simulation result below, only the source IP address 192.168.1.10 and the destination IP addresses 192.168.3.10 are seen, but the path through which the packet goes through is not recognized.

4 Conclusion and Future Work

This paper presented a VPN architecture within an organization that proposed solution to secure traffic through authentication, authorization, payload encryption and privacy protection. Simulation result on cisco packet tracer verifies that they provide secured traffic communication. This paper proposed a simple VPN solution that can be used in an organization. They also have the advantage of flexibility, connectivity and security at cheap cost. Organizational gains from VPN are increased in the scalability and productivity. Future work can be carried out by



EthernetII

PREAMBLE: 101010..10
DEST ADDR:0001.9697.E301
SRC ADDR:00E0.8F0C.1401
TYPE:0x
DATA (VARIABLE LENGTH)
FCS:0x00000000

IP

VER:4
IHL
DSCP:0x00
TL:28
ID:0x004f
FLAGS:0
FRAG OFFSET:0x000
TTL:254
PRO:0x01
CHKSUM
SRC IP:192.168.1.10
DST IP:192.168.3.10
OPT:0x00000000
PADDING:0x00
DATA (VARIABLE LENGTH)

Fig. 10 Simulation result

using other simulation packages order than cisco packet tracer for a simple VPN connection within an organization, and also, the model can also be expanded by using VPN connections across multiple countries.

Acknowledgements The authors appreciate the sponsorship from Covenant University through its Center for Research, Innovation and Discovery, Covenant University, Ota Nigeria.

References

1. Odusami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., Ahuja, R.: An improved model for alleviating layer seven distributed denial of service intrusion on webserver. J. Phys.: Conf. Ser. **1235**(1), 012020 (2019)
2. Odusami, M., Misra, S., Abayomi-Alli, O., Abayomi-Alli, A., Fernandez-Sanz, L.:. A survey and meta-analysis of application-layer distributed denial-of-service attack. Int. J. Commun. Syst. **33**(18), e4603 (2020)
3. Draper-gil, G., Lashkari, A.H., Saiful, M., Mamun, I., Ghorbani, A.A.: Characterization of encrypted and VPN traffic using time-related features. In: Proceedings of the 2nd International Conference on Information Systems Security And Privacy (ICISSP), pp. 407–414, 2016
4. Busschbach, P.B.: ♦ Toward QoS-capable virtual private networks. Bell Labs Tech. J. **3**(4), 161–175 (1998)

5. Deshmukh, D., Iyer, B.: Design of IPSec virtual private network for remote access. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 716–719. IEEE, 2017
6. Nawej, M.C., Technologiae, M.: Evaluation of virtual private network impact on network performance (2016)
7. Liyanage, M., Gurtov, A.: Secured VPN models for LTE backhaul networks. In: 2012 IEEE Vehicular Technology Conference (VTC Fall), Sept 2015, pp. 1–5. IEEE
8. Jaha, A.A., Ben Shatwan, F., Ashibani, M.: Proper virtual private network (VPN) solution. In: Proceedings of 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2008, pp. 309–314, 2008
9. Azhar, M.A., Saudi, M.M., Ahmad, A., Bakar, A.A.: Detection of social media exploitation via SMS and Camera. IJIM **13**(4), 61–78 (2019). Last accessed 01 Mar 21. https://www.learntechlib.org/p/208525/paper_208525.pdf
10. Chze, P.L.R., Leong, K.S.: A secure multi-hop routing for IoT communication. In: 2014 IEEE World Forum on Internet of Things, WF-IoT 2014
11. Das, A., Islam, M.M.: SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems. **9**(2), (2012)
12. Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.: Security issues in mobile ad hoc networks. Proc. Comput. Sci. **3**(5), 1022–1024 (2014)
13. Wu, B., Chen, J., Wu, J., Cardei, M.: COUNTERMEASURES IN
14. Dinesh, D., Kumar, A., Singh, J.: Security attacks in mobile adhoc networks (MANET): a literature survey. Int. J. Comput. Appl. **122**(20), 31–35 (2015)
15. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Netw. **13**(6), 24–30 (1999)
16. Manvi, S.S., Tangade, S.: A survey on authentication schemes in VANETs for secured communication. Veh. Commun. (2017)
17. Assadhan, B., Moura, J.M.F., Lapsley, D., Jones, C., Strayer, W.T.: Detecting botnets using command and control traffic, 4, 156–162 (2009)
18. Lan, J., Zhou, J., Liu, X.: An area-efficient implementation of a message authentication code (MAC) algorithm for cryptographic systems. In: IEEE Reg. 10 Annual International Conference Proceedings/TENCON, pp. 1977–1979, 2017
19. Liu, Z., Lallie, H.S., Liu, L., Zhan, Y., Wu, K.: A hash-based secure interface on plain connection, 1236–1239 (2011)
20. Padmavathi, G., Subashini, P., Aruna, M.D.D.: ZRP with WTLS key management technique to secure transport and network layers in mobile adhoc networks. Int. J. Wirel. Mob. Netw. **4**(1), 129–138 (2012)
21. Liang, Y., Poor, H.V., Shamai, S.: Secure communication over fading channels. IEEE Trans. Inf. Theory **54**(6), 2470–2492 (2008)
22. Kobayashi, M., Shitz, S.S.: Secured communication over frequency-selective fading channels : a practical vandermonde precoding, 2009 (2009)
23. Azeez, N.A., Salaudeen, B.B., Misra, S., Damaševičius, R., Maskeliūnas, R.: Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics **12**(2), 200–213 (2020)
24. Osho, O., Musa, F.A., Misra, S., Uduimoh, A.A., Adewunmi, A., Ahuja, R.: AbsoluteSecure: a tri-layered data security system. Commun. Comput. Inf. Sci. **1078**, 243–255