Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator

Dwi Ely Kurniawan*, Hamdani Arif, N Nelmiawati, Ahmad Hamim Tohari, Maidel Fani

Department of Informatics Engineering, Politeknik Negeri Batam, Indonesia

*dwialikhs@polibatam.ac.id

Abstract. The Internet provides less guarantee of security in the process of information exchange. Virtual Private Network (VPN) IP Security(IPSec) based has been implemented to overcome this issues. This research builds a private network that provides quality and security in accessing the Internet. The entire set of systems were built in a virtual and simulated manner. It is built using GNS3 network simulator software and virtual Cisco ASA Firewall. The result shows that VPN network connectivity is strongly influenced by the hardware used as well as depend on Internet bandwidth provided by Internet Service Provider (ISP). In addition to the security testing result shows that IPSec-based VPN can provide security against Man in the Middle (MitM) attacks. However, the VPN still has weaknesses against network attacks such as Denial of Service (DoS) that causes the VPN server can no longer serve VPN client and become crashes.

1. Introduction
The Internet is a common used to interconnect the world. However, it lacks of security guarantee in terms of information exchange. Due to security reasons, data confidentiality, integrity and availability are important factor that needs to be considered. Therefore, there are lots of security solution have been provided to secure information exchange through the Internet.

Based on the background, VPN is one of solutions have been provided. It is a private connection that uses a public network. It works through tunneling and encryption technology. Moreover, it requires a set of protocol extensions that can provide security assurance, data integrity, and confidentiality. The protocol is IP Security ie, a new standard tunneling technology used on VPN. On this research tries to analyze and implement IP Security (IPSec) on Virtual Private Network (VPN) using GNS3 network simulator software and virtual Cisco ASA Firewall. The entire set of systems has been built in a virtual and simulated manner. It is used to get a good end result before IPSec-based Virtual Private Network technology is applied directly to the real network.

Several similar studies such as an implementation of IPSec-VPN [1], integrate the Two-Factor Authentication Service (TFAS) into low-cost VPN systems [2]. The system has been applied to set up TFAS for VPN system in a bank. The other study compares Packet Tracer (PT) and GNS3 from the perspective of ability and complexity of strengths and weaknesses respectively [3], simulates a corporate network to lower costs with a Wide Area Network (WAN) [4], VPN technology of secure communications between remote locations [5]. From the research, there is no revealing related to the use of Cisco ASA firewall in implementing and analyzing IPSec-VPN on GNS3 Lab. And test the use of VPN and non-VPN networks.
2. Method

The research has built IPSec protocol on the virtual computer network. Topology design used in two types; general topology and network topology in GNS3. General topology is an illustration to show the shape of the network in real conditions, while network topology on GNS3 is the topology used for simulation purposes. Both topologies are the same network topology only used for different purposes. Data retrieval using observation and experiment method directly to the system. The following topology images will be used.

![General Network Topology](image1.png)

Figure 1. General Network Topology

![Network Topology in GNS3](image2.png)

Figure 2. Network Topology in GNS3

On this research was using VPN with Remote Access type ordinary also called Virtual Private Dial-up Network (VPDN). This type of VPN has been used to connect the VPN client to the local network. The client will utilize the VPN service to gain Internet access and get assurance of security against hacker attacks such as Man in The Middle (MiTM) attack during the Internet used.
In general, tunnels are built using point-to-point connections. In the tunneling process, the data will be broken down into smaller sections called packets. As the packet moves through the tunnel, the packets are encrypted and a process called encapsulation will occur. The encapsulation process alters the data packets that are sent to look like ordinary packets (public data), so packets sent over the public network are unnoticed.

The first step is to build a network by installing two virtual PCs ie Windows XP which will act as VPN client and Kali Linux which will act as an attacker to test the VPN network. Firewall is the most important component on this research that is a VPN server. Before VPN can be built the first thing to do is to install Cisco ASA Firewall. In conjunction with the host computer, it needs Qemu. The setting of the ASA firewall is done by disabling CPU throttling and then entering the following command in Kernel-Command-Line.

```
-append ide_generic.probe_mask=0x01 ide_core.chs=0.0:980,16,32 auto
nousb console=ttyS0,9600 bigphysarea=65536 idel=noprobe no-hlt -net
-nic
-vnc none -vga none -m 1024 -icount auto -hdachs
980,16,32
```
Generally, VPN clients can not access the Internet from within the tunnel, therefore a special configuration is required. The following steps are the step to complete ASA firewall configuration.

1. Create hostname ASA
2. Setting ip address outside on GigabitEthernet0 and GigabitEthernet1 interface
3. Create object network and NAT on network inside. Dynamic interface is used to provide LAN-USERS internet access.
4. In order for VPN client to access internet via tunnel it will be used U-turn traffic or hairpin. Source traffic on this NAT is Outside, the VPN-POOL Network will access the internet located on the Outside Network so that the connection through the tunnel will be reversed to the source in order to access the internet.

![Diagram](image)

**Figure 5. Illustration of U-Turn Traffic**

5. Specifies the DHCP IP to be assigned to the VPN client when it is connected to the VPN network. 192.168.137.1 is an IP VirtualBox host-only adapter on Host machine (Windows 8) ie as internet gateway.
6. Create a VPN client username and password. Encrypts the Internet Key Exchange version 1 protocol with AES-256 encryption.
7. Implementation of the IPSec protocol.
8. Create group-policy ie, VPN POLICY with dns server 8.8.8.8 and configure for every traffic to be through tunnel.
9. Creating a tunnel-group remote-access with the VPN-POLTEK name and ikev1 pre-shared-key vpn123.
10. Last is to configure the default policy. IPSec has been successfully implemented. Use the "show crypto" command to display the configuration results.

The local network (Inside Network) is configured with a router so that it can communicate with the VPN client. The router uses IP with 10.1.1.0/24 subnet and gateway 10.1.1.100.

3. Results and Discussions

Connectivity test experiments carried out by running the VPN client software. Before you can connect to a VPN network the first thing to do is to configure the connection list. The VPN client will get the configured DHCP up on the VPN server when connected to the VPN network. Connectivity testing is done by running Ping command to LAN router and then accessing the internet via VPN network.
Test analysis consists of two mechanisms namely the mechanism of connectivity testing and VPN network security.

- The connectivity testing mechanism will be performed on VPN and non-VPN networks. The testing mechanism is carried out with several parameters; traceroute (tracert), delay, round trip time (rtt), packet loss and bandwidth.
- The security testing mechanism on the VPN network is done with several parameters, namely Attacking using Denial of Service (DoS) and Man in the Middle Attack (MitM).

3.1. Traceroute Test
Traceroute (tracert) testing is done by using the tracert command to find out which route the host must travel through to get to the destination. Traceroute will be performed from Windows XP (VPN client) with the aim of www.google.co.id. Figure 7 shows that the connection through the firewall (192.168.137.100) on the first hop before heading to the gateway (192.168.137.1).

3.2. Delay Test
The delay test is performed on VPN and non-VPN networks. Testing is done by pinging from host to destination using Wireshark software. Based on the delay category is obtained ping testing from host to destination at a certain time as much as 400 times the test is divided into 4 times the test.

| Category delay  | ms   |
|-----------------|------|
| Excellent       | <150 ms |
| Good            | 150 - 300 ms |
| Poor            | 300 - 450 ms |
| Unacceptable    | >450 ms |

Table 1. Standard delay according to ITU
Figure 8. Delay Test on Network VPN and Non-VPN

Figure 8 show that can be deduced that the VPN network can provide better network quality compared to unstable non-VPN networks. The results obtained VPN network is quite good and can still be maximized again.

3.3. Round Trip Time (RTT) Test
Round Trip Time measurement is done on VPN and non-VPN network with ping command to send 100 ICMP packets from client to google.co.id.

Figure 9. RTT Experiment Network VPN and Non-VPN

From the test results in figure 9 show that non-VPN networks have better Round Trip Time (RTT) than VPN networks. This is due to the number of hops that a packet has to pass across a VPN network more in number than the number of hops on a non-VPN network.

3.4. Packet Loss Test
This test is to monitor the average, minimum and maximum packet loss over VPN or non-VPN networks. In this test is done by sending 100 ICMP packets from client to google.co.id same as testing on Round Trip Time (RTT). The results show that both VPN and non-VPN networks have good connectivity in the absence of Packet Loss.
3.5. **Bandwidth Test**

Bandwidth testing is done by downloading files from Dropbox over VPN and non-VPN network ie, file installer GNS3 with size 43.6 Mb using internet WiFi with bandwidth 5 Mbps. Testing is done using Wireshark.

![Traffic Table](image)

**Figure 10. Bandwidth of VPN Network**

Figure 10 shows the download time is 155,235 sec and the average bandwidth is 0.125MBit / sec. This amount is not big enough than it should be. Where in real conditions the average speed on the VPN network can reach 54 Mbps even more. This is due to factors such as the transmission media used in real conditions using fiber optics with a maximum speed of 1Gbps, a much higher device specification and support, and large RAM capacity on the server.

![Traffic Table](image)

**Figure 11. Bandwidth of Non-VPN Network**

Figure 11 shows the download time is 170,235 sec and the average bandwidth is 2,407MBit/sec. This amount is much larger than that obtained by VPN network but, it is not very influential because the speed of file download over VPN network is faster than the non-VPN network. Some are caused by factors such as the VPN server (Firewall) filtering the data traffic from the Internet so the number of packets received is less, and the size of the filtered packet has become smaller. As for the bandwidth problem obtained VPN network, caused by the following factors;

- On topology, VPN server only acts as a security service provider for VPN client in accessing the internet.
- Internet gateway is on the outside network.
- Because the VPN server only acts as a service provider, it takes U-Turn Traffic for VPN clients to access the internet, thus affecting the bandwidth that VPN networks can obtain.

3.6. **Denial of Service (DoS)**

The Denial of Service experiment aims to stop or shut down the service on the target computer, in this case, the VPN server. Denial of Service (DoS) is done with hping applications on Linux Times. The target IP address to be attacked is the public IP VPN server (192.168.137.100).
After the attack for about 1 minute then the attack was stopped and obtained the result of packet delivery as much as 2329905 packages and caused the VPN server to crash.

From the above test results can be concluded that the DoS attack successfully attacked and disabled the VPN server in real time. In this case, the VPN server is still vulnerable to attack, although the VPN server has a series of defenses against basic attacks (Basic Threat Detection). To overcome this required higher security by using additional software or hardware Intrusion Prevention Systems (IPS).

3.7. Man in the Middle Attack (MitM)

Man in the Middle Attack (MitM) is one of the hacking attacks carried out from within the network to tap the information. In this test will be done interception of VPN and non-VPN networks. VPN network testing will use the Ettercap app on Linux Times. Before doing the first sniffing determine the target to be attacked ie local server IP (192.168.137.100) and local IP client (192.168.137.5). Then start unified sniffing and select ARP poisoning to start the attack.
Figure 13 shows the VPN client accessing www.facebook.com, but Ettercap cannot catch anything. Next will run the application URLSnarf to tap the client. URLSnarf is a sniffing tool or application that will capture the targeted URL or visited by the target.

Figure 15. URLSnarf the Network VPN

Figure 15 shows URLSnarf cannot capture URLs accessed by the client. This is because the connection is done through the tunnel and the VPN client gets the DHCP IP from the VPN server. Therefore client activity cannot be tapped by the attacker. Based on testing of non-VPN networks it can be concluded that non-VPN networks do not have a security mechanism at all and any activities performed on non-VPN networks can be easily tapped by the attacker.

4. Conclusion

VPN network running well and stable and able to provide better network quality compared to non-VPN network. This can be seen from the time delay and download time better than non-VPN network. But the VPN network that is built still has a deficiency that is in the Round Trip Time (RTT) is quite large compared to non-VPN network. VPN network connectivity is heavily influenced by the hardware used and depends on the Internet bandwidth provided by the Internet Service Provider (ISP). The result of security testing shows that IPSec based VPN can provide security against MiTM (Man in The Middle) attack. However, VPN network still has weaknesses against network attacks such as DoS (Denial of Service) that causes VPN server can no longer serve VPN client and crash.

Acknowledgments

Authors thanks to everyone in Informatics Engineering Department who helped us to finish this study. We also thanked to Meti and Pratama for help us collecting data and developing software for our study.

References

[1] Salman F A, 2017 Implementation of IPsec-VPN tunneling using GNS3 Indones. J. Electr. Eng. Comput. Sci. 7, 3 p. 855–860.
[2] Thanh P N and Kim K, 2013 Implementation of open Two-Factor Authentication service applied to Virtual Private Network in International Conference on Information Networking.
[3] Chou T-S Keith Baker S and Vega-Herrera M, A Comparison of Network Simulation and Emulation Virtualization Tools.
[4] Janarthanan V, 2014 JISET -International J. Innov. Sci. Eng. Technol. 1, 6.
[5] Harmening J T, 2013, Virtual Private Networks, in Computer and Information Security Handbook.