



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: <https://doi.org/10.22214/ijraset.2022.44006>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Comparing Context Based Access Control to Zone-based Policy Firewalls

Alnuman Mohammed Abubaker Altamezwi¹, Abdulwahed Omran E Alalwani², Ashour Alslami³

^{1,2}Technical College of civil Aviation & Meteorology

Abstract: *This paper will be introducing a comparative study on the choices between two best classical software firewalls one is Context Based Access Control (CBAC) and Zone Based firewall (ZBF). Both of them may deliver a stateful inspection of TCP, UDP and/or ICMP control packets. Through this study, two type of networks were designed one used the CBAC firewall and the other works with a zone based firewall. The result obtained showed that ZBF has several feature which are not available in CBAC. Furthermore, ZBF deals with the security zones the traffic will be dynamically inspected as it passes through the zone.*

In order to monitor the network, GNS3 and Wirshrah tools has been used to configure the required network. Then we have used different scenarios to inspect and evaluate the behavior of the network. In this study firewalls were implemented in software not in hardware as separate devices. That is, they are building functions of the routers. In our project, two networks were designed The first one has two areas LAN and WAN, while the second contains three areas LAN, WAN and DMZ.

Key Words: CBAC; ZBF; GNS3; Wirshark; TELNET; SSH; HTTP; Ping.

I. INTRODUCTION

A firewall act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall. In firewall all traffic from inside to outside and vice versa must pass through it. It may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. Firewalls are an excellent security mechanism and, when appropriately selected and implemented, can establish a relatively secure barrier between a system and the external environment. This paper describes the principal of two types of stateful firewalls that are available and presents the advantages and disadvantages of each type one called Context Based Access Control (CBAC) and other Zone-Based Firewalls (ZBF). Although, this project will not examine them, instead concentrating on the operation and configuration of CBAC. In addition, through this paper we will address the operation of CBAC, its benefits, limitation. Finally work through the steps involved in configuration CBAC.

A. Motivation

A firewall is a dedicated hardware, or software or a combination of both, Because of scalability and ease of configuration Cisco developed, a new approach for router-based firewalling known as Context Based Access Control (CBAC) and Zone-based policy Firewall (ZFW), rather than using devices will used only software on the routers by using one of those firewalls. Consider zone based firewall better than context based access control list whereas ZFW introduces the concept of security zones, which allow simpler definition of the degree of trustworthiness of a given interface making administrators lives a lot easier when deploying firewall policies. Zone based policy introduces a new firewall configuration model where policies are applied to traffic moving between zones not interfaces. No interference between multiple inspection policies or ACLs.

B. Context Based Access Control (CBAC)

Cisco's original implementation of a router-based stateful firewall called Context Based Access Control (CBAC) or, in other words, the Classic Input/Output System (IOS) Firewall. The basic configuration element of CBAC is the "ip inspect" command, which instructs IOS software to monitor connection initiation requests for a particular (L4 or L7) protocol that arrive on a given router interface, consider robust stateful inspection based firewall solution for those smaller organizations that may be operating on a tight budget. Cisco IOS firewall feature set allow significant flexibility in managing a perimeter Cisco. The CBAC router is configured to inspect traffic generated inside our network and going through the CBAC router. Figure 1 below shows. It does not include any traffic generated by the router itself. Any traffic generated by the router itself will not be inspected and catered for and will instead have to deal with the current access control list configured on the outside interface (namely deny any log).

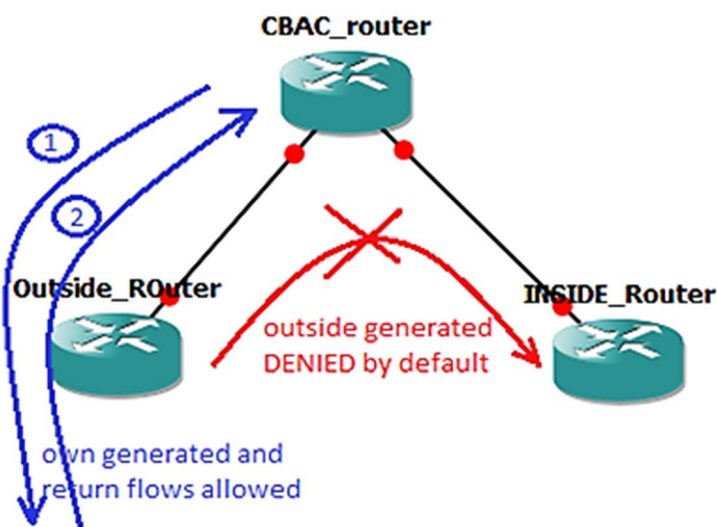


Figure 1 way to work CBAC

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic, which would normally be blocked, and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered CBAC when exiting through the firewall.

C. Traffic Inspection

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions. Inspecting packets at the application layer, and maintaining TCP and UDP session information, provides CBAC with the ability to detect and prevent certain types of network attacks such as SYN flooding. CBAC inspects packet sequence numbers in TCP connections to see if they are within expected ranges CBAC drops any suspicious packets. You can also configure CBAC to drop half-open connections, which require firewall processing and memory resources to maintain. Additionally, CBAC can detect unusually high rates of new connections and issue alert messages. CBAC can provide more protection against certain DoS attacks involving fragmented IP packets.

D. Zone-Based Firewalls (ZBF)

The Cisco IOS Zone Based Firewall is one of the most advanced form of Stateful firewall used in the Cisco IOS devices. ZBF completely changes the way you configure a Cisco IOS Firewall inspection, as compared to the Cisco IOS Classic Firewall. The zone based firewall (ZBFW) is the successor of Classic IOS firewall or CBAC (Context-Based Access Control). When the large corporate networks began to be connected to less-secure public networks (for example, the early Internet), security-conscious network administrators immediately started to feel the need to secure their internal networks from potential intruders. The ZBFW mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones. Also the traffic will be dynamically inspected as it passes through the zones. The zone based firewall came up with many more features that is not available in CBAC

E. Security Zones & Security Zone Firewall Policies

A zone is a group of interfaces that have similar functions or features. They help you specify where a Cisco IOS XE firewall should be applied. whereas security zone is a group of interfaces to which a policy can be applied. By default, traffic flows among interfaces that are members of the same zone. In Security Zone Firewall Policies a class identifies a set of packets based on its contents. Normally, you define a class so that you can apply an action on the identified traffic that reflects a policy. A class designed through class maps. An action is a functionality that is typically associated with a traffic class. For example, inspect, drop, and pass are actions.

F. Implementing Zone-Based Designs

Many devices used in firewall implementations are using a concept of packet filters to filter traffic arriving or departing through an interface. For example, Cisco IOS implements packet filters with the ip access-list and ip access-group configuration commands that enable you to specify filtering conditions based on source and destination IP addresses, Layer 4 protocol (for example, TCP, UDP, or ICMP), and Layer 4 port numbers (for example, TCP port 80 for HTTP). The design below show Figure 2 simple firewall with perimeter

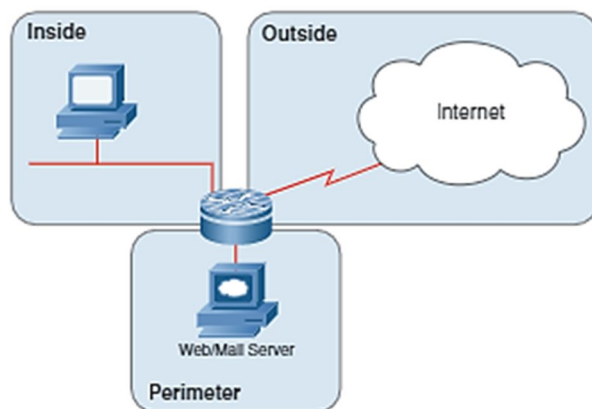


Figure 2 simple firewall with perimeter

However, implementing even a straightforward firewall policy (like the one described in the “Simple Zone-Based Design ”Section) with Cisco IOS access lists can lead to a configuration nightmare.

II. SIMULATION TOOLS USED

In our paper work we are using two software programs GNS3 (Graphical Network Simulator) and Wireshark first software using to configuration all commands and other to monitor the traffic packets exchange between different networks. In our work we are designed the network as below in figure 3 to find the differentiation between two firewall and the configuration on the edges router R1 and R4. The network design process for the simple network has taken the following steps:

- 1) Selecting router devices that support all commands.
- 2) Design the network connection between LAN and WAN; according to the standard organizational structure.
- 3) Configuring static routes as the main routing configuration.
- 4) Implementing the CBAC and ZBF to provide security firewall to the network.

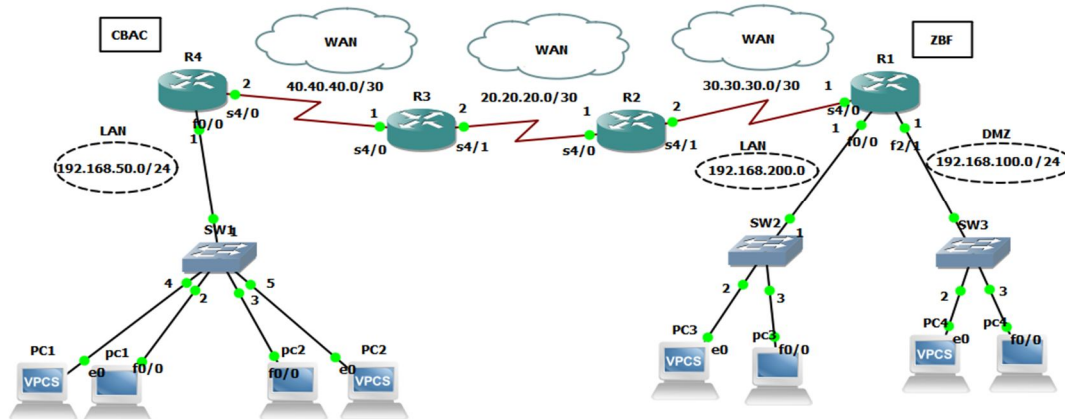


Figure 3 find the differentiation between two firewall

III. DEVICES USED IN THE NETWORK

Table 1 lists the devices selected to implement the sample network, which contain routers, switches, PCs and cloud devices composing the sub-networks of the design.

Table 1 The main devices used to design the sample network

Devices	Devices types
Routers	Emulated CISCO 7200
Switches	Ethernet Switch and always on
Computers	PCs/VPCs devices
Cloud device Internet	Device for external connection

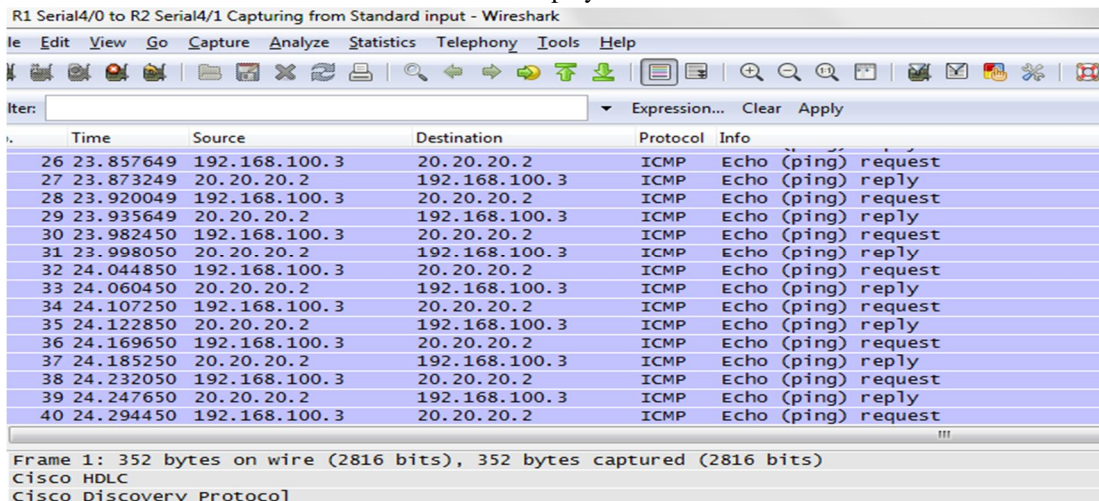
IV. RESULTS AND FINDINGS

This shows the Verification Commands and results of comparison between CBAC and ZBF firewalls. We used Wireshark to get the result and we will use some commands and protocols to test our project for example Ping,SSH protocol, Telnet, HTTP and HTTPs protocol so we apply and enable this commands and protocol in our work we will choose only two results of every connection.

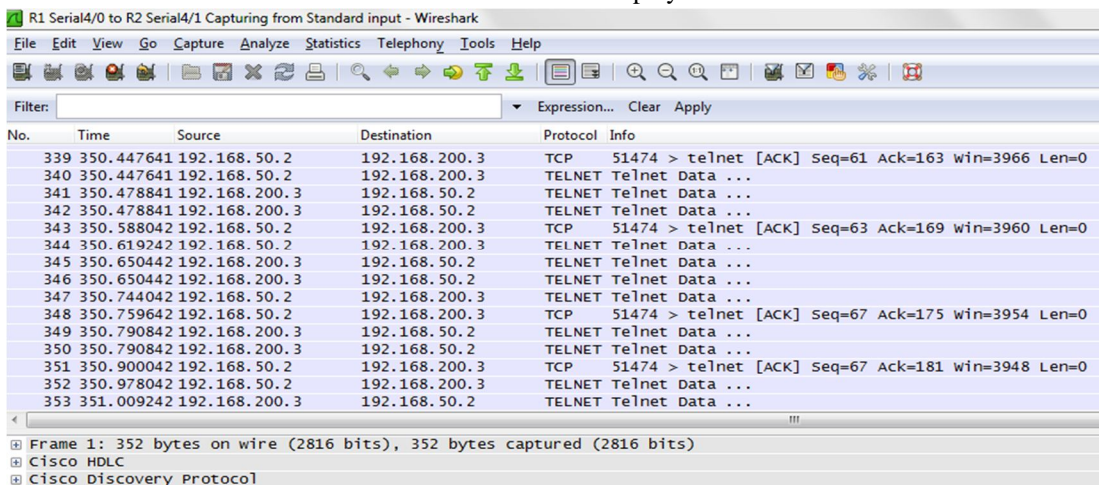
A. Using static Routing Protocol Without Firewall

In all figures when we use the commands to test the result there is always a reply or we can say successful.

1) Test ping command from 192.168.100.3 to 20.20.20.2 the replay is successful



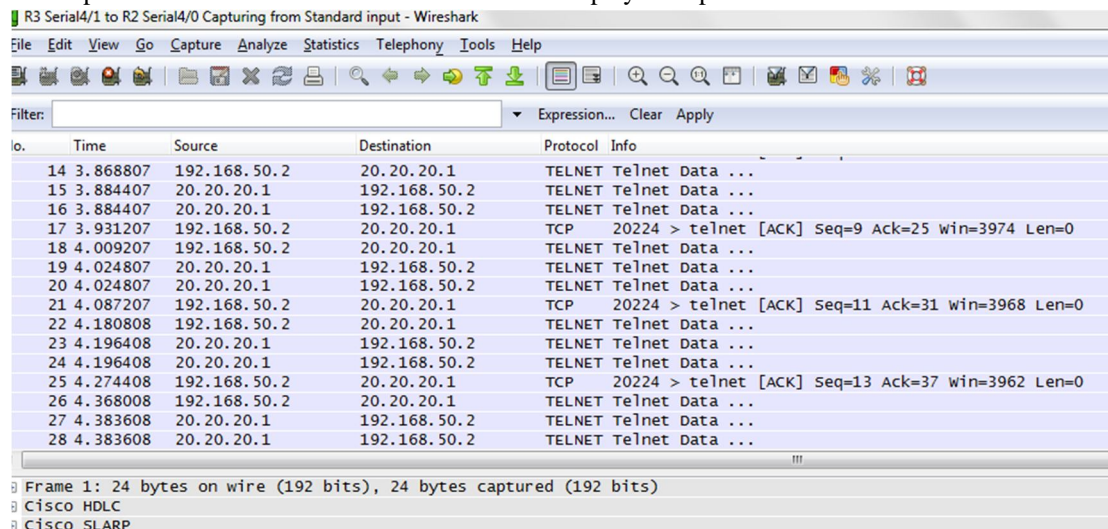
2) Test the telnet command from 192.168.50.2 to 192.168.200.3 the replay is successful



B. Using CBAC firewall from LAN -TO –WAN

In this case all commands and protocols which be sent from LAN to WAN will be successful because the configuration which we have done must be LAN connect to the internet or outside the WAN whereas allow all traffic (TCP , UDP,ICMP) to send ,upload and download any files or messages from WAN areas.

1) Test telnet protocol from 192.168.50.2 to 20.20.20.1 the replay is response.

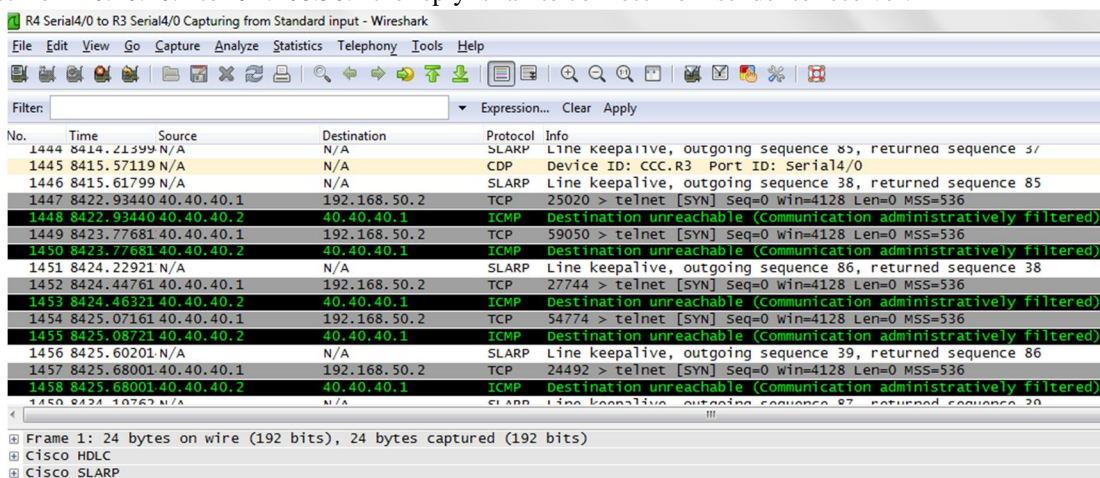


No.	Time	Source	Destination	Protocol	Info
14	3.868807	192.168.50.2	20.20.20.1	TELNET	Telnet Data ...
15	3.884407	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
16	3.884407	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
17	3.931207	192.168.50.2	20.20.20.1	TCP	20224 > telnet [ACK] Seq=9 Ack=25 Win=3974 Len=0
18	4.009207	192.168.50.2	20.20.20.1	TELNET	Telnet Data ...
19	4.024807	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
20	4.024807	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
21	4.087207	192.168.50.2	20.20.20.1	TCP	20224 > telnet [ACK] Seq=11 Ack=31 win=3968 Len=0
22	4.180808	192.168.50.2	20.20.20.1	TELNET	Telnet Data ...
23	4.196408	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
24	4.196408	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
25	4.274408	192.168.50.2	20.20.20.1	TCP	20224 > telnet [ACK] Seq=13 Ack=37 win=3962 Len=0
26	4.368008	192.168.50.2	20.20.20.1	TELNET	Telnet Data ...
27	4.383608	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...
28	4.383608	20.20.20.1	192.168.50.2	TELNET	Telnet Data ...

C. From WAN TO LAN in case of using CBAC.

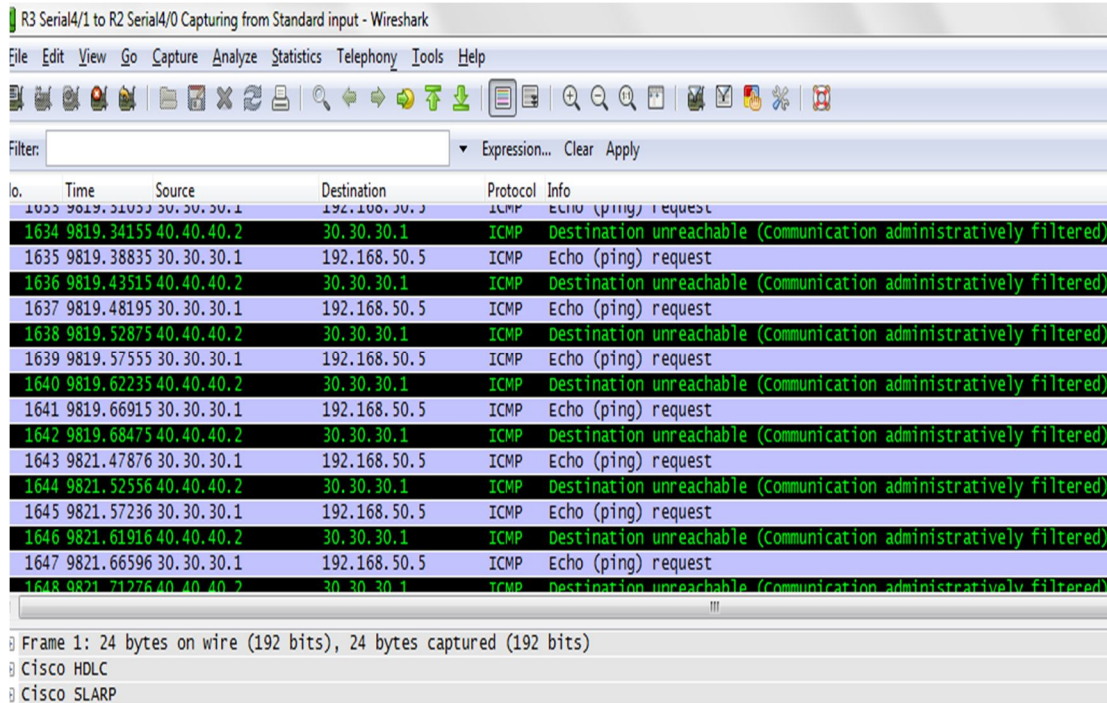
In this case all packet will response unreachable or fail to connect.

1) Test telnet from 40.40.40.1 to 192.168.50.2 the reply is fail to connect from sender to receiver.



No.	Time	Source	Destination	Protocol	Info
1444	8414.21399	N/A	N/A	SLARP	Line keepalive, outgoing sequence 85, returned sequence 3/
1445	8415.57119	N/A	N/A	CDP	Device ID: CCC.R3 Port ID: Serial4/0
1446	8415.61799	N/A	N/A	SLARP	Line keepalive, outgoing sequence 38, returned sequence 85
1447	8422.93440	40.40.40.1	192.168.50.2	TCP	25020 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
1448	8422.93440	40.40.40.2	40.40.40.1	ICMP	Destination unreachable (Communication administratively filtered)
1449	8423.77681	40.40.40.1	192.168.50.2	TCP	59050 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
1450	8423.77681	40.40.40.2	40.40.40.1	ICMP	Destination unreachable (Communication administratively filtered)
1451	8424.22921	N/A	N/A	SLARP	Line keepalive, outgoing sequence 86, returned sequence 38
1452	8424.44761	40.40.40.1	192.168.50.2	TCP	27744 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
1453	8424.46321	40.40.40.2	40.40.40.1	ICMP	Destination unreachable (Communication administratively filtered)
1454	8425.07161	40.40.40.1	192.168.50.2	TCP	54774 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
1455	8425.08721	40.40.40.2	40.40.40.1	ICMP	Destination unreachable (Communication administratively filtered)
1456	8425.60201	N/A	N/A	SLARP	Line keepalive, outgoing sequence 39, returned sequence 86
1457	8425.68001	40.40.40.1	192.168.50.2	TCP	24492 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
1458	8425.68001	40.40.40.2	40.40.40.1	ICMP	Destination unreachable (Communication administratively filtered)
1459	8424.10762	N/A	N/A	SLARP	Line keepalive, outgoing sequence 87, returned sequence 20

2) Test ping command from 30.30.30.1 to 192.168.50.5 the reply is fail to connect from sender to receiver



No.	Time	Source	Destination	Protocol	Info
1634	9819.34155	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1635	9819.38835	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1636	9819.43515	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1637	9819.48195	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1638	9819.52875	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1639	9819.57555	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1640	9819.62235	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1641	9819.66915	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1642	9819.68475	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1643	9821.47876	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1644	9821.52556	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1645	9821.57236	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1646	9821.61916	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)
1647	9821.66596	30.30.30.1	192.168.50.5	ICMP	Echo (ping) request
1648	9821.71276	40.40.40.2	30.30.30.1	ICMP	Destination unreachable (Communication administratively filtered)

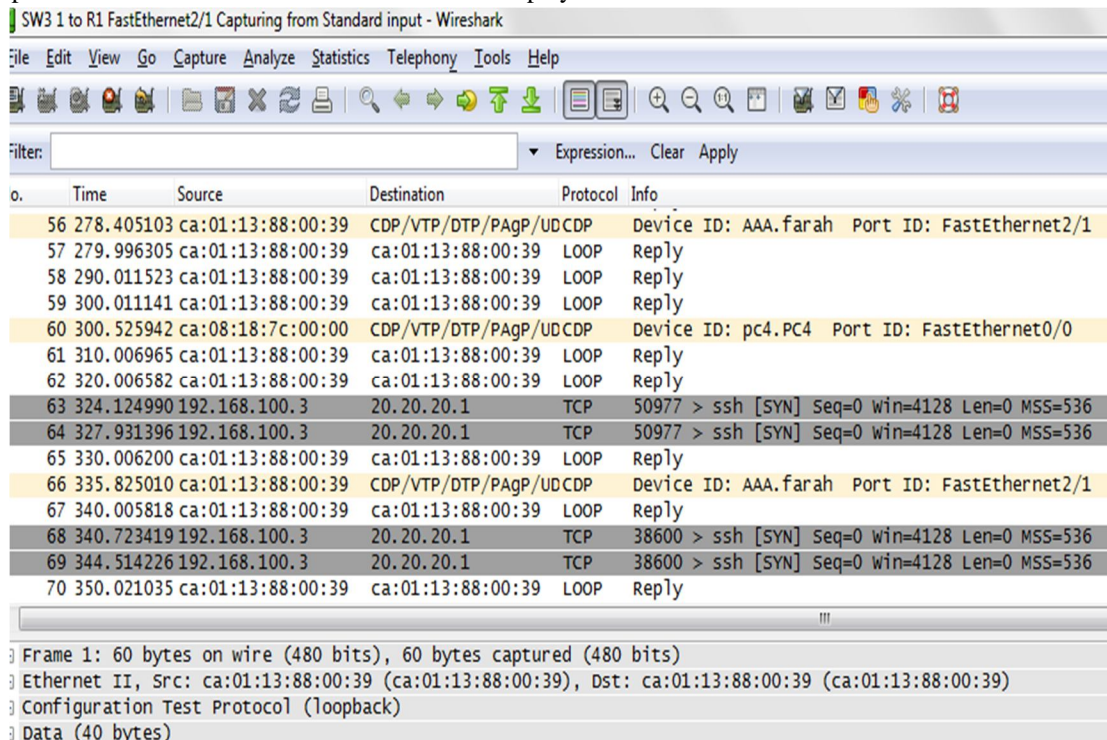
D. Third after using ZONE Based Firewall.

In this case the area of DMZ can't connect with LAN as well as WAN because this area supposed be server's area that's way we can't allow to the any server computer for example to the enter Internet web page.

E. Form DMZ to LAN and WAN

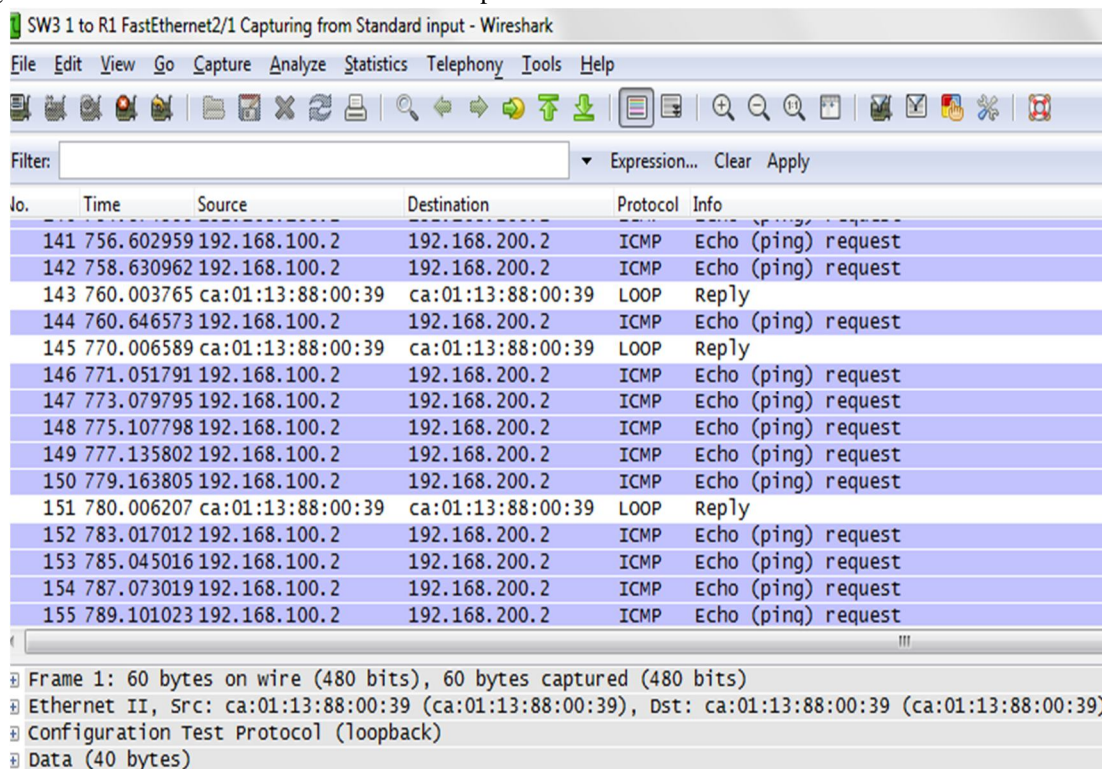
In this case all protocols will be deny, and this also applies to from WAN to LAN.

1) Test SSH protocol from 192.168.100.3 to 20.20.20.1 no replay



No.	Time	Source	Destination	Protocol	Info
56	278.405103	ca:01:13:88:00:39	ca:01:13:88:00:39	CDP/VTP/DTP/PAGP/UDCDP	Device ID: AAA.farah Port ID: FastEthernet2/1
57	279.996305	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
58	290.011523	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
59	300.011141	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
60	300.525942	ca:08:18:7c:00:00	ca:01:13:88:00:39	CDP/VTP/DTP/PAGP/UDCDP	Device ID: pc4.PC4 Port ID: FastEthernet0/0
61	310.006965	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
62	320.006582	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
63	324.124990	192.168.100.3	20.20.20.1	TCP	50977 > ssh [SYN] Seq=0 win=4128 Len=0 MSS=536
64	327.931396	192.168.100.3	20.20.20.1	TCP	50977 > ssh [SYN] Seq=0 win=4128 Len=0 MSS=536
65	330.006200	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
66	335.825010	ca:01:13:88:00:39	ca:01:13:88:00:39	CDP/VTP/DTP/PAGP/UDCDP	Device ID: AAA.farah Port ID: FastEthernet2/1
67	340.005818	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
68	340.723419	192.168.100.3	20.20.20.1	TCP	38600 > ssh [SYN] Seq=0 win=4128 Len=0 MSS=536
69	344.514226	192.168.100.3	20.20.20.1	TCP	38600 > ssh [SYN] Seq=0 win=4128 Len=0 MSS=536
70	350.021035	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply

2) Test ping from 192.168.100.2 to 192.168.200.2 no response found



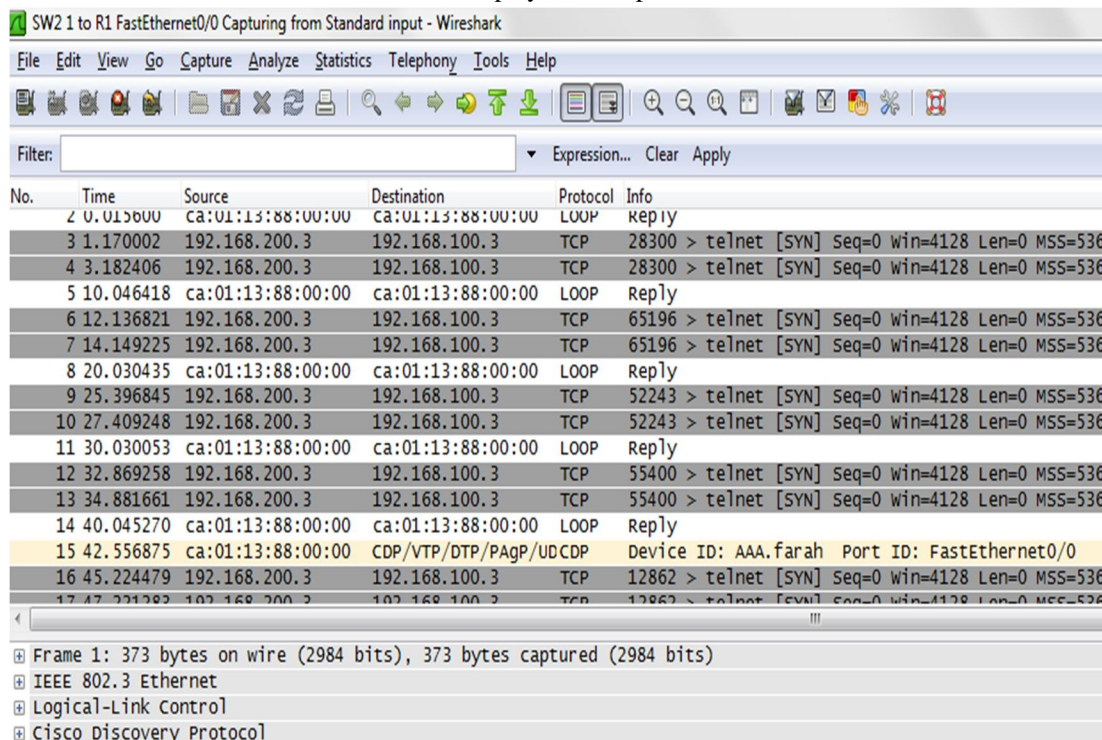
No.	Time	Source	Destination	Protocol	Info
141	756.602959	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
142	758.630962	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
143	760.003765	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
144	760.646573	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
145	770.006589	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
146	771.051791	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
147	773.079795	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
148	775.107798	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
149	777.135802	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
150	779.163805	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
151	780.006207	ca:01:13:88:00:39	ca:01:13:88:00:39	LOOP	Reply
152	783.017012	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
153	785.045016	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
154	787.073019	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request
155	789.101023	192.168.100.2	192.168.200.2	ICMP	Echo (ping) request

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 Ethernet II, Src: ca:01:13:88:00:39 (ca:01:13:88:00:39), Dst: ca:01:13:88:00:39 (ca:01:13:88:00:39)
 Configuration Test Protocol (loopback)
 Data (40 bytes)

F. From LAN to DMZ in zone based firewall

in this case we will allow just two protocol HTTP and HTTPs to be connect successful and other protocol not allow or no response, this also applies to from WAN to DMZ.

1) Test telnet from 192.168.200.3 to 192.168.100.3 the replay is no response found.



No.	Time	Source	Destination	Protocol	Info
2	0.015600	ca:01:13:88:00:00	ca:01:13:88:00:00	LOOP	Reply
3	1.170002	192.168.200.3	192.168.100.3	TCP	28300 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
4	3.182406	192.168.200.3	192.168.100.3	TCP	28300 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
5	10.046418	ca:01:13:88:00:00	ca:01:13:88:00:00	LOOP	Reply
6	12.136821	192.168.200.3	192.168.100.3	TCP	65196 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
7	14.149225	192.168.200.3	192.168.100.3	TCP	65196 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
8	20.030435	ca:01:13:88:00:00	ca:01:13:88:00:00	LOOP	Reply
9	25.396845	192.168.200.3	192.168.100.3	TCP	52243 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
10	27.409248	192.168.200.3	192.168.100.3	TCP	52243 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
11	30.030053	ca:01:13:88:00:00	ca:01:13:88:00:00	LOOP	Reply
12	32.869258	192.168.200.3	192.168.100.3	TCP	55400 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
13	34.881661	192.168.200.3	192.168.100.3	TCP	55400 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
14	40.045270	ca:01:13:88:00:00	ca:01:13:88:00:00	LOOP	Reply
15	42.556875	ca:01:13:88:00:00	CDP/VTP/DTP/PAGP/UDCDP	Device ID: AAA.farah Port ID: FastEthernet0/0	
16	45.224479	192.168.200.3	192.168.100.3	TCP	12862 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536
17	47.221282	192.168.200.3	192.168.100.3	TCP	12862 > telnet [SYN] Seq=0 win=4128 Len=0 MSS=536

Frame 1: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits)
 IEEE 802.3 Ethernet
 Logical-Link Control
 Cisco Discovery Protocol

2) Test http from 192.168.200.3 to 192.168.100.3 this allow to be connect

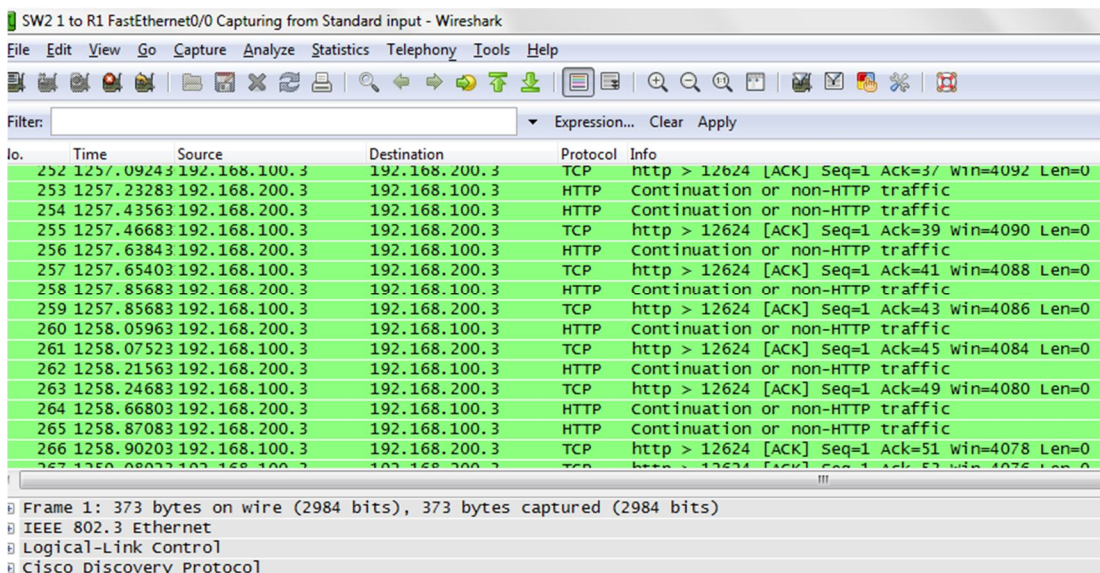


Table (4.1) this table explains the result showed of the comparison between CBAC and ZBF firewalls.

Protocols		http	https	telnet	SSH	Ping
CBAC	LAN TO WAN	Allow	Allow	Allow	Allow	Allow
	WAN TO LAN	Deny	Deny	Deny	Deny	Deny
ZBF	LAN TO WAN	Allow	Allow	Allow	Allow	Allow
	WAN TO LAN	Deny	Deny	Deny	Deny	Deny
	DMZ TO LAN TO WAN	Deny	Deny	Deny	Deny	Deny
	LAN TO DMZ	Allow	Allow	Deny	Deny	Deny
	WAN TO DMZ	Allow	Allow	Deny	Deny	Deny

V. CONCLUSION AND RECOMMENDATION

In this paper we apply the Context based access controls and zone based firewall in design using GNS3 and Wireshark tools, through this study we have notes these are vital when used Cisco routers. Although, CBAC and ZBF can be extremely useful in configuring an elementary stateful firewall inspection mechanism on a cisco router. Moreover, the cisco IOS zone based firewall is considered as one of the most advanced form of stateful firewall used in the Cisco IOS devices. The zone based firewall is the successor of the classical IOS firewall or context based access control.

By comparing Zone based to CBAC firewall we came up with many more features that is not available in CBAC. ZBF mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones. Also the traffic will be dynamically inspected as it passes through the zones.

However, through our practice, we noticed that Context based access depending on Interface Based Configuration and uses inspect statements, while zone based firewall depending on Zone Based Configuration and Uses Class-Based Policy language.

VI. FUTURE WORK

Certainly, developing and invent new approaches in the area of firewalls, whereas software has changed the rules of network security and businesses. Therefore, its necessary to have more confidentiality to protection. Thus, we recommend using hardware firewalls such as ASA CISCO firewall, FORTINET frigate firewall and PALO ALTO firewall etc.; rather than software firewalls because they provide more security to businesses.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)