Journal of Engineering Technology Vol. 9(1): 102-107, 2021
ISSN 2231-8798© 2013 UniKL BMI

The Study of Adaptive Security Appliances Implementation in Virtual Private Network

Miswani Atika Mohd Abdullah, Ahmad Roshidi Amran
[1,2]Communication Technology Section
British Malaysian Institute, Universiti Kuala Lumpur
53100, Gombak, Selangor, Malaysia

Corresponding email: aroshidi@unikl.edu.my

Abstract: According to USA Today, a website that discussed about security network, there were over 130 million malicious software programs were released in 2013 mainly to steal personal, business, and financial data from the personal networks, business and the government. Hackers began to develop a malicious threat aimed at military, government, and commercial networks to steal their data so that hackers can use it to blackmail them if they not fulfilling their request. As the grow of malicious threats rising rapidly, many network administrator or IT professionals start to develop security appliances such as firewall, antivirus, and intrusion prevention system to protect against network harms. New security devices are developed as well such as Cisco Adaptive Security Appliances (ASA). Therefore, research was carried out to study the reliability of Cisco ASA and its configuration. This research is looking on how ASA combines function of firewall, Authentication, Authorization and Accounting protocols (AAA protocols) in virtual private network. The research is conducted using simulation software namely Cisco Packet Tracer by establishing a small-scale network model. The configurations include the application of Access-Control List, configuring the security-level of the network to separate between inside network (private) and outside network (public). Therefore, with proper configurations, any unauthorized access from the outside network are unable to gain entry to the private network to steal confidential data and to install malware.

Keywords: adaptive security appliance, firewall, protect personal data

1.0 INTRODUCTION

According to USA Today, a website that discussed about security network, there were over 130 million malicious software programs were released in 2013 mainly to steal personal, business and financial data from the personal networks, business and the government. As the rising of malicious threats are found, IT professionals are developing many software or hardware to help to secure the network of an organization. Network security nowadays have become an integral part of computer networking and involves in technologies, protocols, device to secure data.

Intrusion Detection System (IDS) was the first tools that were developed in 1984 which it provides real-time detection of certain types of attacks while they are in progress. This well help network security professionals to mitigate the impact of those attacks by using the detection. In 1990s. network security professionals starts to introduce Intrusion Prevention System (IPS) to slowly replace IDS as it enables the detection of harmful threats activity and automatically block the attack in real-time.

Firewalls were then developed to prevent unauthorized traffic for entering private network. The firewalls were made as software features in the existing network devices such as routers. As time goes by, many IT company had developed dedicated firewalls that enable routers and switches to offload memory and the processor-intensive activity of filtering packets. Cisco's Adaptive Security Appliance (ASA) is available as a standalone context-aware firewall

An ASA provides a proven, comprehensive firewall solution. The Cisco ASA 5500 series is a primary component of the Cisco Secure Borderless Network. It delivers superior scalability, a broad range of technology and solutions, and effective, always-on security designed to meet the needs of a wide array of deployments.

2.0 LITERATURE REVIEW

2.1 Modern Network Security Threats

Malicious international threats cause the rise of development of security threats. When the internet was firstly launched, the users did not engage with any activity that might harm the network therefore the development of security network is not required. As time goes by, the threats are rising in numbers and worrying therefore network security professionals need to develop a technique to secure the network as the first Denial-of-Service (DoS) attacks started to occur.

Mohan V. and Anuradha J (2015) claimed that network attack can be in passive or active form. Passive form is when a network intruders intercepts data traveling through the network while active form is when an intruder initiates commands to disrupt the network's normal operation

2.1.1 Type of Network Attacks

Active Attack
Example of active attacks are Sinkhole, Denial of services, wormhole attack and modification.

Passive Attack
Example of passives attacks are eavesdropping, monitoring and eavesdropping

Advance Attack
Example of advance attacks are Black hole attack, Rushing attack, Replay attack and Byzantine attack.

To ensure the safety and security of the networks, the network should be installed with reliable antivirus software and update it regularly. The operating system should be updated regularly and forbid any unwanted access to any users of the network.

2.2 Cisco Adaptive Security (ASA) 5500 Series Firewall

Cisco ASA 5500 is amongst the advance device in securing organizational networks and systems. Threat detection function is one of the most valuable features. Therefore, this paper presents a fuzzy logic aided intelligent threat detection solution, which is a cost-free, intuitive and comprehensible solution, enhancing and simplifying the threat detection process for all.[2]

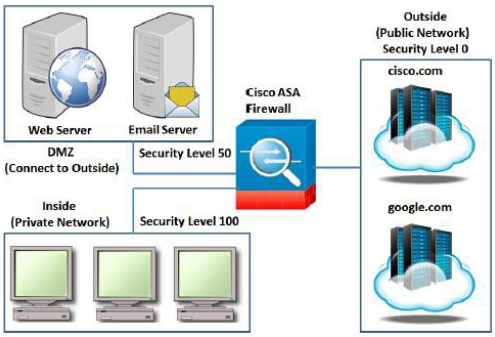


Figure 1: The structural diagram of Cisco ASA Firewall illustrating the connectivity inside, outside.

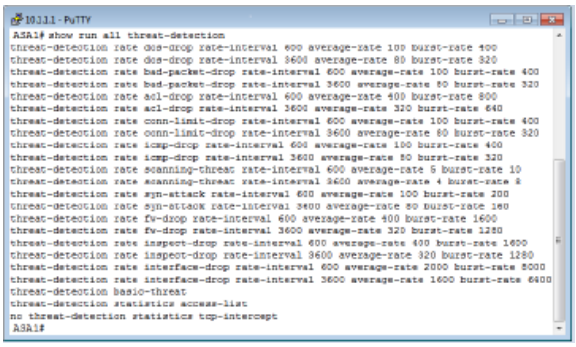


Figure 2: Default Basic Threat Detection Statistics for 10 minutes (600 seconds) and 60 minutes (3600 seconds)

When any of these threats are detected by the Cisco ASA Firewall, a syslog message will be generated on the device (and the external syslog server, if configured).

The researcher concluded that the fuzzy logic aided intelligent threat detection system enhances the threat detection in Cisco ASA. The proposed system employed a fuzzy reasoning system which was based on the threat detection statistics and the presented results/threats, through to the developed dashboard user interface for ease of understanding for administrators/users.

3.0 METHODOLOGY

The ASA version used in this study is Cisco ASA 5505 as it consists of firewall for small business, branch, and enterprise teleworker environments[1]. Therefore, it is suitable to be applied at small scale network to study its configuration to be installed in small business organization.

Cisco ASA 5505 helps business reduced its operational course as it can be easily managed as it features a flexible 8-10 port can be dynamically group into three Virtual Local Area Network (VLANs) as for the separation of the department in the company.

The simulation runs using Cisco Packet Tracer, Cisco Packet Tracer 6.2sv using Windows 10 operation system.

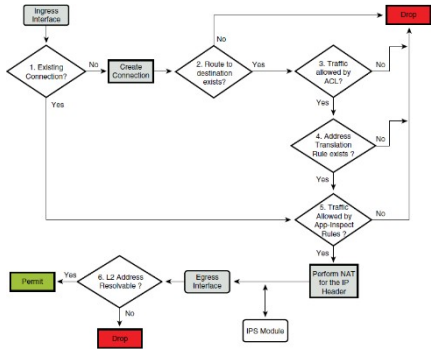


Figure 3: The flowchart of SA is being configured.

The above figure shows the flowchart on how ASA is being configured and how Cisco ASA manage the traffic that pass through it. The flow of the packet can be operated by the scenario when a user inside of the network was trying to access to a website such as Google that is located at the internet which is located outside the network. Then, the packets hit the inside interface of ASA and ASA will verify whether the packets were from the existing connection of internal network. ASA is then checked the packet against the interface of Access Control Lists (ACL). If the packets matched with the allowed ACL entry, it would move forward however, if it does not match with ACL entry, the packets will be dropped.

After that, the packet will undergo inspection to verifies the packet flow with compliance of the protocol. ASA created the inspection through Modular Policy Framework (MPF). If it passes the inspection, the packets will move forward, while if it is not, the packet will be dropped. Next, the actual network address translation happens at this step where the IP header information is translated according to Network Address Translation (NAT) or Port Address Translation (PAT) rules. The ASA translates the internal host address to a global address. The ASA will be restoring the original IP address for detection when the traffic is returned later.

The packet will now be forwarded to the outside interface and the destination interface is decided based on global route lookup and finally packet will be forward by ASA to the next hop.

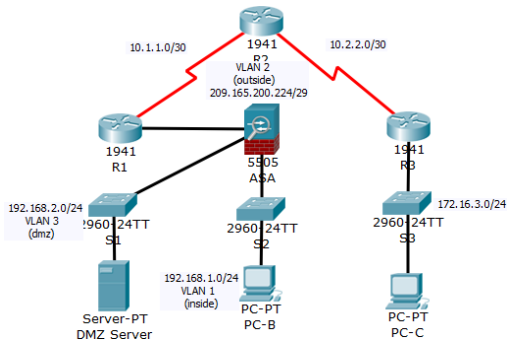


Figure 4: The network topology.

Figure above shows the network design in the simulation Packet Tracer. The network includes 3 routers which each has been assigned as DMZ, Inside and Outside zone. The assignation was used to separate network between private network and public network. The Cisco ASA in this network used Cisco ASA 5505 model.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Figure 5 shows the IP addressing table for the network design.

The IP addressing table shows the IP address of the devices in the network. The network used class C IP address.

4.0 RESULTS AND DISCUSSION

In the results section, it will show the configuration and Cisco ASA. Configuration of Cisco ASA used Command-Line Interface (CLI) in Packet Tracer and connectivity were tested using ICMP pings in Command Prompt.

4.1 The basic configuration for routers has been done for example configure hostname of the routers, configuring IP address of the host and the servers. The configuration made will enable pinging to show that the network equipment is ready and connected.

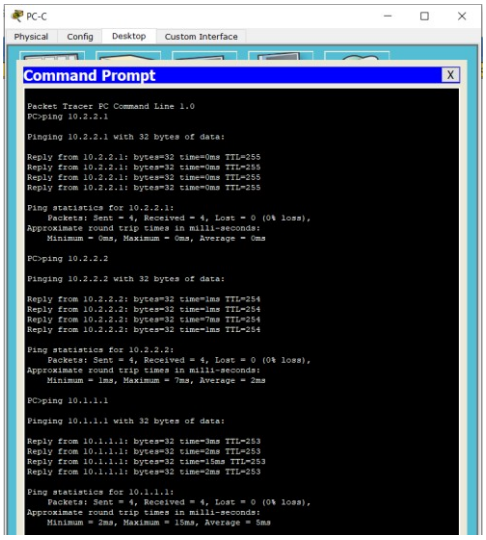


Figure 6: The pinging from PC-C to the router's interface. The pinging is successful.

Since the ASA has not been configured yet, therefore the pinging from PC-B to the ASA and the network inside ASA were not successful. This is due to there is no connection between the PC-C and the network inside the ASA.

4.2 Configuration of inside and outside interface

Figure 7: The interface of ASA with Vlans has been configured.

A Virtual LAN(VLAN) is a subnetwork where it group together a bundle of devices or host on the separated local area networks (LAN). A LAN is a group of computer or devices that shared communications line to a server in the same geographical area. With VLAN, it was easy to partition a single switched network to match the functional and security requirements of the system without having to install new cables.

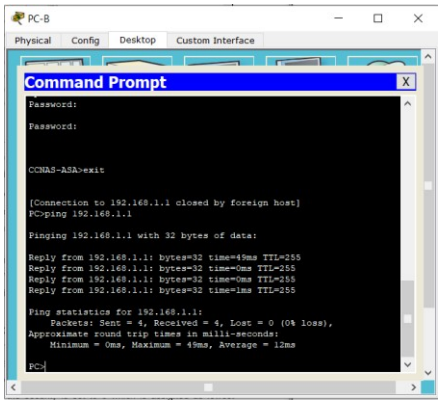


Figure 8: The successful pinging from PC-B(inside network) to Cisco ASA Vlan 1

The pinging shows that only authorized access from the inside network are able to ping to ASA interface. This prevent ASA from being hacked and harmed.

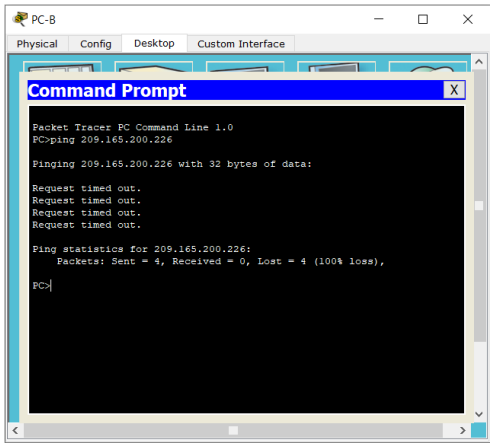


Figure 9:The unsuccessful pinging from PC-B(inside network) to Vlan2(outside).

The unsuccessful pinging results above shows that the outside network are not permitted to the inside network as the result of the pinging to outside vlan2 interface IP address 209.165.200.226 are failed

```
CCNAS-ASA#config t
CCNAS-ASA(config)#int vlan 1
CCNAS-ASA(config-if)#nameif inside
CCNAS-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#security-level 10
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)#int vlan 2
CCNAS-ASA(config-if)#nameif outside
CCNAS-ASA(config-if)#ip address 209.168.200.226 255.255.255.248
CCNAS-ASA(config-if)#security-level 0
```

Figure 10: The configuration of Vlan assigned on the ASA interface.

The ASA 5505 has 8 layer and 2 switch ports. There are 2 types of interfaces configured which is logical vlan interface and switch virtual interface (SVI). On global configuration mode, the SVI has been created and the security level has been assigned. Security level is to assign the interface and separated it to be outside and inside the network.

4.3 Configuration of default static route

A default route is also known as the gateway of the last resort. The route configured on the Cisco ASA is used to forward traffic when no other router exists in the routing table for specific destination network. A default static route is also known as quad zero route as it has four zeros in the IP route command.[4]. This command supports the use of the next hop IP address. Moreover, using the static route 0.0.0.0 is not dependent on any routing protocols as when the Cisco ASA is not able to search a route in its routing table, it forwards the packet to the default route

```
CCNAS-ASA#config t
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#end
CCNAS-ASA#sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    192.168.1.0 255.255.255.0 is directly connected, inside
     209.165.200.0/29 is subnetted, 2 subnets
C       209.165.200.0 255.255.255.248 is directly connected, outside
C       209.165.200.224 255.255.255.248 is directly connected, outside
S*   0.0.0.0/0 [1/0] via 209.165.200.225
CCNAS-ASA#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

CCNAS-ASA#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figure 11: The configuration of static default route and verification in ASA.

With static default route configuration, the ASA can ping R1 interface which means traffics from R1 can now enter the ASA.

4.4 AAA protocol configuration

AAA is an abbreviation for authentication, authorization and accounting. AAA is a framework that intelligently control the access to the computer resources, auditing usage, enforcing policy and providing the information necessary to bill for services.

```
CCNAS-ASA(config)#username admin password adminpa55
CCNAS-ASA(config)#aaa authentication ssh console local
```

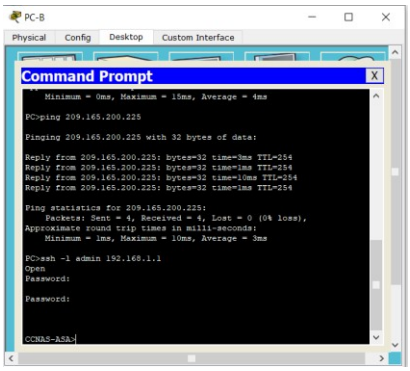
Figure 12: The configuration of AAA in the Cisco ASA.

The configuration of AAA above required user to enter the username : admin and password : adminpa55 when accessing the Cisco ASA. This is to prevent unauthorized access to the Cisco ASA. The configuration of authentication ssh is using local database which is refer to the username : admin and password : adminpa55. This is recommended that the username and password match with the username and passwords on the AAA servers. Therefore, it will provide transparent fallback support.

4.5 SSH configuration

Secure Shell protocol (SSH) is a method to secure remote login from one network device/computer to another[5]. It provides several alternative options for strong authentication and protects the network security with strong encryption. The SSH timeout configured 10 means only 10 seconds provided for user to key in the username or password.

To enable ssh session remotely from the host to the PC, the authentication is required to access the cisco ASA otherwise the login should be failed.



4.6 Configuration of DMZ

Demilitarized Zone (DMZ) is a physical or logical subnet that separates internal LAN from the external LAN which is public network. DMZ locates the external-facing servers, resources and services[6]. Therefore, they are accessible from the internet but not the rest of the internal LAN as it remains unreachable.

```
CCNAS-ASA#config t
CCNAS-ASA(config)#int vlan 3
CCNAS-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)#no forward interface vlan 1
CCNAS-ASA(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNAS-ASA(config-if)#security-level 70
CCNAS-ASA(config-if)#int Ethernet0/2
CCNAS-ASA(config-if)#switchport access vlan3
                                        ^
% Invalid input detected at '^' marker.

CCNAS-ASA(config-if)#switchport access vlan 3
CCNAS-ASA(config-if)#end
```

Figure 14: The configuration on vlan as DMZ of Cisco ASA

As the server does not need for to communicate with the inside server, the command no forward to interface vlan 1 is configured. The security level is set to 70 means that traffics are allowed from the inside network to the DMZ but not from the DMZ back to the inside network. This is to allow the user to connect with the internet securely without worrying outsiders to try to hack the network inside.

```
CCNAS-ASA#config t
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)#access-group OUTSIDE-DMZ in interface outside
```

Figure 15: The configuration of the ACL.

The ASA ACL permit statement must permit access to the internal private DMZ address. The external devices access the server using its public static NAT address, the ASA translates it to the internal host IP address then applies the ACL

5.0 CONCLUSION

The Adaptive Security Appliance (ASA) is standalone firewall device that can protect the inside network from any unauthorized access outside the network. ASA combines the function of firewall, AAA protocol, Intrusion Prevention System functionality into one device and also have the ability to support advanced features such as virtualization, identity firewall, high availability failover and advanced threat control. ASA can be configured in routed mode or in transparent mode

The ASA device has been configured and managed using CLI (Command Line) by using packet tracer simulation for this research. The ASA CLI proprietary OS(OperatingSystem) which has similar look and feel to the router IOS. The configuration and functionalities of ASA has been studied thoroughly with the implementation at CLIinterface.

The capability of ASA to combine the functionalities of Firewall, AAA protocols, Access Control and VPN cryptography have made the device, a very versatile network security appliance. This is evident from the observed result in multiple ways such as by trying to telnet to Cisco ASA from computers in the inside network where username and password were prompted with full authentication and encryption, ensuring unwanted access in the network. Thus, preventing any pilfering of confidential data. The Cisco ASA is not daunting to configure, and the security features are proven reliable which could be adopted by small businesses to protect their network. The objective is achieved.

6.0 REFERENCES

[1] Cisco ASA 5505 Adaptive Security Appliance for Small Office or Branch Locations Data Sheet. (2016, June 2). Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733510.html

[2] Naik, N., Jenkins, P., Kerby, B., Sloane, J., & Yang, L. (2018). Fuzzy logic aided intelligent threat detection in Cisco adaptive security appliance 5500 series firewalls. *IEEE International Conference on Fuzzy Systems*, *2018-July*. https://doi.org/10.1109/FUZZ-IEEE.2018.8491574

[3] Marjanovic, U. (2009). Exploration Of A Method For Constructing An Industrial Ethernet With Ethernet Enabled Devices In An Industrial Environment Using A Cisco Adaptive Security Appliance.

[4] Static and Default Routes. (2020, June 25). Retrieved from https://www.cisco.com/c/en/us/td/docs/security/asa /asa97/configuration/general/asa-97-general-config/route-static.html

[5] SSH Protocol – Secure Remote Login and File Transfer. (n.d.). Retrieved from https://www.ssh.com/ssh/protocol/

[6] What is a DMZ (networking)? | Barracuda Networks. (n.d.). Retrieved from shorturl.at/bhkHL.